Rupali Vishwakarma et al. 2019, 7:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

Survey on Enhance Reputation Based Approach for Detection Malicious Post from Social Networks Apps Using Data Mining Techniques

Phd Scholar *Rupali Vishwakarma*
Department of CSE AISECT University Bhopal, India
rupalidohare25@gmail.com

Dr. Pratima Gautam
Department of CSE AISECT University Bhopal, India
pratima_shkl@yahoo.com

Abstract- Online social networks apps main downside pretends content or malicious uniform resource locator, a.k.a. malicious web site, could be a common and high threat to cyber security. Malicious uniform resource locator host uninvited content (fake post, spam, phishing etc.) on-line social networks like Face book, Twitter, Hike, Instagram and WhatsApp are popularly utilized by community peoples for private and skilled use. the most aim of victimization networking sites are sharing photos, audio and video files and alternative media additionally written works, posting a resume for job looking etc. on these apps Face book is wide used for human action past and current friends, for advertising concerning business, products, textiles, education, etc. Before victimization these sites, we tend to additionally targeted on personal and skilled knowledge security. Hackers well knew the potential of victimization these apps for spreading malware and spam. During this paper, our contribution aims concerning detection unauthorized users and additionally malicious applications. We, so use Facebookapps Face book Rigorous Application authority. That argued to target detection harmful applications on Face book. Facebookapps additionally contributes for distinguishing pretend user account to stop the private data. Our result indicate that classifying malicious apps and observe pretend user requests on Face book. Our survey summary many type problems like spam URL's and fake post or fake information, fake accounts. Allover problem for not secure OSN. But our purpose secure user account and detection malicious applications and fake user accounts.

Keywords: malicious, Online Social Networks, Facebook apps, fake post, spam, Text Analysis.

I. INTRODUCTION

Online social network may be a platform that advantages peoples to make their profiles, finding and creating friends. On-line social networks are a lot of well-liked currently days. There are some OSN well-liked networks like Face book, Instagram and Twitter. Our key contribution is for Face book. Currently a day's third-party apps encourage the improvement in on-line social network (OSN). Such enhancements embrace fascinating or fun ways in which of communication among on-line friends and numerous activities like taking part in games or paying attention to songs. That's Face book provides an API. That facilitates integration of user expertise. 20M apps put in everyday and fascinating to grasp there are 500K apps are accessible on social networks. Recently, hackers have started taking advantage of the recognition of this third-party apps platform and deploying malicious applications. Face book is a lot of well-liked on-line social network website among everywhere the planet that causes increase in black market services [1] that encourage growth in pretend likes, comments and tags. pretend accounts are categorized into 2 sorts known as duplicate accounts and false accounts. During this work a system of economical categorization technique for distinguishing whether or not a post generated by a 3rd party application is malicious or not. Detection malicious URLs are currently a necessary task in network counterintelligence. To take care of potency of internet security, these malicious URLs have to be compelled to be detected, known further as their corresponding links ought to be recognized. Thus, users get protected against it and effectiveness of network security gets enhanced. The malicious users will transfer a content he needs to unfold. The content that contains malicious information is announced to alternative user's wall underneath a special kind. The user mistakes the posts for a true content and clicks the post, which is able to take him to a different page. So the malicious user will have the benefit of this method. So as to induce the eye of the user, the malicious user can embrace keywords or description of pages that may be of interest to the user. These will be adult content or free downloading sites and during this work we tend to targeted on detection malicious applications and fake user accounts. Detection of pretend user is finished on the premise of the user activities and their interaction with alternative users on Face book through analysis of user feed information [2].

II. FAKE ACCOUNT VARIETIES

Fake accounts are categorized into 2 varieties known as duplicate accounts and false accounts.

