Analyzing and Detecting Money-Laundering Accounts in Online Social Networks

**ABSTRACT**

Virtual currency in online social networks (OSN) plays an increasingly important role in supporting various financial activities such as currency exchange, online shopping, and paid games. Users usually purchase virtual currency using real currency. This fact motivates attackers to instrument an army of accounts to collect virtual currency unethically or illegally with no or very low cost and then launder the collected virtual money for massive profit. Such attacks not only introduce significant financial loss of victim users, but also harm the viability of the ecosystem. It is therefore of central importance to detect malicious OSN accounts that engage in laundering virtual currency. To this end, we extensively study the behaviors of both malicious and benign accounts based on operation data collected from Tencent QQ, one of the largest OSNs in the world. Then, we devise multi-faceted features that characterize accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts. Finally, we propose a detection method by integrating these features using a statistical classifier, which can achieve a

high detection rate of 94.2% at a very low false positive rate of 0.97%.

**EXISTING SYSTEM**

* 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 clients involved in the factoring business. The system ﬁnds that risk proﬁles can be predicted by using social network metrics.
* In the system dataset, the most dangerous social actors deal with bigger or more frequent ﬁnancial operations; they are more peripheral in the transactions network; they mediate transactions across different economic sectors and operate in riskier countries or Italian regions.
* Finally, to spot potential clusters of criminals, we propose a visual analysis of the tacit links existing among different companies who share the same owner or representative. The system ﬁndings show the importance of using a network-based approach when looking for suspicious ﬁnancial operations and potential criminals.

**Disadvantages**

* + It is not based on Behavior Analysis and Feature Extraction.
  + There is no Vitality Features to detect malicious attackers.

**PROPOSED SYSTEM**

* The proposed system is designed which is an effective method capable of detecting money-laundering accounts. As a means towards this end, we perform 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 a giant body of reportedly 861 million active users.
* The system has devised multi-faceted features that characterize accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts.
* Experimental results have demonstrated that our method can achieve a high detection rate of 94.2% with a very low false positive rate of 0.97%. To the best of our knowledge, this work represents the first effort to analyze and detect money-laundering accounts in OSNs integrating virtual currency at this large scale.

**Advantages**

* Login activities, which include the account ID, the login date, the login IP address, and the account level.
* The expenditure activities, which include the expenditure account ID, the expenditure date, the expenditure amount, the purchased service, the payment way, and the account ID to receive the service.
* The recharging activities, which include the recharging account ID, the recharging date, the recharging amount, the payment way.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV or later version

➢ RAM - 4 GB (min)

➢ Hard Disk - 40 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP or Later Versions
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL