CHAPTER 4

METHODOLOGY FOR PREVENTION OF CYBER CRIME USING CLASSIFIER ACCURATELY AND EFFICIENTLY DETECTS SUSPICIOUS URLS

4.1 OVERVIEW

Online Social Networks gives the ability to control the messages which were posted to avoid the unwanted content on their own private space displayed by the users. This system has direct full control on the messages of user which were posted on their boundaries. Unfortunately, in the wrong hands, there are also effective tools for spam campaigns to be executed. It is a flexible rule-based structure that it agrees of users that make in order to the filtering criteria to be applied to their walls. To renovate spam communication into campaign for categorization fairly than examining them into individually, machine Learning-based soft classifier automatically finds out suspicious messages in support of content-based filtering. Mainly this research deals with twitter and face book to classify suspicious URLs and its related spam data in such a way that we designed our system as java as front end and My-SQL as back end.

4.2 INTRODUCTION

4.2.1 Online Social Network

Online Social Networks (OSNs) provides facility to post one’s own private space messages to avoid unwanted content and post it to the users. This is a system which allows the OSN users to have a direct access on the messages which is posted on their walls. Unfortunately, there are also effective tools to implement spam campaigns. A flexible rule-based system, allows users to customize the filtering criteria to be applied to their walls and spam messages are constructed into such campaign made for
classification rather than inspect them independently. Here the Machine Learning based soft classifier routinely labeling posters in support of content-based filtering techniques are used. A social network which in turn becomes a social structure made up of a set of common actor (such as organizations or individuals) and a set of the dyadic tie that are connecting these actors. This social network viewpoint analyses a set of functions for analyzing the structure of social entities and also with the categorization of theories which were appealing for explaining the structure of social entities in the patterns were observed in these structures.

A social networking service is a framework to build social relations among who share interest, activities, backgrounds or real life connection which is used to build social networks. Its representation consists of service of each user such as a profile in his or her common association and also with its variety of additional services. Most social network services are web-based and provide means for users to interrelate over the Internet facilities, such as instant messaging and e-mail etc. The links of the online community services are from time to time measured as a social network service, social network service usually means an individual-centered service whereas online community services are group-centered though in a broader sense. Social networking sites allow users to share ideas, posts, events, activities, pictures, and interests with people in their network. An Information filtering system is the one which removes unwanted or redundant information from an information stream using computerized or automated methods facilitate user to convey prior to appearance to a human user. Its key goal is to manage the information overload and to increment the meaning specific to the signal-to-noise ratio. To activate this user's profile this will be compared with a number of reference uniqueness. These ranges of machine method build on the identical morality as those for information mining. Here a notable application that can be found in the turf of email spam filter. Consequently, it is not only the information blast that necessitates
some form of filter, but also accidentally or unkindly introduces pseudo-information. One of the other usages is that it is being discussed in the use of social set of connections in the knowledge base communities.

Social networking allows to increase their familiarity and share ideas in scientific groups, and without these, the new means of making "isolated and irrelevant" and allows other users exterior to the group to open or to close access which were formed to supply with a mini-networks within the superior, more different social network examination. Unlike traditional Internet conversation and mailing lists which were communicated to users, grouping in social networking services allow moderators and owner alike to share related credentials between connections without having to log into every group or each individual groups.

The massive and dynamic character of this information creates the basis for the service of web content removal strategies aimed routinely to discover useful information. These are kept active to provide an active hold in complex and difficult tasks involved in OSN management in which it will be maintained in such a huge instance to access and manage control or information filtering. In reality, OSNs provides very little support to avoid unwanted communication on user walls. Provided that, this examination is not only a subject of using the previously defined web substance in mining practice for a dissimilar application, rather than it requires designing ad hoc categorization strategies. This happens because barrier messages constituted by petite text for which conventional classification methods have severe limitations since short texts do not provide enough word incidents. The main efforts in construction of a robust Short Text Classifier (STC) are concerted in the extraction and collection of description and discriminate features in web strategies. Among many online social networks, twitter and Secure Messager that seems like Facebook and dealt with here.
**Twitter**