- Duplicate Account: a reproduction account refers to associate account maintained by a user additionally to his/her principal account.
- False Accounts: False accounts are more diminished into 2 classes user misclassified accounts and undesirable accounts.
- User-misclassified accounts: It represents the private profiles created by users for a business, organization, or non-human entity like a pet (Face book's terms of service permits such entities as a Page instead of a private profile).
- Undesirable accounts: These are the user profiles that are meant to be used for functions that violate Face book's terms of service, like spamming. fake accounts are primarily wont to below the belt increase ones power and influence among a target community [3]

There are many ways that hackers will have the benefit of a malicious app:

- The app will reach sizable amount of users and their Friends to unfold spam.
- The app will get users personal info like e-mail address, home town, and gender, and
- The app will reproduce by creating different malicious apps in style. In different words, there's motive and chance, and as a result, there are several malicious apps spreading on Face book daily [4].

III. Related work

Xianghan Zheng et al. [5] described a procedure to detect spammers in social networks. Social network users spend plenty of time on social networks to interact with friends. These social networks also attracted by many of abnormal users called spammers. These spammers post the malicious information, advertisements etc in social networks. In this methodology used sina weibo social network and support vector machines (SVM) algorithm to detect spammers. To develop a model they had used 16 million messages from various users in weibo social network. In this model 18 features are used to construct a feature vector. The network users are classified as spammers and non-spammers by manually. From the labeled dataset, 80% spammers and non-spammers are selected randomly as training dataset and remaining dataset considered as test dataset. The network user's behavior is analyzed with content-based features and user-based features. The feature vector dataset is given as input to the model for training. To gain highest spam detection accuracy of this model used 1:2 ratio between spammers and non-spammers of training dataset. With this 1:2 spammer to non-spammers ratio the model classify the dataset with 99.5% spammers accurately and 99.9% non spammers accurately.

F. J. Damerau et al. [6] A technique for computer detection and spelling errors. This paper describes that which word cannot be match in a dictionary, missing or extra letter or a single transposition. The unique word which is get entered is compared to the dictionary again, testing each time to see whether the words match- assuming one of these errors occurred. The words which might be wrong or missing are get detected and correct to it.

C. Lin et al. [7].in analyzes the real-time interaction of micro blogging events especially on Twitter. In their opinion the user may be considered as a sensor to monitor tweets posted recently and to detect different events. Justin Ma et al. have demonstrated the potential of a classifier based on suspicious URLs. They train their dataset on properties such as host-name length, overall URL length, and the count of the sub domain separating character. Combining these lexical features with host information (e.g. DNS registry info), the researchers report an accuracy rate of over 95%.

Hailu Xu et al.[8]. Studied a methodology to detect spam across online social networks. This methodology focuses on combining spam in one social network to another social network. They had used 1937 spam tweets and 10942 ham tweets and 1338 spam posts and 9285 ham posts. In TSD, out of 1937 spam tweets, 75.6% spam tweets contained in URL links, 24.4% spam tweets contained in words.

From 10942 ham tweets, 62.9% tweets are in URL links and words, remaining 37.1% consist of only words. For the spam posts of FSD, 32.8% spam posts consists of URL links and words, 67.2% of spam posts consist of words. For ham posts 95.1% consist of URL links and 4.9% only consist of words. They had used top 20 word features from Twitter spam data and Face book spam data. They had split the TSD and FSD into training and test data sets .The training and test data sets of TSD, FSD are used to train and test various classifiers like Random forest, logistic, random tree, Bayes Net, Naïve bayes.

M. Okazaki et al. [9].presented an initial study to quantify and characterize spam campaigns launched using accounts on Face book. They studied a large anonym zed dataset of 187 million asynchronous wall messages between Face book users, and used a set of automated techniques to detect and characterize coordinated spam campaigns. Authors detected roughly 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts.

Fire et al. [10].developed the Social Privacy Safeguard (SPS) software, which is a set of applications for Face book that aim to improve user account privacy policies. The application examines a user's friends list in order to determine accounts that have a risk to the user's privacy. Such accounts could then be protected by users from accessing their profile information. Using these set of data from the SPS developed over Face book, the authors could test several machine learning classifiers to detect fake profiles, some algorithms are been used: Naive Bayes, Rotation Forest and Random Forest are been used for fake profile detection.

