ISSN 2347 - 3983
Volume 8. No. 4, April 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter62842020.pdf
https://doi.org/10.30534/ijeter/2020/62842020

Pro Guard Malicious Social Network Account Based Online Promotions

K. Ruth Ramya[1], B. Manjula Josephine [2], P. Vara Prasad [3], B.Manikanta[4], P.S.S. Rithvik[5], T.Sri Surya[6]
[1,2,3,4,5,6] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India. ramya_cse@kluniversity.in, manjulajosephine@gmail.com,
varaprasad@kluniversity.in

ABSTRACT

The Online social networks (OSNs) gradually integrate financial capabilities by enabling the usage of real and virtual currency. They serve as new platforms to host a variety of business activities, such as online promotion events, where users can possibly get virtual currency as rewards by participating in such events. Both OSNs and business partners are significantly concerned when attackers instrument a set of accounts to collect virtual currency from these events, which make these events ineffective and result in significant financial loss. It becomes of great importance to proactively detecting these malicious accounts before the online promotion activities and subsequently decreases their priority to be rewarded. In this paper, we propose a novel system, namely ProGuard, to accomplish this objective by systematically integrating features that characterize accounts from three perspectives including their general behaviors, their recharging patterns, and the usage of their currency. We have performed extensive experiments based on data collected from the Tencent QQ, a global leading OSN with built-in financial management activities. Experimental results have demonstrated that our system can accomplish a high recognition rate of 96.57% at a very low false positive rate of 0.43%.

Key words : Malicious accounts, online social network, existing methods, advanced technology, blocking accounts

1. INTRODUCTION

Online interpersonal organizations (OSNs) that incorporate virtual money fill in as an engaging stage for different business exercises, where on the web, intelligent advancement is among the most dynamic ones. Exceptionally, a client, who is ordinarily spoken to by her OSN account, can get compensate as virtual money by taking an interest online advancement exercises composed by business substances. She would then be able to utilize such reward in various ways, for example, web based shopping, moving it to other people, and in any event, trading it for genuine money. Such virtual-money empowered online advancement model empowers tremendous outreach, offers direct nancial upgrades to end clients, and then limits the associations between business substances and nancial establishments. Thus, this model has indicated extraordinary guarantee and increased tremendous predominance quickly. In any case, it faces a significant danger: aggressors can control an enormous number of records, either by enrolling new records or bargaining existing records, to partake in the online advancement occasions for virtual cash. Such noxious exercises will on a very basic level undermine the viability of the advancement exercises, quickly voiding the viableness of the advancement speculation from business substances and in the interim harming ONSs' notoriety. Additionally, a huge volume of virtual money, when constrained by assailants, could likewise turn into a potential test against virtual cash guideline. It consequently happens to basic significance to distinguish accounts constrained by aggressors in online advancement exercises. In the accompanying dialogs, we allude to such records as malignant records. The successful acknowledgment of noxious accounts empowers both OSNs and business substances to take moderation activities, for example, prohibiting these records or diminishing the likelihood to compensate these records. Be that as it may, structuring a viable acknowledgment strategy is looked with a couple Significant 1990. Online Promotions challenges. In the first place, assailants don't have to create noxious substance (e.g., phishing URLs and vindictive executables) to dispatch effective assaults. Similarly, assailants can effectively perform assaults by just clicking connections offered by business elements or sharing the generous substance that is originally appropriated by colleagues. These activities themselves don't noticeably separate from kindhearted records. Second, effective assaults don't have to rely upon social structures (e.g., "following" or "companion" relationship in popular informal organizations). To be more special, keeping up dynamic social structures doesn't bennet to aggressors, which is fund rationally not the same as well-known assaults, for example, spammers[8] in online interpersonal organizations. These two difficulties make the detection of such noxious OSN accounts essentially not the same as the acknowledgment of conventional assaults, for example, spamming and phishing. As a result, it is incredibly difficult to embrace existing techniques to distinguish spamming and phishing accounts. So as to viably identify vindictive records in online advancement exercises by defeating the previously mentioned challenges, we have structured a novel framework, to be specific Proguard. Proguard employs an assortment of social highlights to prole a record that takes an interest in an online advancement occasion. These highlights expect to portray a record from three viewpoints including i) its general use profile, ii) how a record gathers virtual money, and iii) how the virtual cash is spent. Proguard further incorporates these highlights utilizing a measurable classier with the goal that they can be altogether used to segregate between 3 those records constrained by assistants and favorable ones. Apparently, this work speaks to the first exertion to methodically recognize malevolent records utilized for online advancement action participation.

