Detection of Money Laundering in Online Social Networks

DEVUPALLI SIRISHA [#1], GANNU RUPA SANTHI SREE [#2],

KARANAM MARY PRATHYUSHA [#3] , ANDE SOWMYA SRI [#4], RAHIMUNNISA SHAIK [#5]

[#1, 2, 3, 4] B.Tech Scholars, Department of Computer Science and Engineering,
Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ
Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh,530046.

[#5] Assistant Professor, Department of Computer Science and Engineering,
Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ
Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh,530046.

ABSTRACT

In current days online social networks (OSN) have become one of the prominent roles in interchanging the information from one location to another location in the world. Virtual currency in online social networks plays a vital role in performing some financial activities like e-commerce, online games, web marketing, and foreign currency exchange. As we know that OSN users try to purchase virtual currency with their original cash and try to conduct their activities with that virtual money, this laid a path for the attackers to create some sort of attacks on the user account to collect those virtual currencies in an illegal or fake manner. The main motto of the attackers or intruders is to launch a bulk number of web sites to attract the users to exchange the virtual currency and buy those things with low cost and gain huge profit. These attacks not only lose the user financially but also try to harm the other factors of that user. In order to overcome these problems, we try to design an application that can able to differentiate the benign accounts and malicious accounts based on the operations which are performed by that appropriate user. In order to show the performance of our proposed application, we try to choose data collected from Tencent QQ, one of the largest OSNs in the world. And finally, we try to divide the accounts into three aspects like account viability, transaction sequences, and spatial correlation among accounts. By conducting various experiments on our collected database, we finally came to the conclusion that our detection method by integrating these features using a statistical classifier can achieve a high detection rate at a very low false-positive rate.

Key Words:

Online Social Networks, Virtual Currency, Transaction Sequences, Spatial Correlation, False-Positive Rate, Foreign Currency Exchange

I. INTRODUCTION

According to a well-known article social media is defined in **[1],** as a group of internet based applications that build on the ideological and technological foundations of Web 2.0.This is built in order to allow the users to create a new event and try to exchange the same event to users who are residing far away via social media, people can enjoy enormous information, convenient communication experience and so on, which is clearly shown on figure 1. Even though it is more

familiar for end users, this may still face a lot of limitations like virtual currency attacks. This virtual currency attack is one which is created by a lot of attackers or intruders in online social networks to create some sort of fake urls and try to gain illegal money from the genuine users [2].

Figure 1.Denotes the various advantages of using Social Media to Promote Virtual Currency

As we all know that virtual currency and real currency can interact in many ways to promote business, exchange, buy, sell, and share the information one from another. The use of social media for promoting the above all activities makes a popular platform for malicious users to launch attacks in online known as social spammers. These social spammers cannot be identified directly in the online social networks but rather they can be detected by building classifiers based on content and social network information[3].

In this present application we try to use Java API, which is a large collection of ready-made software components that provide many useful capabilities, such as GUI widgets. All the predefined classes and methods are linked under a single library or interfaces known as packages. By using this predefined packages we can able to show the performance of this proposed application. In order to store, access, calculate, classify and cluster[4] the data we try to use JDBC (java database connectivity) technique. JDBC is a java API that offers 0 generic SQL database access mechanisms that provides a consistent interface to a variety of RDBMSs which is developed by Sun Microsystems. He defines J2ME as a highly optimized java runtime environment targeting a wide range of consumer products, cellular phones, screen photos and car navigation systems. It brought a cross platform functionality of java language to small devices, allowing mobile wireless devices to share applications[5].

II. LITERATURE WORK

In this section we mainly discuss about the background work that was carried out in finding the work that is related to detection of money laundering in online social networks.

MOTIVATION

Two well-known authors like Y.Wang and S.D. Main proposed a paper and found that how virtual currency is perceived , obtained, and spent can critically shape gamer's behavior and experience .By analysis from an ethnographic study of virtual currency use in China. Bringing money into HCI design heightens existing issues of realness, trust, and opportunities for users experience innovation[6].

Two well-known authors like X.Hu and J.Tang proposed a paper on general optimization framework to collectively use content and network information for social spammer detection and provide the solution for efficient online processing .Social spammers continuously change their spamming content patterns to avoid detecting. The reflexive reciprocity makes it easier for social spammer to establish social influence and pretend to be normal uses by quickly accumulating more friends[7].