Pern Hui et al. [11] Third-party applications capture the attractiveness of web and platforms providing mobile application. Many of these platforms accept a decentralized control strategy, relying on explicit user consent for yielding permissions that the apps demand. Users have to rely principally on community ratings as the signals to classify the potentially unsafe and inappropriate apps even though community ratings classically reflect opinions regarding supposed functionality or performance rather than concerning risks. To study the advantages of user-consent permission systems through a large data collection of Face book apps, Chrome extensions and Android apps. The study confirms that the current forms of community ratings used in app markets today are not reliable for indicating privacy risks an app creates. It is found with some evidences, indicating attempts to mislead or entice users for granting permissions: free applications and applications with mature content request; "look alike" applications which have similar names as that of popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

J. Kim et al. [12] Twitter can suffer from malicious tweets containing suspicious URLs for spam, phishing, and malware distribution. Attackers have limited resources and thus have to reuse them; a portion of their redirect chains will be shared. We focus on these shared resources to detect suspicious URLs. We have collected a large number of tweets from the Twitter public timeline and trained a statistical classifier with features derived from correlated URLs and tweet context information. Our classifier has high accuracy and low false- positive and false negative rates.

Malik Mateen et al.[13] studied an approach for spam detection in Twitter network. To detect spam in Twitter dataset used different kind of features like user based features, content based features and graph based features. user based features are based on users relationships and properties of user accounts. The spammers have to reach large number of profiles to spread misinformation. Different user account related features are Number of followers, Number of following, age of account, FF ratio and reputation. Content based features are related to tweets posted by user. Different features are total number of tweets, hash tag ratio, URL's ratio, mentions ratio, tweet frequency and spam words. Graph based features are used to identify spammer behaviour. Different features are in/out degree and between's. In the proposed methodology used Twitter dataset consist of 10,256 users and 467480 tweets. To develop a spam detection model used J48, decorate and Naive ayes classifiers. These three classifiers are individually trained on various dataset features and classify the dataset as spam or ham dataset. Out of these three classifiers J48 classifier highest accuracy to classify the data as spam or non spam. Content based features are best suitable for classifying the dataset. To classify the dataset with highest accuracy combine the content, user based and graph based features. The combined feature set is given as input to the three classifiers. But decorate and J48 classifiers have given highest accuracy up to 97.6%.

Sazzadur Rahma et al. [14] has developed Frappe, an accurate classifier for detecting malicious Facebook applications. Most interestingly, he highlighted the emergence of app-nets large groups of tightly connected applications that promote each other.

H. Gao et al. [15]. Due to less security guarantee in feature-based detection, graph-based approach is modeled as finite graph. Assuming that fake profiles can establish limited number of intruded (attack) edges, the sub graph formulated by the set of all real accounts is sparsely connected to false account, that is, the cut over intruded edges is sparse. This method makes prediction and find out such sparse cut with formal guarantees. For example, Tuenti deploy Sybil Rank to rank accounts according to their perceived likelihood of being false, based on structural properties of its social graph and based on their formulation.

Kaufman L et al. [16]. Presented an online spam filtering system that could be deployed as a component of the OSN platform to inspect messages generated by users in real time. Their approach focused on reconstructing spam messages into campaigns for classification rather than examining each post individually.

IV. PROBLEM DESCRIPTION

Online social networks are wide use of late for the aim of communication. Users will share a lot of variety of data among friends. However there exist some social networks users World Health Organization misuse the options of those social networks and promote the spreading of malicious content. They are doing this by uploading the malicious post in different user page. These contents unfold at a quick rate. There's no correct mechanism to notice these malicious posts directly and take away it effectively. Hackers notice the potential of spreading malware and spam victimization malicious apps. Black market services causes growth in pretend account. In existing system we will only notice the malicious app. to overcome this drawback we tend to developed planned system.

V. EXPECTED OUTCOME

- To observe malicious posts on social media.
- To observe malicious shared URL's on social media.
- To block of malicious posts and obstruction of malicious shared URL's.
- To provide directly chart for all problems in step with numerous 3 classes and it offers trustworthy accuracy and potency.

