Detecting Malicious Accounts in OSN based on Promotions

[1]Ms.Usha Nandwani, [2]Mr.SandeepWaghmare, [3]Mr. Santosh Behara, [4]Mr. Sonu Pandit

[1]Asst.Professor, [2, 3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India. [1]*ushanandwani@gmail.com*, [2]*sandeepwaghmare1999@gmail.com*,[3]*santoshbehara.sb@gmail.com*, [4]*sonupandit97@gmail.com*

Abstract- 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, 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.

Keywords: online social networks, malicious accounts, intrusion detection, network security, virtual currency.

I. INTRODUCTION

Online social networks (OSNs) that combine virtual currency deliver as an appealing platform for varied business activities, wherever on-line, interactive promotion is among the most active ones.

Specifically, a user will probably get the reward within the style of virtual currency by taking part in on-line betterment activities she will then use such reward in varied ways in which like on-line searching, transferring it to others, and even exchanging it for real currency. Such a virtual-currency-enabled on-line promotion model allows huge reaching, offers direct money stimuli to finish users, and in the meantime minimizes the interactions between business entities and money establishments.

However, it faces a major threat attackers will management an oversized range of accounts, either by registering new accounts or compromising existing accounts, to participate within the on-line promotion Such malicious activities can basically undermine the effectiveness of the promotion activities, instantly discharge the effectiveness of the promotion contribution from business entities and in the meantime damaging OSNs name. Within the following discussions, it sits down with such accounts as malicious accounts.

The effective detection of malicious accounts allows each OSNs and business bodies to require mitigation actions like prohibition these accounts or decreasing the chance to reward these accounts. [2]

II. AIMS AND OBJECTIVE

a) Aim

Aim of making this system is to systematically integrate features that symbolize accounts from three aspects including their general behaviors, their recharging patterns, and the uses of their currency. [2]

b) Objective

The main objective is to present the outlook of the recent concealment crimes that are occurring and influencing the entire process. A simple heuristic to stop newly registered accounts that are possible to be bots, function entities usually require the participating accounts to be registered for an assured amount of your time. The objective is to style a detection system capable of identifying mischievous accounts that participate in online promotion cases for virtual currency gathering before rewards. Detecting malicious accounts at this specific time leads to exclusive advantages. [2]

III. LITERATURE SURVEY

Paper1: Implementation of a system to detect malicious URLs for Twitter users:

Implementation of a system to detect malicious URLs for Twitter users. By considering this popularity of tweeter hacker's use of short Uniform Resource Locator (URL), as a result it disseminates viruses on user accounts. These are popularly practiced by numerous people to become linked up with each other and partake in their daily happenings through it. Over the last few years, there is a tremendous use of online social networking sites. It's also providing opportunities for hackers to enter

 DOI : 10.35291/2454-9150.2020.0235

easily in-network and do their unauthorized activities. [3]

Paper2: A Multiagent System Based Approached to Fight Financial Fraud: An Application to Money Laundering:

The system will keep up a profile for each customer; based on the transaction history, which will be used along with the rules created from official regulations to combat money laundering, to the capture and signal suspicious transactions processed by the various business systems. The system will decide on some marked cases and learn from the aid provided by the AML analyst during the decision-making process of the most complex cases. It will also monitor recommendations posted by control, flagging those involving money laundering. The database with profile history reflecting the learning period and a set of rules constitute the primary knowledge base of the agents. [5]

Paper3: Money laundering identification using Risk and Structural Framework Estimation:

ML behavioral patterns and ML detection framework features are essential to ML, but traditional research focuses on legislative considerations and compliance requirements. All the methods to identify the money laundering focus on the neighbor transferring in the pattern. Detection money laundering is the most important task for the enforcement directors and finance ministry also. Structural Money Laundering based on Risk Evolution Detection Framework (SMLRD) finds out the potential ML groups among a large number of financial transactions. [1]