2. RELATED WORK

M. Chau and H. Chen [2] portrays as the Web keeps making, it has wound up being powerfully hard to pursue down related data utilizing customary web records. Subject particular web records give an elective method to manage bolster giving to constrain data recovery on the Web more right and patch up looking in changed spaces. In any case, organizers of point particular web look instruments need to address two issues: how to find important documents (URLs) on the Web and how to channel through unessential reports from a blueprint of records gathered from the Web. This paper reports our examination in watching out for the second issue. We propose a machine-learning-based framework[19] that cements Web examination and Web structure examination

Purva et al. [12] presented that online social networking like Facebook and Twitter [13]have the fastest means of communication and having gained wide popularity, have revolutionized interpersonal communications by providing a platform to individuals for expressing themselves for a particular at a global level, beyond their immediate geography. The authors present the study on diffusion dynamics of specific real world events, discussed on Twitter, with respect to location and time. It’s The events were categorizing into broad categories based temporal (short or long), geographical distribution (local or global), information diffusion (viral or gradual),influence (popular or unpopular) and the cause (natural or planned). It was concluding that the three-dimensional analysis of real-world events by exploring relationships among them. The number of social networking [9]site users is increasing immensely not only in India but also across the globe.

Analyzed the factors for the online social networking [25]sites as per users behavior regarding user friends, the peer groups, access patterns, amount of time spend, the effect on personal and professional life. User attitude and behavior is also surveyed for over seven hundred users using a questionnaire consisting of 27 questions which focused on behavior of Indian users in terms of usability, trends and access.

Identifying unwanted content and the advertisers that may be spammers who can makes a lengthy dare that influences on a daily basis. Uninvited or wrong messages can be sent to a more number of persons and it is said to be a spam and also it will have used for a variety of usages and malware influences. Spam can be spread easily by advertising through televisions or else in paper and then spam calls has been a dangerous problem in modern communications with people. By using internet, the spammers reach the more number of people than previous measures. We can say that the old spam method is email spam. In a recent time, Online Social Networks has given the chance to spammers to expand their spam messages in an effective medium. By utilizing social networks, spammers can impersonate themselves as legal users and they can participate in interactions. Simply the spammers can use this platform to send the messages on famous sources or pages, and replying to legal comments by utilizing the spam content. Such variety of chances has often enlarges spammers capability to secret their purposes from conventional filtering in spam [5].

A propose a sentiment analysis method on the tweets in Cloud environment and utilized Hadoop for intelligent analysis and storage of big data on Facebook and Twitter[10]. The reason is that I.J. of Detecting Malicious Accounts[11] in Social-Network-Based Online Promotions Electronics and Information Engineering.

The presented the research effort in ensuring awareness about the social networking site concept, merits, demerits and meaning. The research methodology in this paper was based on primary and secondary data regards to grouping of users having similar type of interests, jobs, activities, backgrounds or some other type of real life similarities by Prateek Dewan [26] et al.

A focused on Big Data Management for Social Networking Sites by review and analysis of how Big Data is being managed for social networking sites by Facebook and Twitter[21]. The data size for social networking sites constitutes almost 105 terabytes of data for every thirty minute, which in itself is a huge chunk of the data, unlike other data sources which has structured, limited data to handle. Facebook uses Hive for storing the data[27] on HDFS (Hadoop Distributed File System) while Twitter has implemented a set of solutions storage inside Hadoop to store the data in LZO compressed format by Purti at al. [3]

The tested for affiliation that exists between Higher Education and Social Networking Site[22]. Mining algorithms provided by NASA tools like Like-Analyser, Gephi, Wolfram Alpha and Node XL to assess presence and participation factor of students and education professionals in social network graphs are utilized in this study and analysis finding related to social network analysis predicted that social networking on Face book in parallel units. n times of traditional print media, there used to be one- way information dissemination which was restricted to geographical limits and presence. The process of information diffusion with arrival of Internet transformed significantly by Mamta et al[15].

Our work aims to address a new problem caused by the new trend of integrating online social networks and [18] activities. Pro guard features new capability of fusing features from both networking and financial aspects for detection. Nevertheless, we believe our method and existing approaches can complement each other to improve the security of online social networks.

