Spammer Detection And Filtering Social Network Abstract

B.Gowtham[1], Dr. Arumugam.S[2]
[1]Dept of Computer Science And Application
[2]Assistant Professor, Dept of Computer Science And Application
[1, 2] Periyar Maniammai Institute Of Science And Technology, Vallam, Thanjavur, Tamilnadu,India

Abstract- *Securing the Message in the social network is one of the challenging tasks in this technological era. There are many type of intruder in the social media or personal application. The user's sensitive messages are stolen by many hackers where they make many psychological problems to them. To avoid this major disadvantage the proposed system implements the security system. Each of your chats has its own security code used to verify that your message or mail. These codes are unique to each message and can be compared between people in each chat to verify that the messages .you can send message with other person suddenly access the notification in your mobile phone. This is main advantages of avoid the misuse your message. The proposed system will greatly help the security enhancement of the end user where the data are protected more efficiently. Electronic mail, also known as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Email is the most efficient way to communicate or transfer our data from one to another. While transferring or communicating through email there is the possibility of misbehave.*

I. INTRODUCTION

Network security consists of the policies and practices take on to prevent and monitor unsanctioned access, misuse, diminish, or rebuttal of a computer network and network- accessible resources. Only network security can remove trojan horse viruses if it is activated. Network certainty covers a variation of computer networks, both public and private, that are used in everyday jobs; direct transactions and conveyance among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which stoutness be open to public access. Network security is involved in organizations, enterprises, and other types of phenomenon. It does as its title explains: It secures the network, as well as protecting and overseeing potency being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though virtual to stop unauthorized access, this constituent may fail to check potentially damaging content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and live in the action of such malware. An anomaly-based intrusion detection system may also praepost or the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis

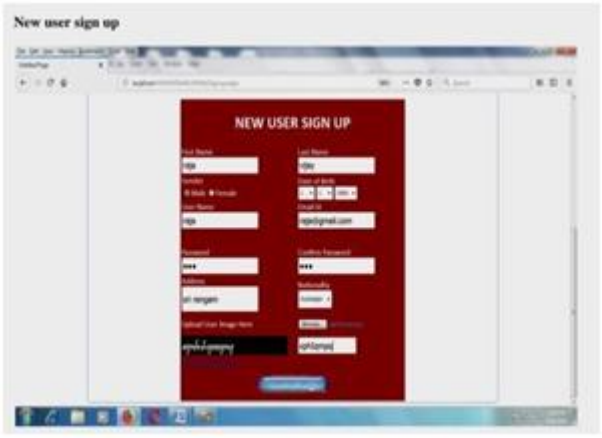
II. METHODOLOGY

A multilayer perceptron (MLP) is a feed forward artificial neural network that engendera set of outputs from a set of inputs. An MLP is characterized by assorted layers of input nodes connected as a directed graph between the input and output layers. MLP uses back propagation for training the network. Multi-layer Perceptron (MLP) is a supervised learning algorithm that learns a function because inputs are combined with the initial weights in a weighted sum and subjected to the activation function, just like in the Perceptron.

III. RESULT

Home page:

Login:



Search request:

My profile:

IV. CONCLUSION

Due to enormous usage of internet technology, there is a huge increase in the network attacks.

Among them, spam is considered as one of the main attacks in launching various attacks like stealing user identities and spreading malware etc. In this project, a spam detector is mature, which can monitor and detect the machines involved in spam across the network. This tool is based on a spam filtering algorithm that has the efficiency of detecting high percentage of spam. It can differentiate spam and nonspam

affect machines in a network of any size. To avoid network administrator to view non-spam emails and to maintain the privacy among the clients in a network, encryption technique is used to encrypt them. The performance is evaluated based on the functionality and results generated with respect to the drawbacks of existing systems using the algorithm. This tool is considered as the light-weight tool because of its minimal amount of time and observations to detect a spam. It can also be used in a network consisting of any number of clients by providing an aggregate large-scale view of the spam in an online manner.

V. FUTURE ENHANCEMENT

In future work, this tool can be extended to image spam detection as this one is completely based on the content spam filtering. It can be further enhanced by incorporating the sending message service feature to personal contact numbers if the spam exceeds the assumed threshold value. And finally, apart from spam attacks several other attacks can also be focused along with the protective measures.

REFERENCES

[1] Beginning ASP.NET 4: in C# and VB by Imar Spaanjaars.
[2] ASP.NET 4 Unleashed by Stephen Walther.
[3] Programming ASP.NET 3.5 by Jesse Liberty, Dan Maharry, Dan Hurwitz.
[4] Beginning ASP.NET 3.5 in C# 2008: From Novice to Professional, Second Edition by Matthew MacDonald.
[5] Amazon Web Services (AWS), Online at http://aws. amazon.com.
[6] Google App Engine, Online at http://code.google.com/appengine/.