
PROGAURD - DETECTING MALICIOUS ACCOUNTS IN SOCIAL-NETWORK-BASED ONLINE PROMOTIONS

K. Rambabu¹, Amirapu Surya Sai Bharadwaj,

¹Assistant professor(HOD) , MCA DEPT, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**

Email:- kattarambabudnr@gmail.com

²PG Student of MCA, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**

Email:- bharadwajamirapu@gmail.com

ABSTRACT

Online social networks (OSNs) gradually integrate financial capabilities by enabling the usage of real and virtual currency. They serve as new platforms to host a variety of business activities, such as online promotion events, where users can possibly get virtual currency as rewards by participating in such events. 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, we propose 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. We have performed extensive experiments based on data collected from the Tencent QQ, a global leading OSN with built-in financial management activities. Experimental results have demonstrated that our system can accomplish a high detection rate of 96.67% at a very low false positive rate of 0.3%.

1 INTRODUCTION

Online social networks (OSNs) that integrate virtual currency serve as an appealing platform for various business activities, where online, interactive promotion is among the most active ones. Specifically, a user, who is commonly represented by her OSN account, can possibly get reward in the form of virtual currency by participating online promotion activities organized by business entities. She can then use such reward in various ways such as online shopping, transferring it to others, and even exchanging it for real currency [1]. Such virtual-currency-enabled online promotion model enables enormous outreach, offers direct financial stimuli to end users, and meanwhile minimizes the interactions between business entities and financial institutions. As a result, this model has shown great promise and gained huge prevalence rapidly. However, it faces a significant threat: attackers can control a large number of accounts, either by registering new accounts or compromising existing accounts, to

participate in the online promotion events for virtual currency. Such malicious activities will fundamentally undermine the effectiveness of the promotion activities, immediately voiding the effectiveness of the promotion investment from business entities and meanwhile damaging ONSs' reputation.

Literature Survey

Detecting Clusters of Fake Accounts in Online Social Networks

Fake accounts are a preferred means for malicious users of online social networks to send spam, commit fraud, or otherwise abuse the system. A single malicious actor may create dozens to thousands of fake accounts to scale their operation to reach the maximum number of legitimate members.

Detecting and taking action on these accounts as quickly as possible is imperative in order to protect legitimate members and maintain the trustworthiness of the network. However, any individual fake account may appear to be legitimate on first inspection, for example by having a real-sounding name or a believable profile.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

In the existing system, many detection methods have been consequently proposed. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts that send malicious content. A spamming attack can be considered as an information flow initiated from an attacker, through a series of malicious accounts, and finally to a victim account.

Disadvantages of Existing System:

- It takes a lot of time to find the spammers and their accounts in Social network
- The false rate is high in this method.
- We want a lot of time and resources to find the spam accounts.
- We need to examine the content of the message and track all the recipients for that message and need to do research on how it finally hits the target client.
- Because of its environmental structure and dependency on other users it does not give the accurate results.

Proposed System & algorithm

In the proposed system, the system proposes 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.

Advantages of ProGuard:

- Enhances security: Protects online promotion events from fraudulent activity.
- Financial protection: Prevents losses due to malicious accounts.
- Efficient reward distribution: Ensures legitimate users receive rewards.