Twitter is a micro blogging and an online social network service that enables users to mail and study "tweets" or letters, in which text messages are limited to 140 characters. These registered different numbers of users can interpret and place tweets but unregistered users are only allowed to read those tweets which were sent by the user. It is a social network, which was micro blogging, but it was firm to define, because it didn't reinstate to define anything. Twitter, in later stages actually was described as place to bring messages in an up to date approach for a common utility. They form tighter clusters on the network they follow one another more readily, they re-tweet each other more often, and more of their posts. Malicious server can include suspicious URLs through tweet post.

**Face book**

Face book is an online social networking service in which its name comes from a union of categorization for the directory given to students at some American universities. The founders had originally limited the website's association to Harvard students and in the later stages this was expanded to colleges in the Boston area, Stanford University and the Ivy League. It steadily added and to extent its support form students at different other universities before it was released to high-school students, and ultimately to any person aged Thirteen and over. Face book, now allows everyone who claims to be at least 13 years old to turn into a listed user of the website to its host. Users must schedule before using the site, following which they may create an individual outline, exchange messages, and receive automatic announcement when they keep their profile posted.
4.2.2 URL Redirection

URL redirection, which is also called URL forwarding, is a World Wide Web procedure for making a web page existing under more than one URL deal with its address. When a web browser tries to open a URL and that has to be redirected, a page with a different URL is released. The URL redirection can be used for URL restriction and to stop broken links when web summon are moved and also agree to such a multiple domain names fit in to the same owner to refer to a particular web site. It also guides such navigation into and elsewhere even to some of a website, for privacy safety, and for less innocent principle such as phishing attacks. A redirect is a page which has no contented itself, but launch the reader to another critique, section of a page, or article usually from a different substitute title. The text prearranged in the link on an embattled redirect page must accurately match the target segment heading or anchor manuscript, including capitalization. URL redirects the received links to an out-of-date URL that can be sent to the truthful location. It is a crime if you apply these to any website without getting any permission from the owner. If crime is proved, he or she will be punished under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable. The malicious users will be punished of imprisonment, which may extended to three years or fine with five lakhs rupees under section 43(a).
4.3 SYSTEM ANALYSIS AND DESIGN

4.3.1 Problem Definition

Previous suspicious URL finding systems are pathetic at protection against restricted redirection servers that differentiate investigators from standard browsers and redirect them to gentle pages to cloak spiteful landing pages. Here new suspicious URL and spam data detection system has been found out for Twitter and Facebook that is ALERT SYSTEM Application tool. Dissimilar to the previous ALERT SYSTEM systems, this application tool is robust and defensive against provisional redirection, because it does not rely on the facial appearance of malicious hallway pages that may not be available and spam data. Instead, it checks the meeting point on the association of multiple redirect shackles that share redirection spam data and its servers. New features that are on the source of these association, implemented a real-time categorization system using these features such as to evaluate the system’s accurateness and their performance that has been initiated. The assessment results showed that our scheme is highly precise and can be deployed as a real-time system to categorize large samples of tweets and various messages from the Twitter public timeline and Facebook. In future, the system can be extended to address dynamic and multiple redirections. A scattered version of ALERT SYSTEM application tool to route all tweets and messages from the Twitter public timeline and Facebook has also been implemented.

4.3.2 Existing System

Account feature-based format use the characteristic features of spam account such as the ratio of tweets that hold the URLs. The examiner pages of character URLs in each tweet, which may not be effectively obtained and which will be considered to be the association of URL redirect chains are taken out from a number of tweets. The attacker’s possessions are generally limited and when needed reuse their URL redirect chains, which usually share the same URLs. The connected URL redirects chains and
their tweet to discover several features and context the information that can be used to classify apprehensive URLs and spam data. Conventional suspicious URL and spam detection systems are ineffective in their security against restricted redirection servers that discriminate investigators from normal browsers and forward them to kindly display pages to cover malicious landing of pages.