IV. EXISTINGSYSTEM

Existing methods on detecting spamming accounts in online social networks, it's faced with new challenges to detect malicious accounts that participate in online promotion activities. First, different from spamming accounts, these accounts neither depends on spamming messages nor need malicious network infrastructures to launch attacks. Second, social structures don't seem to be necessary. Therefore, none of the existing methods is applicable to detecting malicious accounts in online promotion activities. To resolve the new challenges, our method Detects malicious accounts by exploring both regular activities of an account and its financial activities. To be more specific, maintaining active social structures does not benefit to attackers, which is fundamentally different from popular attacks such as spammers in online social networks. [2]

V. COMPARATIVE STUDY

Sr. No	Paper Name	Author/ publication	Technology	Advantage	Disadvanta ge
1	Implementation of a system to detect malicious URLs for Twitter users. [5]	Gawale, Nupur S., and Nitin N. Patil.	Machine learning, Data mining	It's also providing opportunities for hackers to enter easily in-network and do their unauthorized activities.	The purpose of our system is to detect the suspicious URLs from multiple accounts simultaneo usly in a real time manner.
2.	A Multiagent System Based Approached to Fight Financial Fraud: An Application to Money Laundering. [9]	Claudio Reginaldo Alexandre	Content-based Collaborative, Demographic Filtering.	Improve the quality of the process of signaling suspicious profiles in the anti- money laundering process.	Failed to capture suspicious transactions and do not assist Human Specialist.
3.	Money Laundering identification using Risk and Structural Framework Estimation. [1]	DR. G. Krishna Priya	Data mining -based real learning algorithm.	Improve the efficiency of the framework detection accuracy.	Limited presentatio n capacity.

VI. PROBLEM STATEMENT

To figure out new challenges, this method detects malicious accounts by inspecting both regular activities of an account and its financial activities. Compared to current methods on detecting malicious accounts in OSNs, it's faced with new test to detect mischievous accounts that take part in online promotion action. Firstly, different from scamming accounts, the actual accounts neither wait on spamming messages nor need malicious network framework to launch attacks. Secondly, social structures aren't mandatory. Therefore, none of the existing methods is suitable to spot malicious accounts in online promotion action. [2]

VII. PROPOSED SYSTEM

The paper is to style a detection system which able to identifying malicious accounts that participate in online promotion act for virtual currency collection before rewards is devoted. Firstly, straightforward heuristic to stop newly registered accounts that are likely to be bots, business entities normally require the participating accounts to registered for a particular amount of your time. Thus, the

 DOI : 10.35291/2454-9150.2020.0235

detected and weaken malicious accounts cannot be instantly replaced by the newly recorded accounts, thereby extremely limiting attacker's capabilities. ProGuard to automatically detect malicious OSN accounts that perform in online promotion event. ProGuard support three types of features including generic behavior, virtual-currency collection, and virtual-currency usage. Practical results supported labeled data accumulated from Tencent QQ, have demonstrated the detection accuracy of ProGuard, which done a high detection. [2]

VIII. ALGORITHM

Random Forest Classifier Step 1: Data Preprocessing

1. Split the dataset into training and test set (train_data & test_data).
2. Select random N data points from the training set.
3. Extract Independent and dependent Variable from the training dataset
4. Create Feature class based on similar subset variables

Step-2: Build the decision trees associated with the selected data points (Subsets) using RF Classifier as given below.

#classifier= RandomForestClassifier(n_esti mators= x, criterion="entropy")

classifier.fit(x_train, y_train) Where,

- **n_estimators=** The required number of trees in the Random Forest. The default value is 10. We can choose any number but need to take care of the over fitting issue.
- **criterion=** It is a function to analyze the accuracy of the split. Here we have taken "entropy" for the information gain.

Step-3: Predicting the test result

1. Model is first fitted to the training set, for predicting the test result from the available dataset.
   #x_prediction= classifier.predict(trai n_data)
   #y_prediction= classifier.predict(test _data)
2. Above prediction vector and test set real vector can be used to determine the incorrect predictions done by the classifier.

Step-4: Repeat Step 1 & 2.

Step-5: For new data points, find the predictions of each decision tree, and assign the new data points to the category that fits into the larger subset.

IX. 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 Data

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

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

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

X. SYSTEM ARCHITECTURE

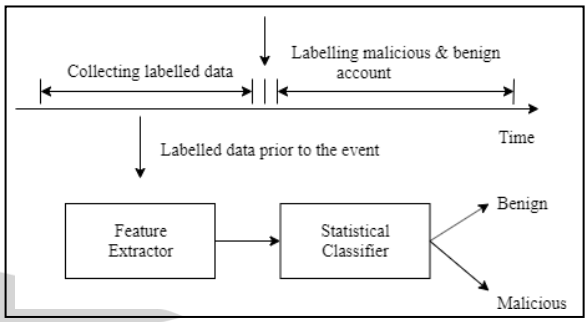

Fig.1: System Architecture

The Figure 1 represents the system architecture of OSNs and the secular relationship among the data compilation process, online promotion events, and the account categorize process. Therefore, it is worth noting that an account may not have any past financial activities since it engaged in the online promotion for the first time. First, it requires an immense amount of manual efforts for forensic examination such as identifying suspicious virtual-currency dealers in external e-commerce websites. In contrast, our method is designed to detect malicious accounts prior to the reward commitment. In addition, evidence for such forensic analysis will be only available after malicious accounts join in online promotion events.

XI. ADVANTAGES

1) The features and the detection framework can be easily applied to other OSNs that integrate financial activities.

2) It can successfully detect malicious accounts used for gathering virtual currency from online promotion activities.

3) Capability of fusing features from both networking and financial aspects for detection.

 DOI : 10.35291/2454-9150.2020.0235

XII. DESIGN DETAILS

Fig 2: Bank Admin Login

XIII. CONCLUSION

Thus, we have tried to implement the paper "Zhou, Yadong, et al". *"Proguard: Detecting malicious accounts in social- network-based online promotions."*IEEE Access 5 (2017) and according to implementation the conclusion of Detecting malicious accounts are as follows. As a system has performed verification of genuine or malicious accounts. It can successfully detect malicious accounts used for gathering virtual currency from online promotion activities.Hence the above project implemented is basically for the detecting malicious accounts of the users in online social networks and block that malicious accounts malicious URLs for Twitter users."

REFERENCE

[1] DR. G. Krishna Priya "Money Laundering identification using Risk and Structural Framework Estimation". Bonfing International journal of Data Mining. 1, Feb 2018.

[2] Zhou, Yadong, et al. "Proguard: Detecting malicious accounts in social- network-based online promotions." IEEE Access 5 (2017).

[3] Gawale, Nupur S., and Nitin N. Patil. "Implementation of a system to detect 2015 International Conference on Pervasive Computing (ICPC).IEEE, 2015.

[4] Kiruthiga, S., and A. Kannan. "Detecting cloning attack in Social Networks using classification and clustering techniques."2014 International Conference on Recent Trends in Information Technology.IEEE, 2014.

[5] Lopez-Rojas, Edgar Alonso, and Stefan Axelsson. "Multi agent based simulation (mabs) of financial transactions for anti- money laundering (aml)." Nordic Conference on Secure IT Systems. Blekinge Institute of Technology, 2012.

[7] S. Lee and J. Kim, "Warningbird: Detecting suspicious urls in twitter stream." in NDSS, vol. 12, 2012, pp. 1–13.

[8] C. Yang, R. C. Harkreader, and G. Gu, "Die free or live hard? empirical evaluation and new design for fighting evolving twitter spammers," in International Workshop on Recent Advances in Intrusion Detection. Springer, 2011, pp. 318–337.

[9] Alexandre, Claudio, and João Balsa. "A Multi-Agent System Based Approach to Fight Financial Fraud: An Application to Money Laundering." (2018).

 DOI : 10.35291/2454-9150.2020.0235