Architecture Diagram

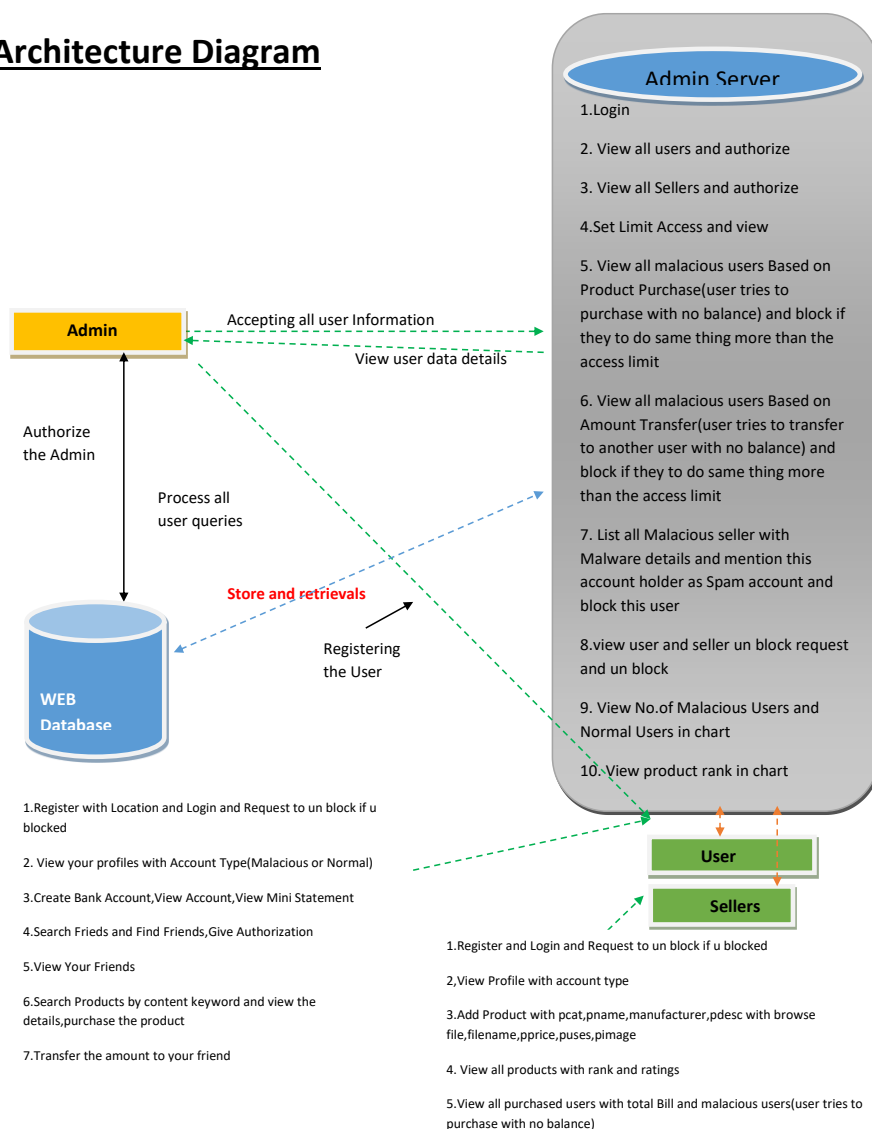


Fig:3.1 System Architecture

IMPLEMENTATION

MODULES

- **Bank Admin**

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View all users and authorize, View all Sellers and authorize, Set Limit Access and view, View all malicious users Based on Product Purchase(user tries to purchase with no balance) and block if they to do same thing more than the access limit, View all malicious users Based on Amount Transfer(user tries to transfer to another user with no balance) and block if they to do same thing more than the access limit, List all Malicious seller with Malware details and mention this account holder as Spam account and block this user, view user and seller un block request and un block, View number of Malicious Users and Normal Users in chart, View product rank in chart

- **User**

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he must wait for admin to authorize him and after admin authorized him. He can login by using authorized username and password. Login successful he will do some operations like --- Register with Location and Login and Request to unblock if you blocked View your profiles with Account Type (Malicious or Normal, Create Bank Account, View Account, View Mini Statement, Search Friends and Find Friends, Give Authorization, View Your Friends, Search Products by content keyword and view the details, purchase the product, Transfer the amount to your friend.

- **Seller**

In this module, there are n numbers of users are present. Seller should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized username and password. Login successful he will do some operations like View Profile with account type, Add Product with pcat,pname,manufacturer,pdesc with browse file,filename,pprice,puses,pimage , View all products with rank and ratings, View all purchased users with total Bill and malicious users (user tries to purchase with no balance)