3. SYSTEM MODEL

Our objective is to design a detection system capable of identifying malicious accounts[14] that participate in online promotion events for virtual currency collection (at the collection phase) before rewards are committed. Detecting malicious accounts[16] at this specific time point (i.e., before the commitment of rewards and at the Figure 1. Virtual currency flow for malicious OSN accounts. collection phase) results in unique advantages. First, as a simple heuristic to prevent freshly registered accounts that are likely to be bots, business entities usually require the participating accounts to be registered for a certain amount of time (e.g., a few weeks). Therefore, the detected and mitigated malicious accounts cannot be immediately replaced by the newly registered accounts, thereby drastically limiting attackers' capabilities. In contrast, no constraint is applied for accounts used for virtual currency transferring and laundering. This implies such accounts can be easily replaced by attackers if detected, resulting negligible impact to attackers' capabilities. Second, our detection system will label whether an account is malicious when it participates in an online promotion event[3]; this enables business entities to make actionable decisions such as deprioritize this account from being rewarded in this event. Therefore, it can proactively mitigate the financial loss faced by business entities.

4. SYSTEM ARCHITECTURE

Figure 1 presents the temporal relationship among the data collection process, online promotion events, and the account labeling process. Therefore, It is worth noting that an account may not have any historical financial activities (even for virtual currency collection activities) since it participates in the online promotion for the first time. Figure 1.The architectural overview of the system Although the aforementioned ''trace-back'' method is effective in manually labeling malicious accounts, using it as a detection method is impractical. First, it requires a tremendous amount of manual efforts for forensic analysis such as identifying suspicious virtual-currency dealers in external e-commerce websites, correlating spamming content with user accounts[4], and correlating sellers' profiles with user accounts. In addition, evidence for such forensic analysis will be only available after malicious accounts participate in online promotion events. Therefore, this data labeling process[17], if used as detection method, cannot guide business entities to mitigate their financial loss proactively. In contrast, our method is designed to detect malicious accounts prior to the reward commitment. For each account, we collect a variety of information including 1) login activities, 2) a list of anonymized accounts that this account has sent instant messages to, 3) service purchase activities, 4) the recharging activities, and 5) the expenditure activities.

The bottom of Figure 1 presents the architectural overview of ProGuard. As a variety of statistical classifiers have been developed and widely used, designing features capable of discriminating between malicious accounts and benign accounts becomes of central focus. In this section, we will introduce various features and demonstrate their effectiveness on differentiating malicious accounts from benign ones. We propose three general guidelines to steer the feature design. General Behaviors: Benign accounts are

- usually used by regular users for variety of activities such as chatting, photo sharing, and financial activities. In contrast, malicious accounts are more likely to be driven by online promotion events. Therefore, the benign accounts tend to be more socially active compared to malicious accounts.

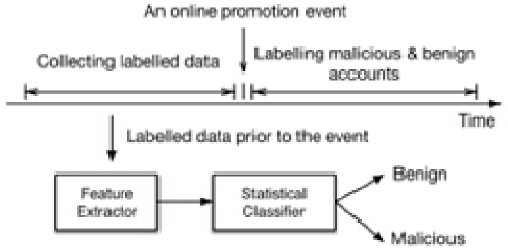

An online promotion event
Collecting labelled data
Labelling malicious & benign accounts
Time
Labelled data prior to the event
Feature Extractor
Statistical Classifier
Benign
Malicious

Figure 1: System Architecture

Currency Collection: The malicious accounts

- under investigation focus on using online promotion activities to collect virtual currency. In contrast, benign users are likely to obtain virtual currency from multiple resources.

Currency Usage: Attackers' ultimate objective

- is to monetize the virtual currency. In contrast, benign users use their virtual currency in much more diversified ways.

4.1 General-behavior features

Malicious accounts tend to be less active compared to benign accounts with respect to the non-financial usage. Attackers usually control their accounts to only participate in online promotion activities. In contrast, benign accounts are more likely to engage in active interaction with other users.

- Feature 1: The Ratio of Active Days. This feature represents the ratio of the number of active days of an account for the passed one year. pro guard: Detecting Malicious Accounts in Social-Network-Based Online Promotions logged in at least once for a day, this day will be labeled as ''active'' for this account.