**Demerits of Existing System**

- It is ineffective against features fabrications
- No user defined BL
- Spammers can easily change the shape of message
- Plotting twitter graph is somewhat difficult
- Lack of BL Management
- It consumes much time and resources

**4.3.3 Proposed System**

Twitter and Face book users share a URL and data with friends via tweets or messages. In order to reduce the URL Length of messages in social network, they use URL shortened services and also their relation will focus on more robust features where malicious suspicious user cannot intrude in their connectivity. Account and relation feature based scheme does not detect spam messages from compromised accounts, because the compromised accounts have benign features. A link farming attacks for increasing spammers’ social influences have been conducted.

To cope with malicious tweets, many Twitter and Face book Spam Detection Schemes being proposed. Here in this research, an application tool - suspicious URL and spam detection system for Twitter and Facebook has been proposed. By using this tool multiple twitter and Facebook user account can be added. Initially, enable follow, unfollow, tweet, retweet etc... should be followed.
By selecting tweet we can enter the message in the text field and it automatically updates or can send message in twitter and Face book public timeline. If any suspicious URLs and data are present in that account which means it can easily be corrected and detected by our Application tool.

For the reason that attackers’ resources are limited and their need to be reused and a portion of their redirect chains have to be shared. So by use of this Application tool we categorize suspicious URLs from their normal URLs and spam data from normal data. The proposed method architecture is shown in Figure 4.1 and the proposed method data flow diagram is shown in Figure 4.2.

**Merits of Proposed System**

- Effectively remove unwanted message by FR.
- User defined block list is possible
- Investigate correlation of URLs
- Email provides the beneficiary a selection to respond instantaneously.
- A business opportunity for email service providers can be set as new data.
- Very quick and easy to find relevant information.

**4.3.4 System Architecture**

![Fig.4.1 System Architecture](image-url)
4.3.5 Data Flow Diagram

Fig. 4.2 Data Flow Diagram

4.3.6 System Requirements

Hardware Requirements

- **System**: Pentium IV 2.4 GHz
- **Hard Disk**: 160 GB
- **Monitor**: 15 VGA color
- **Mouse**: Logitech.
- **Keyboard**: 110 keys enhanced
- **Ram**: 1GB
Software Requirements

O/S : Windows XP.
Language : Java.
IDE : NetBeans 6.9.1
Data Base : MySql

4.3.7 System Specification

Java

Java is an Object Oriented programming language which was originally developed by James Gosling and his teammates at Sun Microsystems (a subordinate of Oracle Corporation Pvt. Ltd) and released Java in 1995 as a core component of Java Software from Sun Microsystems' Java platform. The language derives most its syntax from C and C++ and also it has a simpler object model with low-level facilities in fewer. Java applications are normally assemble to byte code (class file) that can be used to run on any platform for Java Virtual Machine (JVM) which were regardless of its computer architecture and platform it has. Java is a class-based, object-oriented language, concurrent, general-purpose language which is specifically designed to have as little execution dependency as feasible. It is intended to let interface application developers to raise "write once, and can run anywhere". Java is at present one of the majority of popular Object Oriented Programming languages in use, particularly for the use of client-server web applications.

Java Platform

One characteristic of the Java is portability, which means the computer programs written in Java language should run similarly on any of the Hardware or in its specific Operating System Platform. This is attained by compiling Java programming language code to an intermediate language representation called Java byte code. These Java byte code instructions are highly optimized set of instruction which are analogous to machine
code and are intended to be interpreted by a virtual machine (VM) written purposely for
the host hardware System. End-users usually use a Java Runtime Environment (JRE)
which will be installed on their independent machine for standalone Java application, or
in a Web browser for Java applet. Standardized libraries have provided a way to access
host-specific graphics, networking and threading features.