5 RESULTS AND DISCUSSION

2 SCREENSHOTS



Fig: 1.1 – Home Page



Fig: 1.2 – Home Page

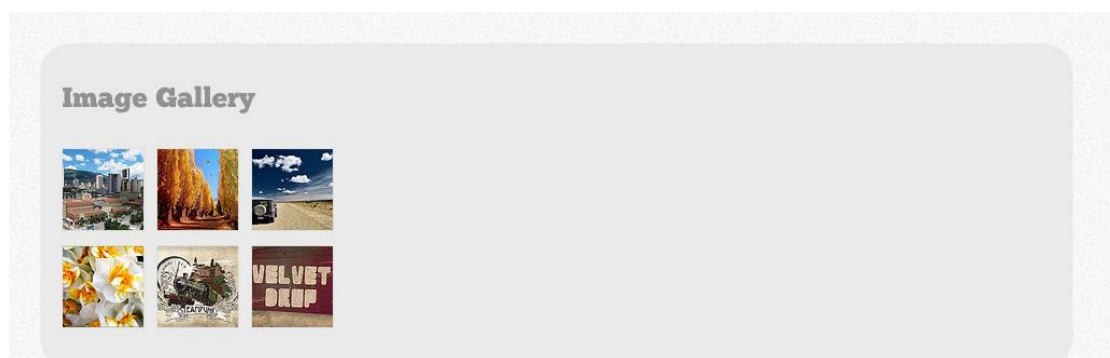
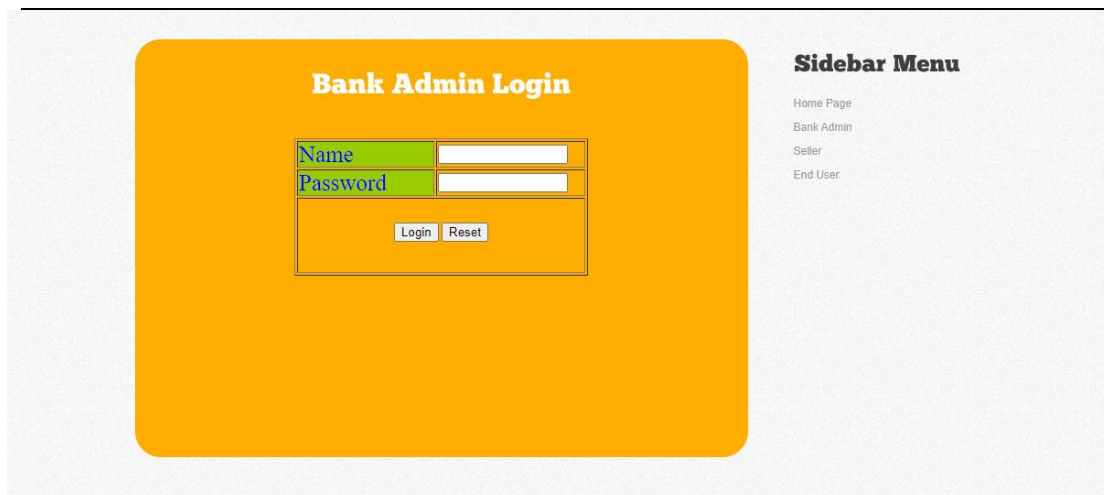
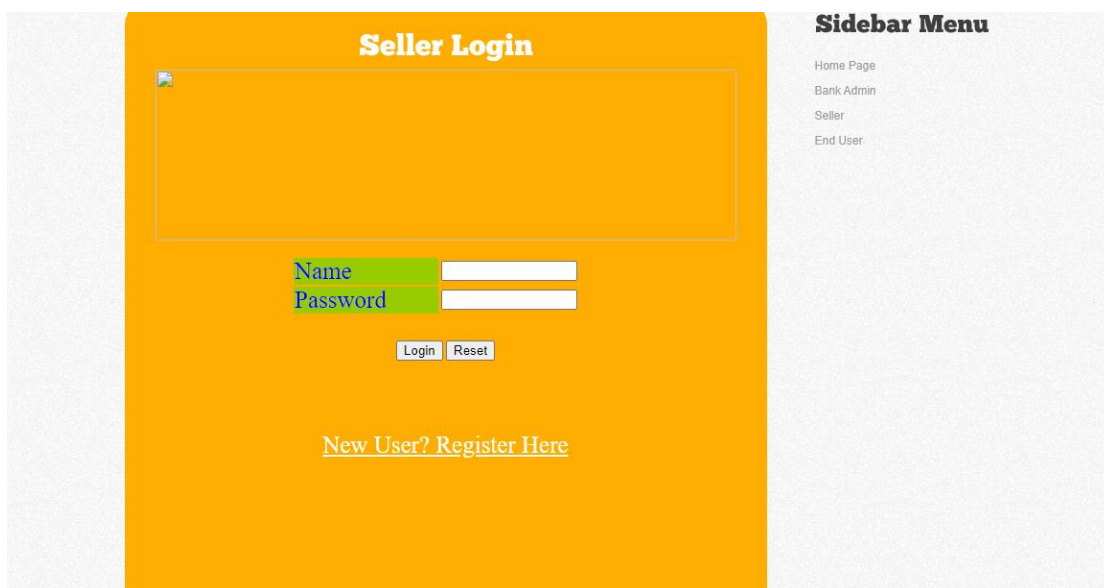


Fig: 1.3 – Home Page



The image shows a web application interface for a Bank Admin Login. The main content area has a light blue background. On the left, there is a white rounded rectangle containing the title "Bank Admin Login" in bold black text. Below the title is a login form with two input fields: "Name" and "Password", both with light blue labels and white input boxes. Below these fields are two buttons: "Login" and "Reset". On the right side of the page, there is a "Sidebar Menu" with a list of links: "Home Page", "Bank Admin", "Seller", and "End User".

Fig: 2 – Admin Login Screen



The image shows a web application interface for a Seller Login. The main content area has a light blue background. On the left, there is a white rounded rectangle containing the title "Seller Login" in bold black text. Below the title is a large white rectangular placeholder for a profile picture. Below this is a login form with two input fields: "Name" and "Password", both with light blue labels and white input boxes. Below these fields are two buttons: "Login" and "Reset". At the bottom of the white rectangle, there is a link: "New User? Register Here". On the right side of the page, there is a "Sidebar Menu" with a list of links: "Home Page", "Bank Admin", "Seller", and "End User".