Attackers usually login malicious accounts for participating in online promotion activities that involve virtual currency. Therefore, malicious accounts tend to be silent in the absence of online promotion activities. The availability of promotion activities is significantly influenced by timing and spatial factors. For example, promotion activities are intensive over holiday seasons, special dates, and regional events while occasionally available for other time periods. As a consequence, malicious accounts tend to be inactive generally. Comparatively, benign accounts are used by regular users and their logins are driven by the daily usage such as chatting and photo sharing. Many users configure their applications to automatically login upon the bootstrap of the underlying system (e.g., a smart phone), which further facilitates volatility of benign accounts.

- Feature 2: The Number of Friends. This feature summarizes the number of friends for each account. As a common feature for almost all online social networks, each OSN account has a list of friends. It usually implies a considerable amount of user-user interaction for one user to add another one as her friend. It is common for a benign user to maintain a relatively lengthy friend list for various social activities such as chatting and photo sharing. In contrast, an attacker usually lacks the motivation to maintain a friend list since it contributes little to promotion participation but costs significant efforts such as solving captcha challenges.
- Feature 3: The Number of Services Purchased By an Account. This feature represents the total number of types of upgraded membership that an account has paid for through all possible methods. It is a common feature in many online social networks that an user can upgrade his/her account by making a certain amount of payment through various ways such as credit card, wire transfer, and virtual currency.

4.2 Currency collection features

In addition to collecting virtual currency by participating in online promotion activities, an OSN user can recharge her account with virtual currency through various ways such as wire transfer, selling virtual goods, and transferring from other accounts. Generally, benign users should be more active with respect to recharging their accounts. We propose two features to characterize this trend from two aspects including the amount of recharging and the important sources for recharging. • Feature 4: The Average Recharge Amount of Virtual Currency. This feature represents the average amount of virtual currency for each recharge regardless of the sources for recharging. Benign users who participate in online promotion activities are usually also interested in other online financial activities. Therefore, these benign users tend to actively recharge their accounts. The recharge amount for each time by a benign user is commonly considerably large since users tend to decrease the hassle of recharging. In contrast, if a malicious account has been recharged, the amount of virtual currency for each recharge is usually bounded by a relatively small volume offered by the online promotion activity.

- Feature 5: The Percentage of Recharge from Promotion Activities. The feature intuitively profiles[23] how significantly online promotion activities contribute to the wealth of an account. Benign users are inclined to employ a variety of sources for recharge. Comparatively, malicious[24] accounts usually exclusively rely on online promotion activities to collect virtual currency.

4.3 Features of usage activities

As an increasing number of business capabilities are integrated into social networks, users conduct a variety of activities such as shopping and gifting. Features in this category characterize how users spend their wealth.

Feature 6: Total Amount of Expenditure.

- This feature characterizes the total amount of expenditure of an account regardless of the possible sources such as the associated bank accounts, the virtual currency, and other online social network platforms. As the popular online social networks are integrated into almost all mainstream e-business infrastructures, shopping and gifting through these accounts becomes prevalent. Users keep recharging their accounts, persistently associate their bank accounts with OSN accounts, and actively engage in shopping and gifting. Therefore, we expect that benign accounts accumulate a high amount of expenditure. Comparatively, the total amount of currency controlled by each malicious account is constrained by the total number of virtual currency collected from online promotions, which is expected to be relatively small.

Feature 7: The Percentage of Expenditure

- from Banks. User can associate her bank account with the OSN account. This bank account can be directly used for shopping and gifting in addition to recharging the OSN account with virtual currency.

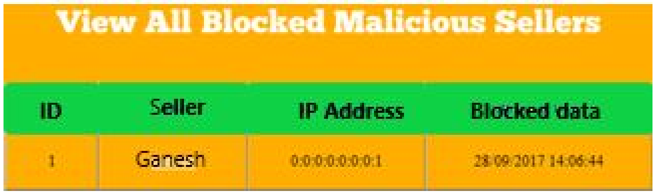
ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions exposure of users' bank identities in case of law enforcement.

Feature 8: The Percentage of Expenditure as

- Gifts. After malicious accounts collect virtual currency from the online promotion activities, they will transfer it to malicious accounts used for trading. Sending online gift cards becomes the best option for malicious accounts to transfer currency for two reasons. First, sending online gift cards inside an OSN usually does not incur any cost. Second, such transfer is independent to any bank, thereby requiring no personal information and consequently minimizing the exposure of attackers. We therefore design this feature to quantify the percentage of all expenditure that is used for gifts.