**Java a High-level Programming Language**

A high-level Object Oriented programming language was developed by Sun
Microsystems. Java was at first called OAK language which was also named in an edible
oil corporation, and initially designed for handheld devices and also for set-top boxes.
Oak was unsuccessful so that in 1995 Sun Microsystems changed the name from OAK
to Java and modified the programming language to take advantage of burgeoning World
Wide Web.

**Net Beans and J2EE**

The Net Beans Platform is a reusable Integrated Development Environment
framework to simplify the programming development of Java Swing desktop
application. The Net Beans IDE provides bundle for Java SE and all its packages which
contains files and organizes what is needed to start to develop Net Beans plug-in and
also to its Net Beans Platform based applications. Here, no additional SDK is required in
this software.

**WAMP Server**

WAMPs are packages of individually created series of code which were installed
on computers that may use a Microsoft Windows operating system platform. WAMP is
an acronym formed from the initial of the Microsoft Windows operating system and the
principal component of this package: Windows, Apache, MySQL and one of PHP or
Perl or Python.
Apache is a web server which is renowned as a Tomcat web server for freeware. MySQL is an open-source database which has given a contribution to all other open source software. PHP is a scripting language which is used to manipulate information held in a database and can also generate web pages dynamically each time when it is requested by a browser window. Other programs may also be included in this package, such as phpMyAdmin which provide a Graphical User Interface for MySQL database manager connectivity, or the alternative scripting languages such as Python or Perl. Equivalent packages are LAMP (for the Linux operating system) and MAMP (for the Apple Mac).

MySQL

The MySQL development project made source code obtainable under the terms of the GNU General Public License which is a freeware, as well as under a selection of proprietary software agreements. MySQL have possession of and sponsored by a single organization for-profit firm, the Swedish company called MySQL AB, now again obtained by Oracle Corporation.

Free software or open source projects that require the features of database management system which uses MySQL. For commercial use, several paid editions are available and also an offer for additional functionality in its sequence.

4.4 SYSTEM IMPLEMENTATION

4.4.1 System Modules

- Suspicious URLs Detection System
- Social Network account Creation and Posting Messages
- Short Text Classifier
- Content Based Filtering
Module Description

Suspicious URLs Detection System

Detection is the mining of particular information from a bigger flow of data without precise support from or synchronization with the dispatcher. The term "detector" was first used for a device that detects the presence or absence of a simple radio communication signals. Duplication detector locates passages in which the text on the two pages is the same. The detection system cannot notice suspicious URLs with active substance. All of these discovery systems may still not make the grade to notice doubtful sites with restricted behaviors. Conventional doubtful URL discovery systems are unsuccessful in their defense against restricted redirection servers that differentiate investigators starting from normal browsers and forward them to gentle pages to cover malicious land pages. Attackers can construct the features of their assault to dodge our recognition system. This online report of ALERT SYSTEM returns doubtful URLs that have come into sight in the previous hour near actual time detection. It implies that attackers had changed the characteristics of their accounts to avoid detection.

Twitter and Facebook spam account detection system label the collected data sets; one can argue that it just mimics the Twitter’s and Facebook detection system at most. The detection system had a time delay for suspicious account detection. The status information of accounts is checked for at least one month later from their posting of tweets. A suspicious URL detection system for Twitter and Facebook that is vigorous enough to defend against restricted redirections. URL discovery system for Twitter which is based on the association of URL redirect chains, which are hard to manufacture. The scheme that can find correlated URL redirect chains using the commonly shared URLs to determine their suspiciousness in almost real time.
Social Network account Creation and Posting Messages

- Interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks.

- The range of appliance methods in work builds on the same values as those for data mining.

- An Information filtering scheme is a system that remove surplus or unnecessary information from a sequence stream using automatic or computerized methods prior to the arrangement of a human user.