Fig: 3 – Seller Login Page

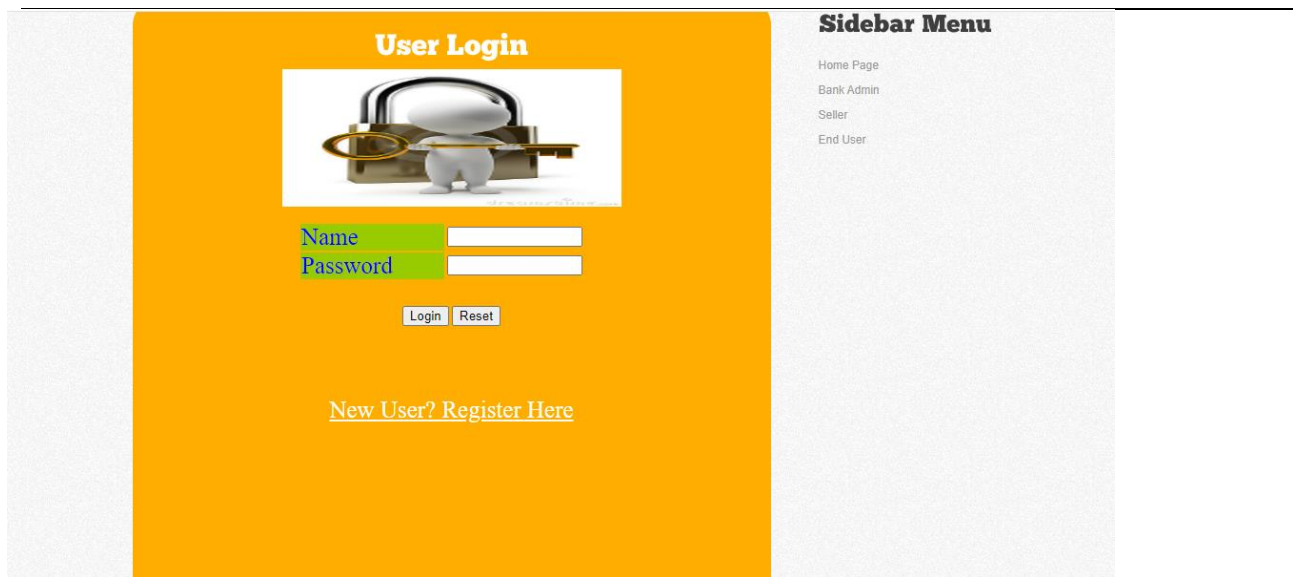


Fig: 4 – User Login Screen

6. CONCLUSION AND FUTURE WORK

CONCLUSION

This paper presents a novel system, *ProGuard*, to automatically detect malicious OSN accounts that participate in online promotion events. *ProGuard* leverages three categories of features including general behavior, virtual-currency collection, and virtual-currency usage. Experimental results based on labelled data collected from Tencent QQ, a global leading OSN company, have demonstrated the detection accuracy of *ProGuard*, which has achieved a high detection rate of 96.67% given an extremely low false positive rate of 0.3%.

7. REFERENCES

- [1] Y. Wang and S. D. Mainwaring, "Human-currency interaction: Learning from virtual currency use in China," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2008, pp. 25_28.
- [2] J. S. Gans and H. Halaburda, "Some economics of private digital currency," Rotman School Manage., Toronto, ON, Canada, Tech.Rep. 2297296, 2013.
- [3] X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in *Proc. 28th AAAI Conf. Artif. Intell.*, 2014, pp. 59_65.
- [4] X. Hu, J. Tang, and H. Liu, "Leveraging knowledge across media for spammer detection in microblogging," in *Proc. 37th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr.*, 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 Trans. Depend. Sec. Comput.*, vol. 9, no. 6, pp. 811_824, Nov. 2012.

-
- [6] Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog orblock: Detecting blog bots through behavioral biometrics," *Comput. Netw.*, 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 *Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2015, pp. 1769_1778.
- [8] Y.-R. Chen and H.-H. Chen, "Opinion spammer detection in Web forum," in *Proc. 38th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr.*, 2015, pp. 759_762.1998 VOLUME 5, 2017Y. Zhou *et al.*: *ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions*
- [9] F.Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in microblogging with social context regularization," in *Proc.24th ACM Int. Conf. Inf. Knowl. Manag.*, 2015, pp. 1601_1610.
- [10] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering," *Inf. Sci.*, vol. 260, pp. 64_73, Sep. 2014.