iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10091

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Vale: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Review on Detecting OSN Malicious Account and Fake Reviews in Online Promotions

Prof. A. R.Gaidhani[1], Sagar Khaire[2], Rushikesh Shirsat[3], Shree kumar Sabu[4], Kiran Chaudhari[5]
[1,2,3,4,5] *Department of Computer Engineering, Sandip Institute of Engineering and Management*

***Abstract**: In today's world, everyone has become associated with the online social networks, it has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Facebook, Myspace, or Twitter), this OSN platforms earn evenue from aid's and Online promotion activities.*
The E-Commerce platforms plan various kinds of online promotions through social networking platforms where people participate in those promotions, as these online promotions do offer some reward points/virtual money to achieve more publicity. If the user buy any product from this online promotions they can be rewarded with some reward points as per that product offers. For normal users this process is fine. But most of the time attackers plan various fake malicious accounts in social networking platforms. This accounts participates in online promotions and steal reward points/virtual money.
In this project we came up with a system that detect fake malicious accounts by different behavior and classification techniques like Decision trees to classify the profiles into fake or genuine classes. The project also focuses on detecting fake product reviews in online E-Commerce platform.
***Keywords**: E-Commerce, Malicious, virtual money, social networking Accounts, facebook, reward point.*

I. INTRODUCTION

Today E-Commerce world get most of its business from online promotion events which occurs on various Online Social Networking sites. Most of the time online promotion events offers reward points (virtual currency) as result it attract more customers from various OSN sites as it's good for business. Eventually there are attackers, who plans various malicious accounts on OSN sites, such accounts participates in online promotion events and steal reward points (virtual currency). The fake Product reviews in E-Commerce site can manipulate customer's decision on that product.

II. LITERATURE REVIEW

Manuel Egele, et. all [1] :- In this paper, a system is presented to detect compromised user accounts in social networks. And it is applied on two popular social networking platforms, Twitter and Facebook. In this paper they uses two approach first one is composition of statistical modeling and second one is anomaly detection to identify accounts that experience a sudden change in behavior. They developed a tool, called COMPA, They run that on large-scale dataset of more than 1.4 billion publicly-available Twitter messages, as well as on a dataset of 106 million Facebook messages. COMPA was able to identify compromised accounts on both social networks with precision. Detecting Malicious Posts in Social Networks Using Text Analysis. Neeraja M, et. all [2] :- In this paper work they have develop a detection mechanism to distinguish between malicious and genuine posts within seconds after the posts are up- loaded by user. This work proposes an extensive keyword set based on the textual content and URL features to identify malicious content on Facebook at zero time. The intent is to catch malicious or vulgar content that is currently evading Facebook's detection mechanisms. Gianluca Stringhini, et.all [3] :- In this paper, they analyze how spammers who target social networking sites operate. To collect the data about spamming activity, They created a large and diverse set of "honey-profiles" on three large social networking sites, and logged the kind of contacts and messages that they received. Then analyzed the collected data and identified anomalous behavior of users who contacted the profiles. Based on the analysis of this behavior, They developed techniques to detect spammers in social networks, and they aggregated their messages in large spam campaigns. There results show that it is possible to automatically identify the accounts used by spammers, and there analysis was used for take-down efforts in a real-world social network. More precisely, during this study, They have collaborated with Twitter and correctly detected and deleted 15,857 spam profil Meng Jiang, et.all [4] :- In this paper a multimillion-node network of who-follows-whom like Twitter, since a high count of followers leads to higher profits, users have the incentive to boost their in-degree. Here one question arise Can we spot the suspicious following behavior, which may indicate zombie followers and suspicious followers? To answer the above question, They propose Catch-Sync, which exploits two tell-tale signs of the suspicious behaviour : Synchronized behavior and Abnormal behavior. Gianluca Stringhinix, et.all [5] :- Here they present, a system name EVILCOHORT that detects online ac-

counts that are accessed by a common set of infected machines. There sys- tem only needs the mapping between an online account and an IP address to operate, and can therefore detect malicious accounts on any online regard- less of the type of malicious activity that these accounts perform. Here the system can identify malicious accounts that are controlled by botnets but do not post any malicious content (e.g., spam) on the service. They have evaluated ”EVILCOHORT” on multiple online services of different types (a webmail service and four online social networks), and show that it accurately identifies malicious accounts.

R. Nithin Reddy, et.all [6] :- In this project consist a framework which automatic detects fake profiles. This framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify The profiles into fake or genuine classes. As, this is an automatic detection method, It can be applied easily by online social networks which has millions of people whose profiles cannot be examined manually.

Pete Burnap, et.all [7] :- In this paper they have develop a machine classification system that distinguish between Malicious and benign URLs within seconds of the URL being clicked. They have train the classifier using machine activity logs created while interacting with URLs extracted from Twitter data collected from large sporting event and test it using data collect from another large sporting event the Cricket World Cup. There results show that machine activity logs produce precision performances of up to 0.975 on training data from the first event and 0.747 on a test data from a second event.