5. PREVIOUS WORK

Since online social networks play an increasing important role in both cyber and business world, detecting malicious users in OSNs becomes of great importance. For the further experiments for Many detection method shave been consequently proposed. Considering the popularity of spammers in OSNs, Figure 2 shows that these methods almost exclusively focus on detecting accounts that's end malicious content. Spamming attack can be considered as an information flow initiated from an attacker, through a series of malicious accounts, and finally to a victim account. Despite the diversity of these methods, they generally leverage partial or all of three sources for detection including, the content of the spam message, the network infrastructure that hosts the malicious information. The social structure among malicious accounts and victim accounts.



View All Blocked Malicious Sellers

ID	Seller	IP Address	Blocked data
1	Ganesh	0:0:0:0:0:0:0:1	28/09/2017 14:06:44

Figure 2: Blocked malicious seller

1. In the existing system, many detection methods have been consequently proposed. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts that send malicious content. A spamming attack can be considered as an information follow initiated from an attacker, through a series of malicious accounts, and finally to a victim account.

2. Despite the diversity of these methods, they generally leverage partial or all of three sources for detection including

1) the content of the spam message

2) the network infrastructure that hosts the malicious information (e.g., phishing content or exploits)

3) the social structure among malicious accounts and victim accounts. and then propagated maliciousness score using the derived graph.

6. MODULES DESCRIPTION

Bank Admin :In this module, the Admin needs to login by utilizing substantial client name and secret word. After login effective he can do a few activities, for example, View all clients and approve, View all Sellers and approve, Set Limit Access and view, View every single malignant client Based on Product Purchase(user attempts to buy with no parity) and square in the event that they to accomplish same thing more than the entrance limit, View every malevolent client Based on Amount Transfer(user attempts to move to another client with no equalization) and square on the off chance that they to accomplish same thing more than as far as possible, List all Malicious vender with Malware subtleties and notice this record holder as Spam record and square this client[7], see client and dealer un square solicitation and un square, View No of Malicious Users and Normal Users in outline, View item rank in diagram

User : In this module As per figure 3 shows there are n quantities of clients are available. Client should enlist with bunch choice before doing a few tasks. After enrollment effective he needs to sit tight for administrator to approve him and after administrator approved him. He can login by utilizing approved client name and secret key. Login effective he will do a few activities like - Register with Location and Login and Request to un square if u blocked View your profiles with Account Type(Malicious or Normal, Create Bank Account, View Account, View Mini Statement, Search Friends and Find Friends, Give Authorization, View Your Friends, Search Products by content catchphrase and view the subtleties, buy the item, Transfer the sum to your companion.

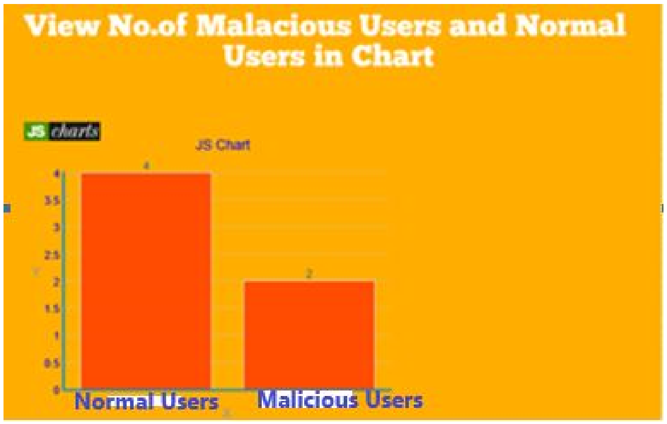


Figure 3: User chart

Seller : In this module, there are n quantities of clients are available. Merchant should enroll with bunch alternative before doing a few activities. After enrollment fruitful he needs to hang tight for administrator to approve him and after administrator approved him. He can login by utilizing approved client name and secret word. Login fruitful he will do a few tasks like View Profile with account type, Add Product with p cat, p name, manufacturer, p desc with peruse file, filename, p price, p uses, p image, view all items with rank and evaluations, View all bought clients with all out Bill.

7. RESULTS & DISCUSSIONS

This framework proposes a novel framework, specifically pro guard, to achieve this target by methodically coordinating highlights that describe accounts from three viewpoints including their general practices, their energizing examples, and the use of their money.