Two well-known authors like Z.Chu and S.Gainvecchio proposed a paper on studying in detection of automation of twitter accounts as it is new application playing dual roles of online social networking and micro blogging. They focused on classification of human, bot and cyboard accounts in twitter. They observed the difference among human and cyboard in terms of tweeting behavior ,content and accounts properties over large scale accounts an d proposed a classification system which are used to combined features extraction from unknown users to determine likelihood of being human, bot or cyborg. They also detected blog bots through behavioral biometrics, primarily mouse and keystroke dynamics to distinguish between human and bot[8].

.

Two well-known authors like S.Fakhraej and J.Foulds proposed a paper on 99 a social network as a time, stamp multi relational graph to identify spammer accounts by using structural features, sequence modeling and collective reasoning They used PSL and Graph lab create to prototype experimentally evaluate solutions[9].

VIRTUAL CURRENCY

Virtual currency is a type of un-specified digital money, which is issued by a private member or community and usually accepted among the members of that community. In the year 2014, the first virtual currency is launched and approved by the European bank as a digital representation of value that is neither issued by a central bank or a public authority. This is approved under some special conditions or constraints like accepting by natural or legal persons as a means of payment and can be transferred, stored or traded electronically".

Figure 2.Denotes the BITCOIN as one of the major Virtual Currency

From the above figure 2, we can able to clearly identify Bitcoin is one form of virtual currency, which is mainly a decentralized currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries. These bitcoins will be purchased based on user original currency, if the user has full amount to pay 1 bit coin he will deposit his original currency into the account linked with this site and the site will grant a virtual currency like bit coin equal to the original cash. This value will not be same always as due to market statistics the value of virtual currency may be increased or decreased dynamically in the time period[10].

III. THE EXISTING METHOD

In this section we mainly discuss about the existing method used for virtual currency and its limitations.

Lin et al. ranked the importance of fraud factors used in financial statement fraud detection, and investigated the correct classification rates of three algorithms including Logistic Regression, Decision Trees, and Artificial Neural Networks. Throckmorton et al. proposed a corporate financial fraud detection method based on combined features of financial numbers, linguistic behavior, and non-verbal vocal. Compared to the studied financial fraud detection problems, account behaviors of collecting and using the virtual currency in online promotion activities are almost completely different with traditional financial systems since they do not only involve financial activities but also networking and online promotion activities. Lee et al. devised a method to first track HTTP redirection chains initiated from URLs embedded in an OSN message, then grouped messages that led to web pages hosted in the same server, and finally used the server reputation to identify malicious accounts.

IV.THE PROPOSED METHODOLOGY USED

In this section we mainly discuss about the proposed method used for virtual currency and its advantages compared with the existing systems.

PRELIMINARY KNOWLEDGE

The goal of our system is to design an effective method which is capable of detecting money boundary laundry accounts .In this through an extensive study of behavior of current booted on data collected from Tencent QQ which is shown in below fig 3, which is one of the largest OSN dataset having million active users .We devised multi features that characteristics account from three aspects account viability, transaction sequence, & spatial correlation among account. Our method achieve high detection rate of 94.2 percent.

Tencent QQ is a leading OSN from which we have collected the data. This data set offers a variety of services which are glued together using Qcosn. The virtual concurrency distributed and managed by Tencent QQ. In many ways we can get the virtual currency . In our system we get it by play online games and we purchase something with it and then we can detect a user as malicious or not.

Figure 3.Denotes the HISTORY of Tencent QQ Web Portal

IMPLEMENTATION

The proposed method is implemented using java language to develop a system which is online social network; here we have an admin who looks after the transactions a producer and a consumer. Here the user is a consumer, he gets registered in the website login and then play a game then he purchase the goods from the website by using the virtual currency which he gets by playing a game. In this user have a limit that user has to plays only once in a day. To play the game he first add the bank account.

The malicious user, changes the system operations, to violate the limit assigned by the admin and try to gain illegal profit from the virtual currency. These all will be recorded by the admin after the purchase is done in the later stage. Now the admin logs in the websites and checks if any malicious uses is detected.

V. EXPERIMENTAL REPORTS

We have conducted experiment on several sample offline data using JAVA programming language using HTML and JSP as front end GUI and JDBC as backend connectivity logic and MYSQL as database to store all the records of OSN users. Finally, we developed an application which can able to show the performance of our proposed application by taking sample transactions collected from Tencent QQ database.

GENERAL BEHAVIOUR FEATURE

In this module, the 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.

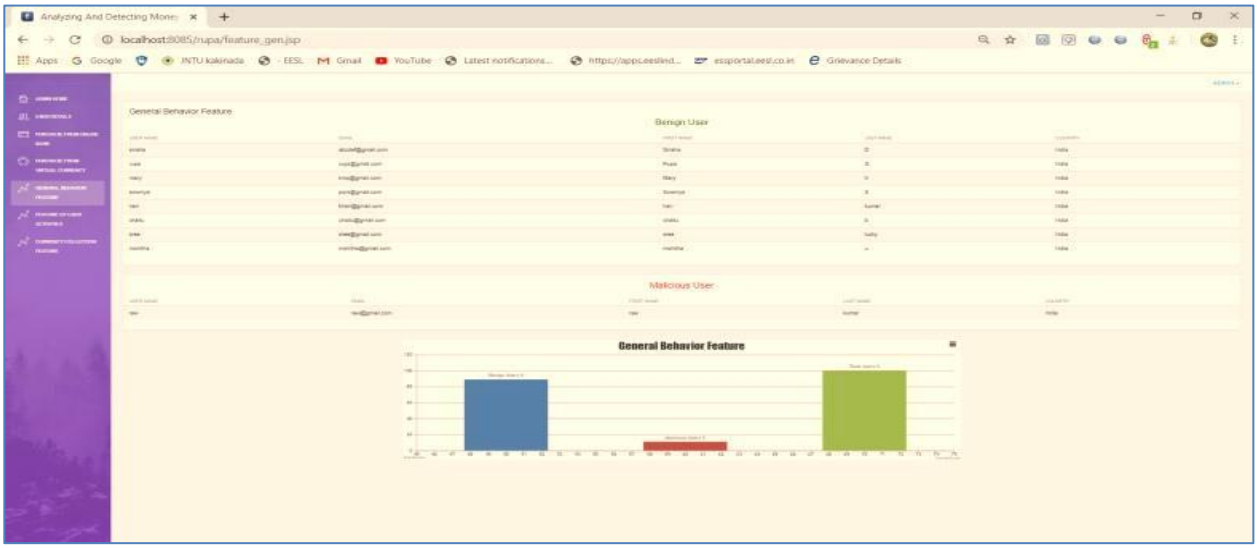

Figure 4.Denotes the General Behaviour Feature

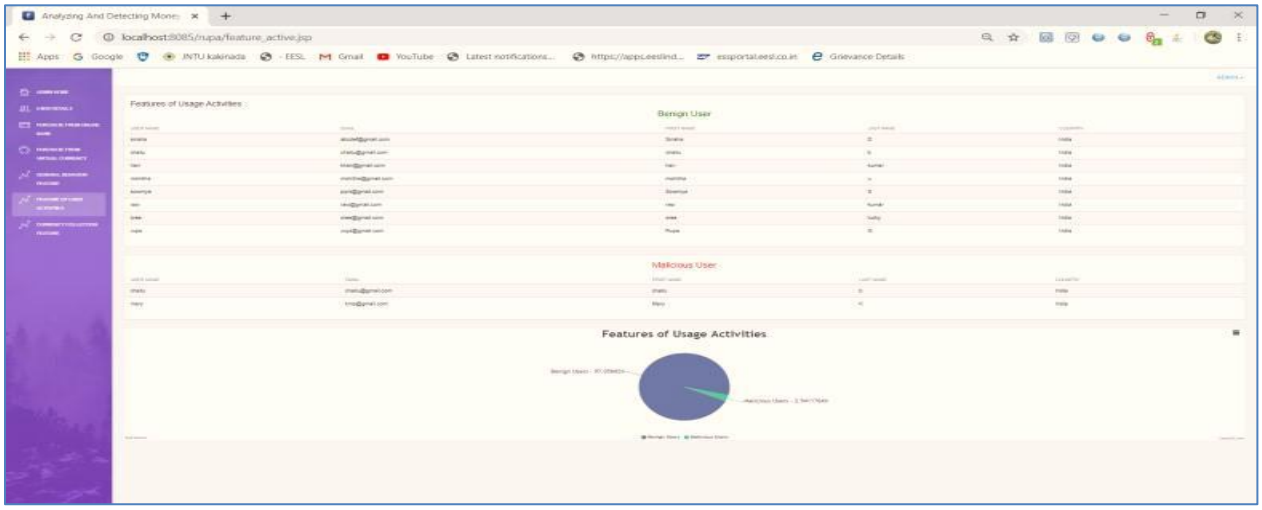

Figure 5.Denotes the Main Features of User Activity

CURRENCY COLLECTION FEATURE

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, buying virtual goods, and transferring from other accounts. The 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.