- This social network perspective provide a set of method for analyzing the construction of whole common entities as well as a range of theories explanation to the pattern observed in these arrangement.

- Social set-up and the study of them is a naturally interdisciplinary intellectual field which emerges from social psychology.

- One of the main paradigms in modern sociology is social set-up analysis. It is also working with a number of other social and official sciences.

- The term is used to illustrate a social arrangement determined by such relations.

- The social network approach in considerate social communication is that social phenomenon should be mainly conceive and investigate through the properties of associations between and within these units, in its place the properties of the units within themselves.
Short Text Classifier

- The major effort in building a robust Short Text Classifier (STC) is concentrated in the extraction and selection of a set of characterizing and discriminated features.
- The text classification may be classified according to their subjects or according to other attributes.
- At designing and evaluating various representation techniques are combined with a neural knowledge plan to semantically classify short texts.
- A list of grades is then used by the subsequent phases of the filtering process.

Content Based Filtering

- The content of each entry is represented as a set of terms or descriptors, naturally the words that happen in a document.
- Same terms are used to represent the user profile and they are built up by analyze the contented of matter which have been seen by the client.
- The terms are assigned routinely a technique has to be selected that can mine these terms from objects.
- The terms have to be represented such that both the user outline and the objects can be comparing in an important way.
- The content of each entry is represented as a set of expression or descriptor, typically the expressions that arise in any document.
- The user outline is represented with the same vocabulary and built up by analyze the contented of items which have been seen by the client.
- Several issues have to be measured carefully when implement a content-based filter system.
- Genetic Algorithms and Neural networks are usually much slower compared to other knowledge methods as several iterations are desirable to decide whether or
not an article is related.

➢ The ability of a knowledge method is to adapt to the changes in the user’s preferences also plays an important role in content based filtering.

4.5 RESULT AND DISCUSSION

4.5.1 Algorithm used to find out suspicious URLs and its related data

Step 1:

➢ Initially before initializing variables we have to store some suspicious URLs, normal URLs, spam data and normal data in database using Wamp server.

Step 2:

➢ In twitter, suspicious URLs are classified using Enhanced Offline Supervised Algorithm

1. Get the input from user
2. Compare with database
3. Provide output to user

➢ In Facebook, URLs and its related spam data are classified using two techniques

1. Short text Classify-Used to expand short text
2. Content based filtering-Used to filter spam data

Step 3:

➢ In twitter, after enabling all task time has to be set to run a particular task

1. Follow amount per time.
2. Interval time between 2 follow.
3. Maximum follows per day.

➢ In case of facebook the following terms are calculated

1. No of variables in posted message
2. Calculate TF, DF, IDF, TFIDF value in posted message

Step 4:

➢ In twitter, after setting run time by using Enhanced Offline Supervised Algorithm suspicious URLs can be easily classified.

➢ Whereas, in the case of Facebook messages it has to be filtered using content based filtering technique.

Step 5:

➢ After filtering suspicious URLs and its related spam data, particular message can be posted or unwanted message can be removed.

4.5.2. Results and Discussions

Classifying Suspicious URLs in Twitter Stream

Figures 4.3, 4.4 and 4.5 depict the twitter account status, the numbers of suspicious URLs found, normal URLs that are created based on the data stored in database and efficient classification of the suspicious URLs from normal URLs using Enhanced Supervised Learning Algorithm. Figures 4.3, 4.4 and 4.5 represents only twitter account status and Suspicious URLs in the created account.