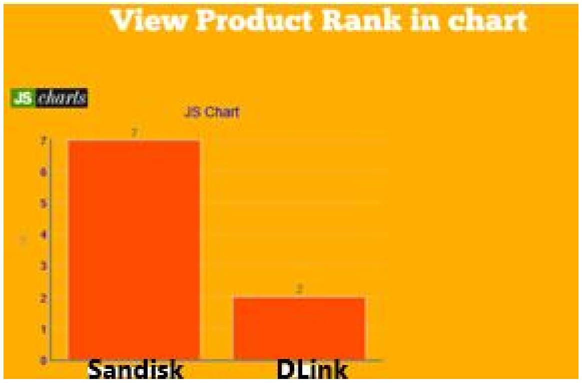


Figure 4: Product rating chart

The framework has performed broad examinations dependent on information gathered from the Tencent QQ, a worldwide driving OSN with worked in money related administration exercises [1].

To the best of our knowledge, this work represents the first effort to systematically detect malicious accounts used for online promotion activity participation. We have evaluated our system using data collected from online social network that uses a widely-accepted virtual currency (i.e., Q coin), to support online financial activities for active accounts.

Our experimental results in figure 4 have demonstrated that system can achieve a high detection rate of 96.57% with a very low false positive rate of 0.43%.This work represents the first effort to systematically detect malicious account used for online promotions activity participation.

8. CONCLUSION AND FUTURE WORK

This paper presents a novel system, pro guard, to automatically detect malicious OSN accounts that participate in online promotion events. pro guard leverages three categories of features including general behavior, virtual-currency collection[6], and virtual currency usage. Experimental results have demonstrated that our system can accomplish a high detection rate of 96.57% at a very low false positive rate of 0.43%.

There is a possibility that an attacker may hack some benign accounts and use them to participate in online promotion events. Hacking a considerable number of benign accounts is not a trivial task, which usually implies significant cost. In addition, mainstream social networks have usually enforced effective means to assist victim users to recover their hacked accounts. On the contrary, it is free for any user, including the attacker, to register a large number of accounts, which are dedicated to persistent malicious activities. Therefore, attackers have extremely limited motivation to use hacked accounts for this type of attacks. Nevertheless, if a hacked account is indeed used by an attacker for such attacks, this account will experience mixed benign and malicious behavior. If the malicious behavior dominates (i.e., the benign online financial activities are negligible), then we expect our method can still detect this account; unfortunately, if the benign activities dominates (i.e., this account is very active at online financial activities), this account is likely to introduce a false negative. Addressing false negatives in this case is definitely an important issue and seeking effective solutions falls into our future work

All the proposed features are based on essential financial functions such as recharging and gifting. In addition, all current features rely on coarse-grained information that minimizes privacy concerns, which may foster the deployment of the proposed system in a detection-as service model. Despite the fact that ProGuard can effectively detect malicious accounts used for collecting virtual currency from online promotion activities, it is not designed for detecting malicious accounts used for transferring and laundering virtual currency. Extending ProGuard to include such detection capabilities falls into our future work.

REFERENCES

1. Y. Wang, S. D. Mainwaring. **Human-currency interaction: Learning from virtual currency use in China,** in *Proc. SIGCHI Conf. Human Factors Computer Syst*ems, 2008, pp. 25-28. https://doi.org/10.1145/1357054.1357059
2. J. S. Gans and H. Halaburda, **Some economics of private digital currency**, Rotman School Management, Toronto, ON, Canada, Tech. Rep. 2297296, 2013.
3. X. Hu, J. Tang, and H. Liu. **Online social spammer recognition**, in *Proc. 28th AAAI Conf. Artificial Intelligence*, 2014, pp. 59-65.
4. X. Hu, J. Tang, H. Liu. **Leveraging knowledge across media for spammer recognition in micro blogging**, in *Proc. 37th Int. ACM SIGIR Conf. Research & Development in Information Retrieval*, 2014, pp. 547-556.
5. Z. Chu, S. Gianvecchio, H.Wang, and S. Jajodia. **Detecting automation of twitter accounts: Are you a human, Bot, or cyborg?,** *IEEE Trans. On Dependable and Secure Computing*, Vol. 9, pp. 811-824, Nov. 2012. https://doi.org/10.1109/TDSC.2012.75
6. Z. Chu, S. Gianvecchio and A. Koehl, H. Wang, and S. Jajodia. **Blog or block: Detecting blog bots through behavioral biometrics**, in Proc. *Computer Networks, Vol*. 57, pp. 634-646, 2013.
7. S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor. **Collective spammer recognition in evolving multi-relational social networks,** in *Proc. 21th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, 2015, pp. 1769-1778.