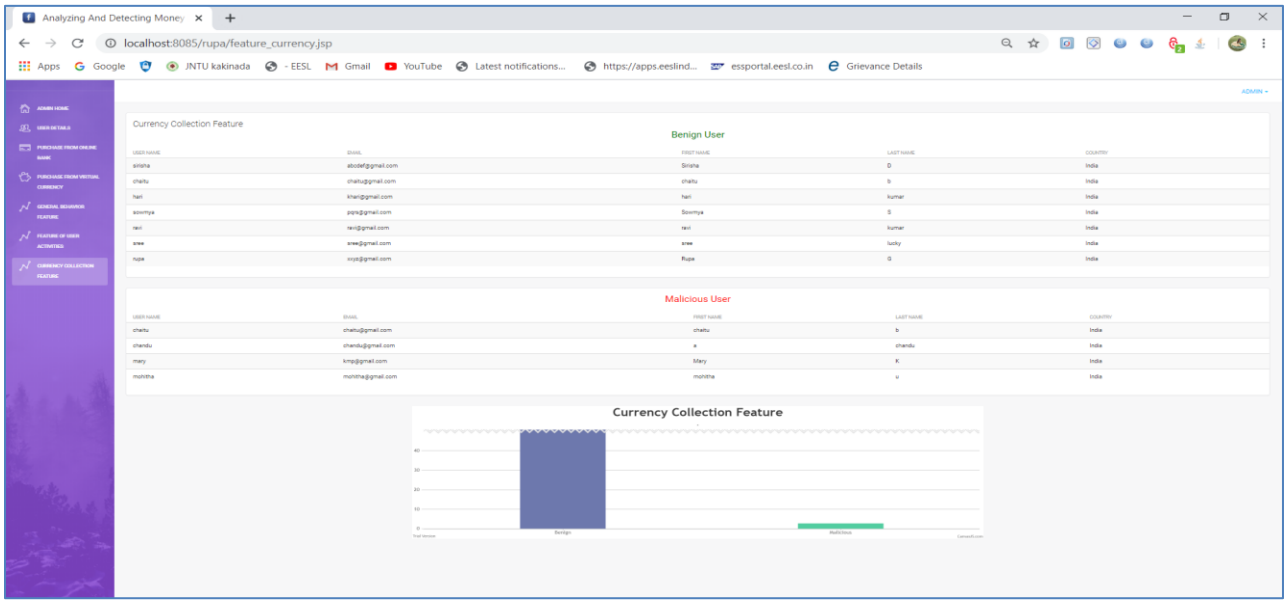

Figure 6 .Denotes the Currency Collection Feature

VI. CONCLUSION

This system presents the analysis and detection method of money laundering accounts in OSNs. We analyzed and compared the behavior of both malicious and benign accounts from three perspectives: the account viability, the transaction sequences, and spatial correlation among accounts. We designed a collection of features to systematically characterize the behavior of benign accounts and malicious accounts. Experimental results based on labeled data collected from Tencent QQ, a global leading OSN, demonstrated that the proposed method achieved high detection rates and very low false positive rates

VII. REFERENCES

[1] 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.

[2] J. S. Gans and H. Halaburda, "Some economics of private digital currency," Rotman School of Management Working Paper, no. 2297296, 2013.

[3] X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65.

[4] "Leveraging knowledge across media for spammer detection in microblogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 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 Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, 2012.

[6] Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog or block: Detecting blog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

[7] S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, "Collective spammer detection in evolving multi-relational social networks," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769–1778.

[8] Y.-R. Chen and H.-H.Chen, "Opinion spammer detection in web forum," in Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2015, pp. 759–762.

[9] F. Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in microblogging with social context regularization," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610 .

[10] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering," Information Sciences, vol. 260, pp. 64–73, 2014.

VIII. ABOUT THE AUTHORS

1) **DEVUPALLI SIRISHA** is currently pursuing her final year B.Tech in Computer Science and Engineering at Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh, 530046.Her area of interest includes Data Mining.

2) **GANNU RUPA SANTHI SREE** is currently pursuing her final year B.Tech in Computer Science and Engineering at Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh,530046. Her area of interests includes Networking.

3) **KARANAM MARY PRATHYUSHA** is currently pursuing her final year B.Tech in Computer Science and Engineering at Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh,530046.Her area of interests includes Android.

4) **ANDE SOWMYA SRI** is currently pursuing her final year B.Tech in Computer Science and Engineering at Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh,530046.Her area of interest includes Artificial Intelligence.

5) **RAHIMUNNISA SHAIK** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Vignan's Institute of Engineering for Women, Duvvada, Vadlapudi post, Backside of VSEZ Kapujaggaraju Peta, Visakhapatnam, Andhra Pradesh, 530046.She has more than 3 years of teaching experience and her research interests includes Data Mining and Artificial Intelligence.