Implementation on Social Networking Malicious Activities and Prevention Techniques

Palash Pramod Patil[1], Ajinkya Santosh Patil[2], Sanket Narayan Mane[3], Shailesh Marutirao Rathod[4]
[1, 2, 3, 4] Department of Computer Engineering
[1, 2, 3, 4] NBN Sinhgad School Of Engineering, Pune

Abstract- *With the extending use of social networking site, there are increases in the malicious and fake application as well as URLs. Approximately in world daily more than 15 million new users are register on social networking site. As social networking helps to communicated people to each other by sitting at any location of the world, use of this technology is increasing very quickly. Disastrously, hackers have comprehended the ability of using applications for spreading malware and spam. Besides, days this issue is more essential, as our survey find that no fewer than 13% of utilizations in our dataset are vindictive. In this paper, we took the audit of some social networking sites correspondence regions and application and malignant activity relates to it. Similarly we indicate the unmistakable systems or methods to control dangerous activities for different social networking sites Twitter, Facebook.*

Keywords- Facebook Apps, Malicious Apps, Profiling Apps, Online Social Networks, Social Network Security, Spam profiles.

I. INTRODUCTION

Almost 90% of the people in the world are using social networking site for different reasons daily. A latest new related to Facebook said that in world there are only two types of people are present now one which have Facebook account and rest all people don't have internet facility available so they are not having Facebook account. On basis of this we can image how the uses of social networking sites are increased now a day. Also this is not case about Facebook only other sites like Twitter, LinkedIn or application like Whatapp have the similar condition. And because of increase in use of social networking sites there is increase in malicious links or application on network, which helps hacker to retrieve user data and using that data fraud are happen.

Hackers utilize numerous sorts of malware and extortion, all of which uses HTTP or HTTPS conventions, yet might likewise utilize different conventions and parts, for example, joins in email or IM, or malware connections or on servers that get to the Web. They advantage cybercriminals by taking data for resulting deal and retain contaminated PCs into botnets. Malicious application represent an expansive scope of dangers, including budgetary harms, wholesale fraud, loss of private data/information, burglary of system assets, harmed brand/individual notoriety, and disintegration of purchaser trust in e-business and web managing an account.

The online Social networking communication sites like Facebook, twitter, MySpace and so on are utilized by a great many individuals to speak with one another however they're such a great amount of far from each other. Numerous papers have been distributed on the recognition of spam profiles or malicious application on social networking sites. However, so far not very much survey paper has been distributed in this field which united the ebb and flow research. Our paper expects to give an audit of the scholastic research and work done in this field by different scientists and highlight the future exploration course.

II. PREVIOUS WORK DONE

1] Firefox add-ons for Facebook Application: In paper [1] they specified Facebook applications are a reason for Facebook engaging quality. As, various users don't know about the way that numerous malicious Facebook applications exist. To instruct users, to raise user's mindfulness and to enhance Facebook user's security and protection, they built up a Firefox add-on that alarms users to the quantity of introduced applications on their Facebook profiles. In this study, they exhibit the transient investigation of the Facebook applications establishment and evacuation dataset gathered by their extra. This dataset comprises of data from 2,945 clients, gathered amid a time of over a year. They utilized straight relapse to examine their dataset and found the direct association between the normal rate change of recently introduced Facebook applications and the quantity of days went subsequent to the user at first introduced their extra.

2] Twitter Spam detector using Slanting points method: In paper [2] they concentrate on another application called Twitter. Twitter spam location is a late territory of examination in which most past works had concentrated on the distinguishing proof of pernicious client records and honeypot-based methodologies. Be that as it may, in

this paper they display a procedure in view of two new angles: the recognition of spam tweets in separation and without past data of the client; and the use of a measurable investigation of dialect to recognize spam in slanting subjects. Slanting points catch the developing Internet patterns and subjects of examination that are in everyone's lips. They initially gathered and named a huge dataset with 34 K slanting points and 20 million tweets. At that point, they have proposed a lessened arrangement of elements scarcely controlled by spammers. Also, they have built up a machine learning framework with some orthogonal components that can be joined with different arrangements of elements with the point of breaking down new attributes of spam in informal organizations. They have additionally led a broad assessment prepare that has permitted us to demonstrate how our framework has the capacity get a F-measure at the same level as the best cutting edge frameworks taking into account the identification of spam records. In this way, There framework can be connected to Twitter spam identification in inclining subjects continuously because of the examination of tweets rather than client accounts.