Fig.4.3 Twitter Login
Fig. 4.4 Posting URLs in Twitter

Fig. 4.5 Classify URLs
Classifying Suspicious URLs and its spam data in Facebook (Secure Messenger)

Figures 4.6, 4.7, 4.8, 4.9, 4.10, 4.11 and 4.12 depict the Facebook account status and find out the number of spam data and normal data in that created account based on data stored in database and efficiently classifying the spam data from normal data. Figures 4.6, 4.7, 4.8, 4.9, 4.10, 4.11 and 4.12 represents the Facebook account status, their spam data in created account and also blacklisting the account having spam data. After blacklisting the spam data it enables to post the messages without any spam by separately classifying spam data using Content based filtering technique.

Fig 4.6 Secure Messenger Login
Fig. 4.7 Secure Messenger Account Status

Fig. 4.8 Application Tool Running
Fig 4.9 Posting Messages

Fig.4.10 Spam Detected
Fig 4.11 Blacklisting

Fig 4.12 Without Spam we can Post Message
4.5.3 Comparison Results

Figure 4.13 depicts the twitter and Facebook (Secure Messenger) account status and the number of suspicious messages are found. In the first phase, the comparisons are done based on the posted message and the application tool, enables to calculate the normal words in the particular posted message. In the second phase, the application tool calculates the normal words along with suspicious words based on the posted message.

Fig 4.13 Comparison between phase 1 and phase2 based on number of normal message and spam message post
Figure 4.14 depict the counting rate in twitter account status having normal URLs and the suspicious URLs which are used for calculating the total count of suspicious URLs and normal URLs in a particular twitter account. By using Enhanced Supervised Offline algorithm it compares with database and calculates suspicious URLs. The account having suspicious URLs and normal URLs are counted based on the above values.

![Fig 4.14 Classifying Normal URLS and Suspicious URL s](image)

Figure 4.15 explains about calculating the number of words in the particular posted message and also calculates or counts the number of variables present in the given posted message in Facebook (Secure Messenger), these values are used to calculate the spam data and also blacklist the suspicious data.

![Fig 4.15 Calculating the total number of variables in posted message](image)
Figure 4.16 calculates the number of words in the particular posted message and also calculates or counts the number of variables present in the given posted message in Facebook (Secure Messenger). These values are used to calculate the spam data and blacklist the suspicious data. It is also used to calculate the total number of words at the time of calculating TF, DF and IDF values and also classify suspicious data.

Fig 4.16 Calculating TF, DF, IDF values that is used to calculate spam data based on posted message

Figure 4.17 calculates the number of words in the particular posted message and also counts the number of variables present in the given posted message in Facebook (Secure Messenger). These values are used to calculate the spam data and blacklist the suspicious data. It is also used to calculate the total number of words at the time of calculating TF, DF and IDF values and also classify suspicious data.
Fig 4.17 Calculating TF, DF, IDF, TFIDF values that is used to classify spam data based on posed message.

Fig 4.18 Blacklisting spam data based on TF, DF, IDF, TFIDF values that is used to classify spam data based on posted message.
The above Figure 4.18 denotes the number of spam and normal data, displaying the blacklist details in created account placed in Facebook. It mainly displays spam and normal data in created account that is to be stored in the database. By comparing dataset, it will classify normal data from spam data.

4.6 SUMMARY AND CONCLUSION

Conventional suspicious URL and spam detection systems are not effective due to their security against restricted redirection servers which differentiate normal browsers from investigators and to benign pages to cloak malevolent pages it redirects. Unlike the conservative system, ALERT SYSTEM is robust when protecting against conditional redirection and spam data, because the features do not rely on the malicious landing pages with its spam data. The evaluation results show that the proposed system is deployed as a near real-time system and also as a highly accurate system to classify large samples in tweets from the Twitter and Facebook public timeline.

In the future, the proposed system can be extended to address dynamic and multiple redirections. A distributed version of ALERT SYSTEM is also implemented to process all tweets or messages from the Twitter and Facebook public timeline. Future plans can contemplate a deeper investigation in particular on two mutually dependent tasks. The first concerns are the extraction or collection of related features that has shown to have a high discriminative power with its features. The next task which involves the learning phase in distributed environment.