8. Y.R. Chen and H.H.Chen, **Opinion spammer recognition in Web forum**, in *Proc. 38th Int. ACM SIGIR Conf. on Research Development and Information Retrieval,,* 2015, 1998 pp. 759-762.
9. F.Wu, J. Shu, Y. Huang, and Z. Yuan. **Social spammer and spam message 36 co-detection in micro blogging with social context regularization**, in *Proc. 24th ACM International Conf. on Information and Knowledge Management*, 2015, pp. 1601-1610.
10. Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang. **Twitter spammer recognition using data stream clustering**, *Information Sci*ences, Vol. 260, pp. 64-73, March. 2014,
11. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. **Detecting and characterizing social spam campaigns**, in *Proc. 10th ACM SIGCOMM Conf. on Internet Meas*urement, 2010, pp. 35-47. https://doi.org/10.1145/1879141.1879147
12. S. Lee and J. Kim. **Warning Bird: Detecting suspicious URLS in twitter stream,** in *Proc. NDSS*, Vol. 12. 2012, pp. 1-13.
13. C. Yang, R. C. Harkreader, and G. Gu. **Die free or live hard? Empirical evaluation and new design for fighting evolving twitter spammers**, in Proc. *Int. Workshop Recent Advances in Intrusion Recognition*, 2011, pp. 318-337.
14. A. Abdallah, M. A. Maarof, and A. Zainal. **Fraud recognition system: A survey**, *Journal of Network and Computer Applications.*, Vol. 68, pp. 90-113, Oct. 2016.
15. J.West and M. Bhattacharya. **Intelligent financial fraud recognition: A comprehensive review**, *Computers and Security*, Vol. 57, pp. 47-66, Jun. 2016.
16. D. Olszewski. **Fraud recognition using self-organizing map visualizing the user profiles,** *Knowledge based Systems*, Vol. 70, pp. 324-334, Jan. 2014.
17. C.C. Lin, A.A. Chiu, S.Y. Huang, and D. C.Yen. **Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts judgments**, *Knowledge Based Systems,* Vol. 89, pp. 459-470, Sep. 2015.
18. C. S. Throckmorton, W. J. Mayew. M. Venkatachalam, and L. M. Collins. **Financial fraud recognition using vocal, linguistic and financial cues**, *Decision Support Systems*, Vol. 74, pp. 78-87, Jun. 2015.
19. Z. Afzal, M. J. Schuemie, J. C. van Blijderveen, E. F. Sen,M. C. Sturkenboom, and J. A. Kors. **Improving sensitivity of machine learning methods for automated case identification from free-text electronic medical records**, *BMC Medical Information Decision Makin*g, Vol. 13, pp 30, 2013. https://doi.org/10.1186/1472-6947-13-30
20. L. Breiman. **Random forests,** *Machine Learning*, Vol. 45, pp. 5-32, 2001.
21. Nagaratna Harikant and Suma V. **Risk Analysis in Facebook Based On User Anomalous Behaviors**, in *Proc*. of *International Conference on Intelligent Computing and Control Systems* ICICCS, 2017, pp 967-971.
22. Santa Barbara and Pittsburgh. **COMPA: Detecting Compromised Accounts on Social Networks**, in *Proc. of NDSS Symposium*, 2017.
23. M. A. Devmane and Dr. N. K. Rana. **Detection and Prevention of Profile Cloning in Online Social Networks**, in *Proc. of ICRAIE*, 2014.
24. Yasmeen Sultana and Prof. B.I.Khodanpur. **Detecting the Malicious Application using FRAppE**, in *Proc*. of *International Conference on Intelligent Computing and Control Systems* ICICCS, 2017, pp 1027-1032. https://doi.org/10.1109/ICCONS.2017.8250621
25. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen and Ben Y. Zhao. **Detecting and Characterizing Social Spam Campaigns,** in *Proc. of 10th ACM SIGCOMM on Internet Measurement*, 2010, pp 35-47.
26. Prateek Dewan and Ponnurangam Kumaraguru. **Towards Automatic Real Time Identification of Malicious Posts on Facebook**, in *Proc. of Thirteenth Annual Conference on Privacy, Security and Trust (PST)*, 2015.
27. Tao Stein, Erdong Chen and Karan Mangla, **Facebook Immune System**, *in Proc. of the 4th Workshop on Social Network Systems*, 2011,pp 1-8. https://doi.org/10.1145/1989656.1989664