3] Detection of Suspicious URLs using WARNING BIRD APPLICATION : In [4] paper they took overview of recognition of suspicious URL on long range interpersonal communication locales. Long range interpersonal communication use to speak with one another over the long separation. In any case, it additionally draws in the aggressors in completing diverse assaults or get the data being shared by the long range interpersonal communication destinations users. Person to person communication locales users can send the messages to one another as content, that messages have the size confinement of most extreme 140 characters. So to share the site pages URL shorting is utilized. Aggressors send the suspicious URLs in writings and move the clients to pernicious pages. This paper exhibits a review of distinctive techniques used to distinguish the suspicious URL (locales) in twitter stream. This paper likewise introduces a WARNING BIRD APPLICATION. It is a close constant framework to recognize the suspicious URLs by characterizing them. This framework explores connections of URL send chains separated from numerous tweets. As a consequence of assailants have predetermined number of assets and aggressors utilizes them over and over, this framework gathers different tweets from the Twitter open course of events and construct a connected math classifier exploitation them. Investigation results demonstrate that this classifier precisely and quickly recognizes suspicious URLs. This WARNINGBIRD framework is a close ongoing framework for grouping suspicious URLs inside of the Twitter stream.

4] Detection of Malicious Application on Facebook using - FRAppE

In [5] this is the fundamental paper on which we going to center. We are making so as to execute this technique some upgrade in the framework. Their key commitment is in creating FRAppE—Facebook's Rigorous Application Evaluator—ostensibly the first apparatus concentrated on identifying noxious applications on Facebook. To create FRAppE, they utilize data accumulated by watching the posting conduct of 111K Facebook applications seen crosswise over 2.2 million users on Facebook. In the first place, they recognize an arrangement of elements that offer us some assistance with distinguishing pernicious applications from considerate ones. For instance, they find that malignant applications frequently impart names to different applications, and they regularly ask for less consent than favourable applications. Second, utilizing these recognizing elements, they demonstrate that FRAppE can distinguish noxious applications with 99.5% exactness, with no false positives and a low false negative rate (4.1%). At long last, they investigate the biological community of noxious Facebook applications and distinguish systems that these applications use to spread.

III. SYSTEM RESULTS

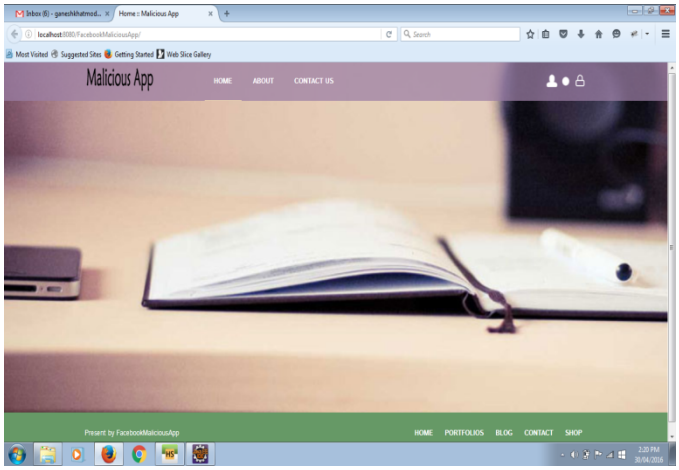

Fig 3.1 Home Page

In above figure it shows the home page of our system. It contains login option, information about application and other general things.

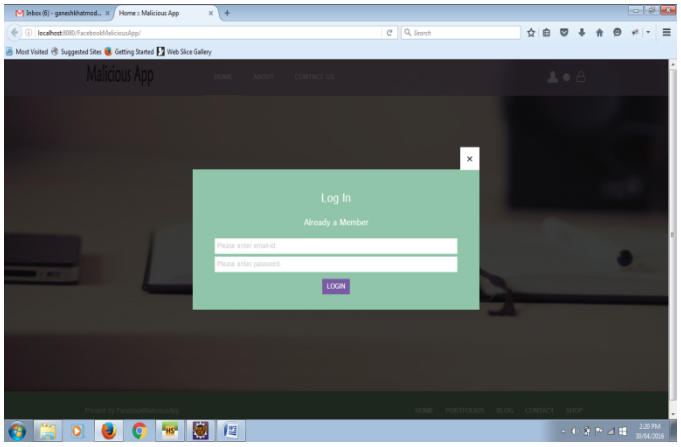

Fig 3.2 Login Screen

As shown in above screenshot it will be the login screen.

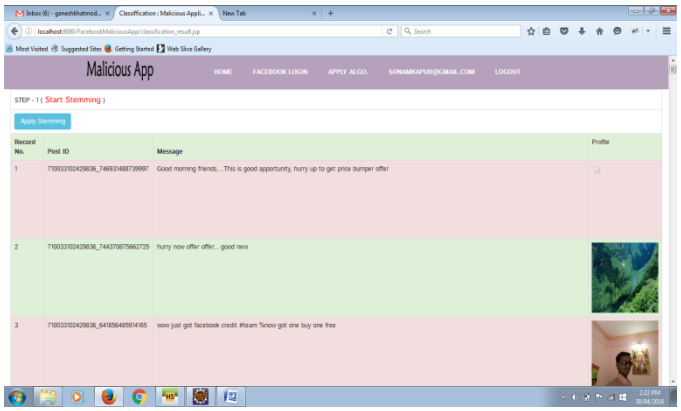

Fig 3.3 First option- start Streaming

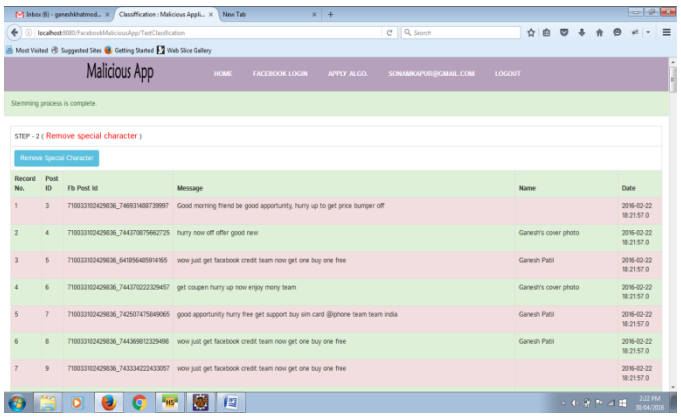

Fig 3.4 Step 2- Remove Special Characters

As shown in above screenshot in step 2 the system will remove the special character and then remove the stop words.

After this system will apply the Cosign-Similarity Algorithm and Display malicious application.

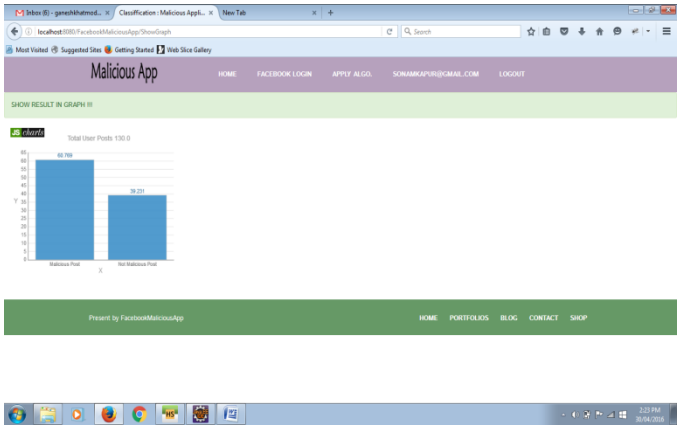

Fig 3.5 Final output

Above fig shows the graphical output.

IV. CONCLUSION

Social networking sites and associated technologies can bring significant benefits to the business as well as to people, but as the use of these technologies grows, it will become difficult for organizations to tightly control all of the many forms of activities related to it. Many problems related to these can be control by some of the technique and we summarize these recent techniques to control malicious activities. Also we have implemented our system on the basis of proposed architecture and our survey.

REFERENCES

[1] Facebook Applications Installation and Removal: A Temporal Analysis, Dima Kagan, Michael Fire, Aviad Elyashar, and Yuval Elovici Telekom Innovation Laboratories and Information Systems Engineering Department, Ben-Gurion University of the Negev, Beer-Sheva, Israel Email: fkagandi,mickyfi,aviade, elovicig@bgu.ac.il.

[2] Detecting malicious tweets in trending topics using a statistical analysis of language,Juan Martinez-Romo ⇑, Lourdes Araujo,NLP & IR Group, Dpto. Lenguajes y Sistemas Informáticos, Universidad Nacional de Educación a Distancia (UNED), Madrid 28040, Spain.

[3] Techniques to Detect Spammers in Twitter- A Survey,Monika Verma, Divya,Sanjeev Sofat, Ph.D Professor Department of Computer Science PEC University of Technology.

[4] Detection of Suspicious URL in Social Networking Site Twitter: Survey Paper Jyoti D.Halwar, Sandeep Kadam , Vrushali Desale, D.Y.Patil College Of Engg.

[5] FRAppE: Detecting Malicious Facebook Applications Md Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos Dept. of Computer Science, University of California, Riverside Riverside, CA 92507 rahmanm, huangt, harsha, michalis@cs.ucr.edu

[6] S. Lee and J. Kim, "WarningBird: Detecting suspicious URLs in Twitter stream," in Proc. NDSS, 2012.

[7] Antoniades, I. Polakis, G. Kontaxis, E. Athanasopoulos, S. Ioannidis, E. P. Markatos, and T. Karagiannis, "we.b: The web of short URLs," in Proc. WWW, 2011.

[8] Klien and M. Strohmaier, "Short links under attack: geographical analysis of spam in a URL shortener network," in Proc. ACM HT, 2012.

[9] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbotnetwork: when bots socialize for fame and money," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM,2011, pp. 93–102.

[10] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM transactions on Intelligent Systems and Technology, 2, 2011.

[11] P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals. In WWW, 2012.

[12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 2012.