Girisha Khurana, et.all [8] :- In this paper they have reviewed the existing techniques for detecting spam users in Twitter social network. Features for the detection of spammers could be user based or content based or both and spam classifier methods. They used classification approaches like SVM, Decision Tree, Naive Bayesian, and Random Forest, KNN. Detection that has been done on the basis of user based features or content based features or a combination or on both.

Junxian Huang, et.all [9] :- In this paper, They have present a framework, SocialWatch, to detect attacker- created accounts and hijacked accounts for online services at a large scale. The framework explores a set of social graph properties that effectively model the overall social activity and connectivity patterns of online users, including degree, PageRank, and social affinity features. They have using a large, real dataset with more than 682 million users and over 5.75 billion directional relationships.

Binghui Wang, et.all [10] :- In this paper a system is proposed SybilSCAR, It is a new structure based method to perform Sybil detection in OSNs. There proposed framework unify RW-based and LBP-based methods. They have certain methods which can be viewed as iteratively applying a different local rule to every user, which propagates label information among a social graph. They also have compare there system with a state of threat RW-based method and a state-of-the-art LBP-based method, using both synthetic Sybils and large-scale social network datasets with real Sybils.

III. SYSTEM ARCHITECTURE

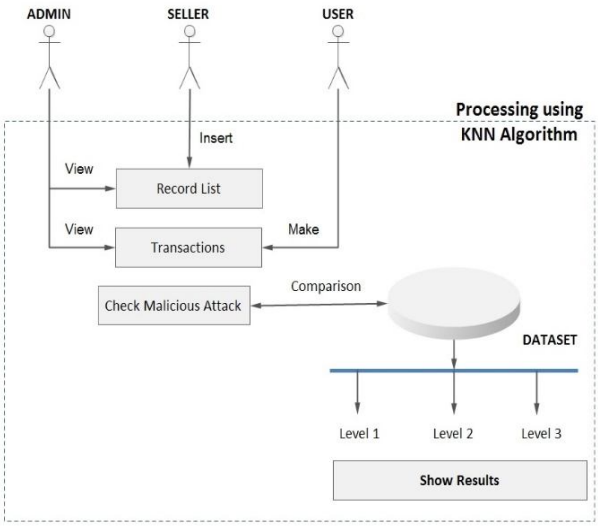


Fig. 1 System Architecture

The above diagram illustrates the system architecture. The architecture consists of one data set and by performing different activities on in and result is generated.

IV. MATHEMATICAL MODEL

Mathematical modeling is used for measurement of how the system is implemented mathematically. It provides flexible i.e. mathematical thinking and use of concepts of set theory.

Let,

S= {A,U,F,R}

Where,

S = System

A = Admin

U = {u1,u2,u3,u4,.....,un } set of users

F = {f1,f2 } is set of Algorithms

f1 = Algorithm 1

f2 = Algorithm 2

R = {r0,r1,r2,r3....rn } is set of results

Activities

fa(A) → (R) Here admin can examine the result.

fa(A) →(U) Here admin can manage the user.

fn(F) → (R) Algorithm for displaying result.

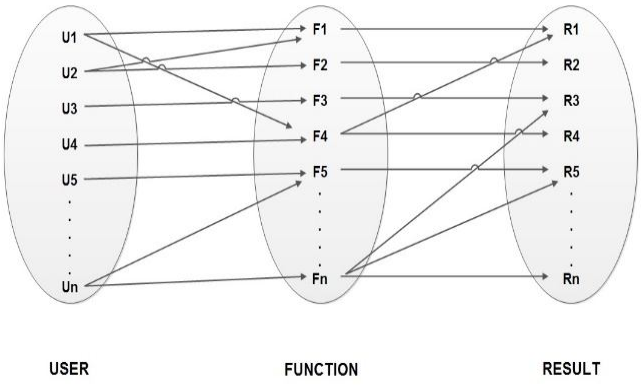


Fig.2 Mathematical Model

V. FUTURE WORK

In order to maintain the robustness of the system, we can implement J48 algorithm for classification. This algorithm helps to classify attacks or attributes which helps in finding the results more efficiently.

VI. CONCLUSIONS

The presented system automatically detect malicious OSN accounts that participate in online promotion events. The system also prevent manipulating customer's decision on E-Commerce product by detecting fake product reviews. The proposed system is in beta state there are future expansions in this system.

REFERENCES

[1] Manuel Egele, Gianluca Stringhini, Christopher Kruegel , "COMPA Detecting Compromised Accounts on Social Networks" NDSS Symposium 2013, Carnegie Mellon University, Pittsburgh, PA

[2] Neeraja M, John Prakash, "Detecting Malicious Posts in Social Networks Using Text Analysis", Journal of Theoretical & Applied Information Technology . 3/31/2015, Vol. 73 Issue 3, p405-410. 6p.

[3] Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna, "Detecting Spammers on Social Networks" ACSAC'10 Proceedings of the 26th Annual Computer Security Applications Conference. Pp 1-9 .

