Analyzing and Detecting Money Laundering Accounts in OSN

[1]Miss. Usha Nandwani,[2]Miss. Sarika Mohape, [3]Miss. Namrata Dandekar, [4]Miss.Minakshi Patil
[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]sarikamohape0621@gmail.com, [3]namratadandekar21@gmail.com,
[4]minaakshipatil5@gmail.com

Abstract-Money laundering refers to activities that camouflage money sustain through illegitimateoperations and make them legal. Virtual money in online social networks (OSNs) play and increasingly important role in supporting various financial activities such ascurrent exchange, online shopping and paid games. Users usually purchase digitalcurrency using real currency. This fact motivates attacker to instrument an army ofaccounts to collect virtual currency unethically with no or very low cost andthen launder the collected cyber cash for massive profit. Such attacks not onlyintroduce significant financial damage of victim users, but also harm the viability of theenvironment. It is therefore of central importance to detect OSN accounts thatengage in laundering digital currency. This extensively study the behavior of bothmalicious and benign accounts based on operation data collected from, oneof the largest OSNs in the world. Finally, it is proposing a detection method by integratingthese features using a statistical classifier.

Keywords:Virtual Money, OSN, Malicious Account, System Vulnerability.

I. INTRODUCTION

Online social networks (OSNs) have started to leverage virtual currency as an effective means to glue financial activities across various platforms such as online shopping, paid online games, and paid online reading. Examples of virtual currency in such OSNs include but are not limited to Q Coin, Facebook Credits. Usually, users purchase virtual money using real currency at a regulated rate; a user can also transfer it to another via various ways such as recharging accounts and sending out gifts.

An attacker can collect virtual currency with low or zero cost. For example, attacker can compromise and subsequently control a legitimate account or register a huge number of accounts to win gifts (in the form of virtual currency) in online promotion activities, attacker can compromise andsubsequently control a legitimate account or register a huge number of accounts to win gifts (in the form of virtual currency) in online promotion activities. Next, attacker can instrument accounts under control to transfer virtual currency to other accounts in return for real currency, with rates that are usually much lower compared to the regulated rate. Attackers usually post advertisement in popular e-commerce websites to attract potential buyers. Money-laundering accounts have a caused a tremendous financial loss for compromised accounts, fundamentally undermined the effectiveness of online promotion activities, and possibly introduced potential conflicts against currency regulations. [1]

II. AIMS AND OBJECTIVE

a) Aim

The Aim is to identified money laundering activity. It discusses the challenges before banks and financial institutions, prevailing industry trends, and how emerging technologies can be used to monitor transactions to identify suspicious activities. The system disguises the sources, change the form, or move the funds to a place less likely to attract attention. A huge number of fraud acts is to produce a profit for the single or group that carries out the act.

b) Objective

The main objective of the study is to present the outlook of the recent money laundering offences that are occurring and affecting the whole economic activity. Objective is to design a detection system able to identifying fraud accounts that participate in online advertising event for virtual currency collection (at the collection phase) before awards are devoted.

III. LITERATURE SURVEY

Paper1: Detection of Money Laundering Groups: Supervised Learning on Small Networks:

 DOI : 10.35291/2454-9150.2020.0221

The system is designed to run as an ongoing monitoring tool in a live environment and is expected to analyze millions of transactions. This includes the construction of a network model representing relationships derived from financial records held by AUSTRAC, extraction of meaningful communities from this network, generation of features capturing the key characteristics of these communities, and finally, classification using a supervised learning approach. System advances the current state of the art by analyzing both explicit and implicit relationships derived from supplementary information. This system advances the current state-of-art by analyzing both explicit transactions relationships and implicit relationships derived from supplementary information.

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.[3]

Paper3:A model for Identifying Relationship of Suspicious Customers in Machine Learning using Social Network Functions:

AMLsystem provides a solution that identifies customers and illegal transactions in money remittance. The solution works based on specified rules on transactions trends that identify suspicious customers who involve in money laundering.The relationships such as business relationship, parent relationships, spouse relationships, etc. are identified using social networking functions.The database with profile history reflecting the learning period.[2]

IV. EXISTINGSYSTEM

In the existing system, an approach to sort and map relational data and present predictive models – based on network metrics – to assess risk profiles of client involved in the factoring business. The system finds that risk profiles can be predicted by using social network metrics.

The system shows the importance of using a network-based approach when looking for fraudulent financial operations and potential criminals.[6]

V. COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	METHOD	ADVANTAGE	DISADVANTAGE
1.	Detection of Money Laundering Groups: Supervised Learning on Small Networks	David Savage, Xiuzhen Zhang, Qiangmain Wang, XinghooYo	Support Vector Machine (SVM) Algorithm.	Network Analysis combining financial transaction and supplementary relationship.	System is that network structure is represented solely through graph invariant.
2.	A Multiagent System Based Approached to Fight Financial Fraud: An Application to Money Laundering	Claudio ReginaldoAlexandre	Content-based Collaborative, Demographic Filtering	Improve the quality of the process of signaling suspicious profile in anti-money laundering process.	Failed to capture suspicious transactions and do not assist Human Specialist.
3.	A model for Identifying Relationship of Suspicious Customers in Machine Learning using Social Network Functions	Abdul R. Shaikh, AmrilNazir	Data Mining based-Decision tree approach.	Good Approach Explained	Time Consuming
4	A Survey on Image Cryptography using Lightweight Encryption Algorithm	BhinalChauhan, ShubhangiAote	Cryptography lightweight-advanced encryption algorithm	It gives two layers of security data and satisfies the basic key factor of information security system which includes CIA & repudiation.	It is very difficult to identify the hidden image for the third party without knowing the bits of the frames.

VI. PROBLEM STATEMENT

Money laundering (ML) poses a serious risk not only to the financial organizations but also to the country. The increasing amount of lead to inflation and disrupts the whole cash flow and the economy. However, traditional investigative consumes numerous man-hours.

VII. PROPOSED SYSTEM

The system is designed which is an effective method capable of detecting money-laundering accounts. As a means towards this end, it performs an extensive study of behaviors of money-laundering accounts based on data collected from Tencent QQ, one of the largest OSNs in the world with an enormous body of reportedly 861 million active users.The system has conceived multi-faceted features that identified accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts.

VIII. ALGORITHM

Step 1: Data Preprocessing

 DOI : 10.35291/2454-9150.2020.0221

1. Import Dataset or add used already stored dataset values
2. Extract Independent and dependent Variable from the dataset
3. Split dataset into training and testing set

Step-2: Create a Support vector classifier

#classifier = SVC (kernel='linear', random state=0)

we have used **kernel='linear'**, as here we are creating SVM for linearly separable data

Step-3: Predicting the test result

1. Model is first fitted to the training set, for predicting the test result from the available dataset.

   #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: Segregate the data elements into minimum identified sub classes with best matching.

IX. MATHEMATICAL MODEL

Linear Kernel Calculation

It can be used as a dot product between any two observations. The formula of linear kernel is as below −

$$K(x, xi) = sum(x, xi)$$

It implies that the product between two vectors says$x\&xi$ is the sum of the multiplication of each pair of input values.

The kernel defines the similarity or a distance measure between new data and the support vectors. The dot product is the similarity measure used for linear SVM or a linear kernel because the distance is a linear combination of the inputs.

Radial Basis Function (RBF)/ Gaussian Kernel

RBF kernel, mostly used in SVM classification, maps input space in indefinite dimensional space. Following formula explains it mathematically −

$$K(x, xi) = exp(-gamma\ sum(x - xi\hat{}2))$$

Here, *gamma* ranges from 0 to 1. We need to manually specify it in the learning algorithm. A good default value of *gamma* is 0.1.

X. SYSTEM ARCHITECTURE

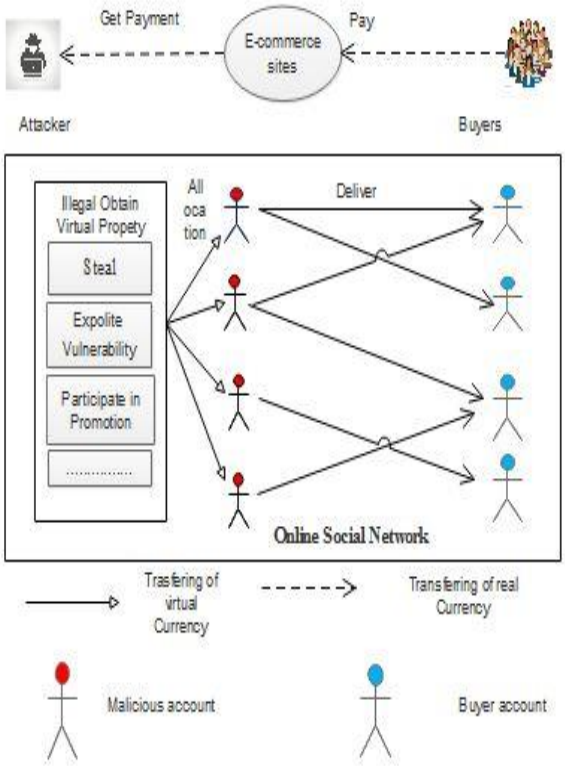

Fig.1: System Architecture

Description:

Figure demonstrates a regular procedure of virtual cash washing. The first step is to collect virtual money with zero or very minimal effort. For instance, assailants can hack client's records (and along these lines control their virtual cash), abuse the system vulnerabilities, or take part in online promotion exercise to win virtual money for nothing or at altogether limited rates. Next, assaulters draw in potential purchasers with impressive limits, through different ways, for example, spreading spams and posting ads, sell the virtual money in prevalent internet business sites, for example, eBay or Tobao. When a purchaser submits the buy (i.e., pays genuine cash to an aggressor through the internet business sites), their record will get virtual money (e.g., as blessings) from one or different vindictive records constrained by an assailant. Since OSNs may investigate a record in the event that it has started countless in a brief timeframe, an assaulter for the most part circulates their virtual cash over numerous records and uses them then again to exchange virtual money to purchasers.

XI. ADVANATGES

1. Login activities, which include the account ID, the login date, the login IP address, and the account level.
2. The expenditure activities, which include the expenditure account ID, the expenditure date, the

 DOI : 10.35291/2454-9150.2020.0221

expenditure amount, the purchased service, the payment way, and the account ID to receive the service.

3. The recharging activities, which include the recharging account ID, the recharging date, the recharging amount, the payment way.
4. It is based on behaviour analysis and Feature Extraction.
5. There is vitality Feature to detect malicious attackers.

XII. DESIGN DETAILS

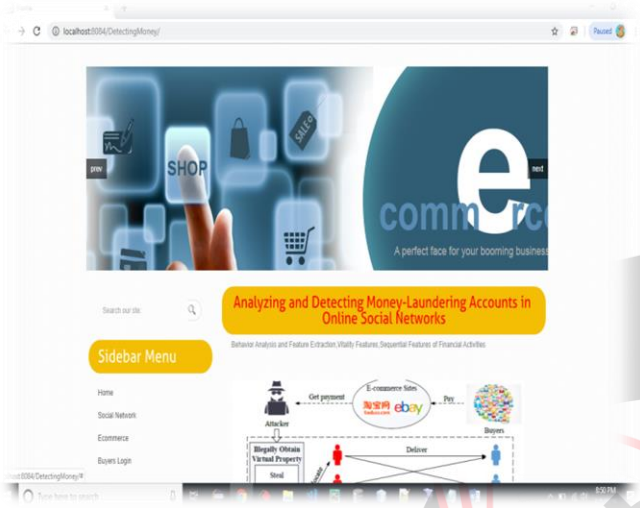

Fig 2: Result

XIII. CONCLUSION

Thus, we have tried to implement the paper "Yadong Zhou, Ximi Wang, Junjie Zhang, Peng Zhang, Lili Liu, Huan Jin, and Hongbo Jin", "*Analyzing and Detecting Money Laundering Account in OSN*", IEEE 2017. And according to implementation of Detecting malicious account the conclusion is as follows: System has performed verification of real and malicious account. Also, It can effectively detect malicious account that is used for collecting virtual currency from online promotion activities. Hence, the above project is implemented basically for the detecting malicious accounts of the user in online social network and find that malicious account.

REFERENCE

[1] DavidSavage, Xiuzhen Zhang, Qiangmain Wang, Xinghoo Yo. (2017). "Detection ofMoney Laundering Groups: Supervised Learning on Small Networks". The AAAI-17Workshop on AI and Operation Research for social Good WS-17-01, IEEE 2017.

[2] Abdul R. Shaikh, Amril Nazir, Member, IAENG (2018) "A model for Identifying Relationship of Suspicious Customers in Machne Learning using Social Network Functions". Proceeding of the World Congress on Engineering July 4-6, 2018, London

[3] Claudio Reginaldo Alexandre "A Multiagent System Based Approached to Fight Financial Fraud: An Application to Money Laundering". IEEE 2018

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

[5]Bhinal Chauhan, Shubhangi Aote "A Survey on Image Cryptography using Lightweight Encryption Algorithm" IJSRSET 2018.

[6] Y. Wang and S. D. Mainwaring, "Human-currency interaction: learning from virtual currency use in China," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.

[7] Y. Zhou, D. Kim, J. Zhang, et al., "ProGuard: Detecting Malicious Accounts in Social- Network-Based Online Promotions," IEEE Access, vol. 5, 2017, pp. 1990-1999.

 DOI : 10.35291/2454-9150.2020.0221