VI. PLANNED APPROACHES

Proposed approach initial determines the varied options like followers, followers, URL's, spam words, Replies and hash tags. These options are wont to observe spam accounts in twitter dataset. Manually all user accounts are pictured as spammers and non-spammers. In pre-processing step all continuous options are regenerate into separate options. In cluster approach user accounts are classified as spammers and non-spammers by hard the chance of user account. Cluster is an unsupervised learning approach, supported similar feature values the whole dataset is classed as sender or non-sender categories. In call tree learning approach, a choice tree structure was ready and also the decision was created at each level of tree to classify information set as spam or non-spam dataset. To enhance the accuracy of spam detection these 3 approaches are integrated. The integrated approach was distinctive the given dataset as sender or non-sender with find best accuracy. Problems overcome through Genetic algorithm using SOM and HC, FCM.

VII. CONCLUSION

Spamming could be a major drawback in internet-based things further as in social media. Totally different techniques are planned for spam filtering is exposed across numerous platforms with varies degree of measures. This survey targeted on a number of the current methods used for filtering social spam. Beginning with differing types of social spam, the paper has mentioned regarding recent developments within the field of elimination of social spam. At present, fake profiles are created by intruders to accomplish tasks like cyber-bullying and cyber-stalking. This survey centered on a number of the current techniques used for fake profile detection. Some data processing techniques used for detection and mitigation of cyber activities. In future analysis, progress chase mechanism aren't been used for dominant cyber problems like cyber-bullying and cyber-stalking. So there are several access management methods, policy-ensuring mechanism, access management protocols are major techniques will used for making certain protection over OSN framework. These techniques will build OSN framework as secure and safety interface for communication.

REFERENCES

[1]. B. Viswanath, et al. Towards Detecting Anomalous User Behavior in Online Social Networks. Proceedings of the 23rd USENIX Security Symposium (USENIX Security), August, 2014.

[2]. Y. Lee, W. Kang, and H. Son, "An internet traffic analysis method with map reduce, Data analysis for industrial sectors", in FGTYJ International Conference, 2015.

[3]. Z. Yang, et al. Uncovering social network sybils in the wild. Transactions on Knowledge Discovery from Data (TKDD), Vol. 8, No. 1, 2014.

[4]. HackTrix, "Stay away from malicious Facebook apps," 2013.

[5]. Xueying Zhang, Xianghan Zheng, A Novel Method for Spammer Detection in Social Networks, IEEE,2015.

[6]. F. J. Damerau, A technique for computer detection and correction of spelling errors, Commun.ACM, vol.7, no.3, pp.171–176, Mar.1964.

[7]. C. Lin, B. Zhao, Q. Mei, and J. Han. Pet:"A statistical model for popular events tracking in social communities", In Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data is mining. ACM, 2011.

[8]. Hailu Xu,Weiqing sun,Ahmad javaid: Efficient spam detection across online social networks,IEEE- 2015.

[9]. T. Sakaki, M. Okazaki, and Y. Matsuo: "Realtime event detection by social sensors", In Proceedings of the 19th international conference on World wide web ACM, 2010.

[10]. M. Fire, D. Kagan, A. Elyashar, Y. Elovici, Friend or foe? fake profile identification in online social networks, Social Network Analysis and Mining 4 (1) 1–23, 2014.

[11]. Chia, Pern Hui, Yusuke Yamamoto, and N. Asokan. "Is this app safe? a large scale study on application permissions and risk signals." Proceedings of the 21st international conference on World Wide Web. ACM, 2012.

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

[13]. Mateen, Malik, et al. "A hybrid approach for spam detection for Twitter." Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on. IEEE, 2017.

[14]. Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos,"Detecting Malicious Facebook Applications", IEEE/ACM transactions on networking,2012.

[15]. H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. N. Choudhary. Towards Online Spam Filtering in Social Networks. In NDSS, 2012.

[16]. Kaufman L., Rousseeuw P. J."Finding groups in data: An introduction to cluster analysis", in nescience, 2010.