[4] Meng Jiang,Peng Cui,Alex Beutel, "Detecting Suspicious Following Behavior in Multimillion-Node Social Networks" Proceedings of the 23rd International Conference on World Wide Web. Pp 305-306

[5] Gianluca Stringhinix, Pierre Mourlanne, Gregoire Jacobz, Manuel Egeley, "EVILCOHORT: Detecting Communities of Malicious Accounts on Online Services" USENIX Security Symposium 2015

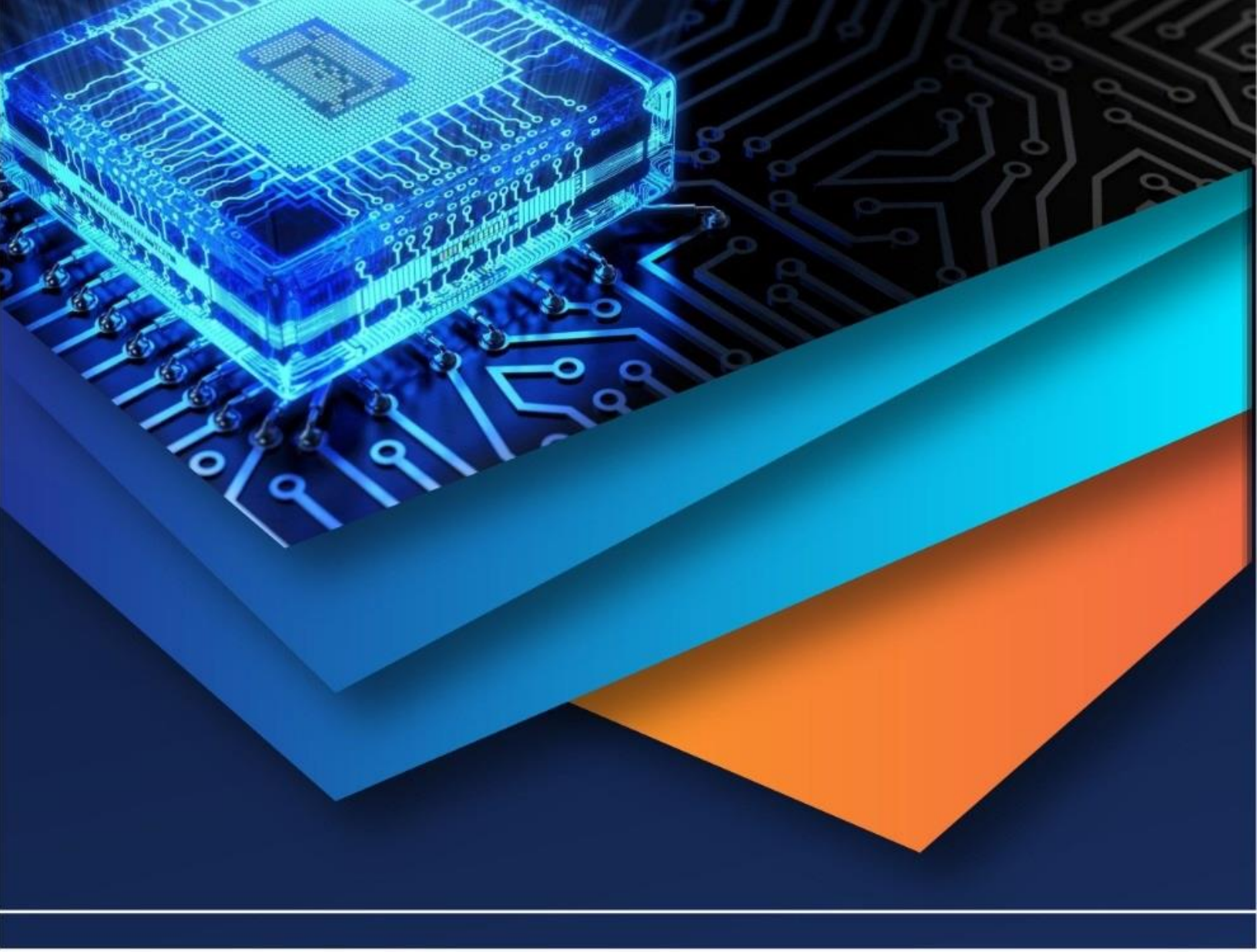
[6] R. Nithin Reddy Nitesh Kumar, "Automatic Detection of Fake Profiles in Online Social Networks " ASONAM '12 Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012). Pp 1071-1078

[7] Pete Burnap, Amir Javed, Omer F. Rana, Malik S. Awan, "Real-time Classification of Malicious URLs on Twitter using Ma- chine Activity Data" ASONAM '15 Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015. Pp 970-977

[8] Girisha Khurana, Mr Marish Kumar, "Review: Efficient Spam Detection on Social Network" ASONAM '15 Proceedings of the 2015 IEEE/ACM International Conference.

[9] Junxian Huang, Yinglian Xie, Fang Yu, Qifa Ke, Mart´ın Abadi, "SocialWatch: Detection of Online Service Abuse via Large-Scale Social Graphs" 8th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)

[10] Binghui Wang, Le Zhang, Neil Zhenqiang Gong, "SybilSCAR: Sybil Detection in Online Social Networks via Local Rule based Propagation" ACM Transaction On Intelligent System and Technology (TIST) archieve , Volume 8 Issue 6 , August 2017



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY