ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.4

Fake Detection on Social Network Accounts Based on Image Watermarking

R.priyanka[1], R.sandhya sharma[2], J.yamini[3], C.S.Anita[4]
B.Tech Student[1, 2, 3], Assistant Professor[4]
Department of Computer Science and Engineering
R.M.D Engineering College, Anna University, Chennai, Tamilnadu, India

Abstract:
On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Well known sites such as Facebook, LinkedIn, Twitter, and Google+ have millions of users across the globe. With the wide popularity there are lot of security and privacy threats to the users of Online Social Networks (OSN) such as breach of privacy, viral marketing, structural attacks, malware attacks and Profile Cloning. Social Networks have permitted people have their own virtual identities which they use to interact with other online users. It is also completely possible and not uncommon for a user to have more than one online profile or even a completely different anonymous online identity. Sometimes it is needed to unmask the anonymity of certain profiles, or to identify two difference profiles as belonging to the same user. Entity Resolution (ER) is the task of matching two different online profiles potentially from social networks. Solving ER has a identification of fake profiles. Our solution compares profiles based similar attributes. The system was tasked with matching two profiles that were in a pool of extremely similar profiles.

I. INTRODUCTION

Social Networks have permitted people have their own virtual identities which they use to interact with other online users. Social networks such as Facebook, Twitter and Google+ have attracted millions of users. One of the most widely used social networks, Facebook, recently had an initial public offering, which was among the biggest in Internet technology. These social networks allow real world people to create online profiles based on the information they give. The profiles are online identities that are capable of being totally independent of their real life identity. The interaction between these profiles happens through direct communication with other users, publishing posts and pictures, expressing opinions on other people's content, etc. Each profile can be seen as a node on a graph and the friendship relations between profiles are the vertices, hence the term social network. Such profiles are created during the registration process. Since the registration process for the average social network requires the user to manually enter their information it is very easy and not an uncommon occurrence to create a profile with fake or erroneous information. It could be to the interest of multiple parties to acquire the public information of these profiles from different social networks to correlate and match data in order to identify a single entity with different profiles. This process of matching profiles into a single entity representing one real world entity is known as Entity Resolution. ER also has real world uses such as the construction of a more detailed source of information on people, searching for people across different social networks, employers being able to know their employee candidates more before hiring them, improving marketing strategies, detecting fake profiles, etc. we present an alternative form of comparing profiles that takes advantage of other information that is available, without using training phase. To solve ER, we went farther than just comparing image based features between profiles; we also compared other types of information if it was publically available. Image based features such as the profile's images and posted images were compared with string comparison methods that obtain best results.

II. LITERATURE SURVEY

TITLE: 1 DESIGN AND EVALUATION OF A REAL-TIME URL SPAM FILTERING SERVICE

AUTHORS: Kurt Thomas, Chris Griery, Justin Ma, Vern Paxsony, Dawn Song

YEAR:2011

DISCRIPTION:
On the heels of the widespread adoption of web services such as social networks and URL shorteners, scams, phishing, and malware have become regular threats. Despite extensive research, email-based spam filtering techniques generally fall short for protecting other web services. a real-time system that crawls URLs as they are submitted to web services and determines whether the URLs direct to spam. We evaluate the viability of Monarch and the fundamental challenges that arise due to the diversity of web service spam. The Internet has seen a massive proliferation of web services, including social networks, video sharing sites, blogs, and consumer review pages that draw in hundreds of millions of viewers. On the heels of the widespread adoption of these services, phishing, malware, and scams have become a regular threat. While email spam has been extensively researched, many of the solutions fail to apply to web services. In particular, recent work has shown that domain and IP blacklists currently in use by social network operators and by URL shortening services perform too slowly (high latency for listing) and in accurately for use in web services. By restricting our analysis to URLs, Monarch can provide spam protection regardless of the context in which a URL appears, or the account from which it originates. This gives rise to the notion of spam URL filtering as a service. Email spam provides little insight into the properties of Twitter spammers, while the reverse is also true. We explored the distinctions between email and Twitter spam, including the overlap of spam features, the persistence of features over time, and the abuse of generic redirectors and public web hosting

MERITS:

- It provides fine-grained decisions that allow services to filter individual messages posted by users; but functions in a manner generalizable to many forms of web services

DEMERITS:

- The IP address of spam infrastructure achieves much less accuracy.

EXISTING SYSTEM

- As a user of an Online Social Network one should always see to it that his/her profile is safe and has not been cloned by anyone

- For detecting cloned profiles, we have designed a mechanism using which we can find whether the profile of a user is cloned as well as is their presence of fake profile of the user.

- This strategy succeeds most of the time and sometimes may not as there are many users having similar credentials. The User's profile is analyzed to search for rare pieces of information. This information may be specific to a particular user. The user credentials like name of the user, profile photo, Education details, workplace etc. are used to identify the particular use.

- A comparison is made between the original profile and the searched record and after the comparison a similarity Index is calculated.

- Profile photo is having very important role in the process to verify the cloned profile.

PROPOSED SYSTEM

- We designed mechanisms to detect the same site profile cloning profile cloning. This mechanism also detects the Fake profile if it is present in the site.

- We propose a technique using steganography in which we add an id to the profile and posted pictures which the id will be an email id of the user which is added to the image while uploading.

- The images downloaded from fake profile users and uploaded it when the notification alert sends to the original users.

- If the original profile user gives the permission when the picture was uploaded otherwise it was blocked.

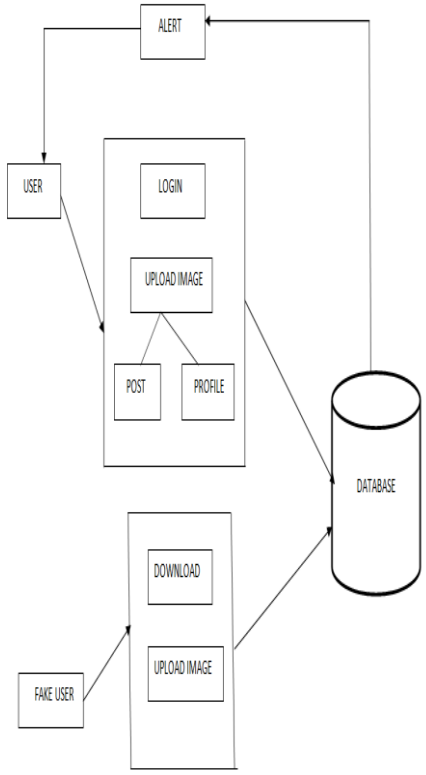
HARDWARE REQUIREMENTS

- Processor : Pentium IV
- RAM : 2 GB
- Hard Disk : 10GB

SOFTWARE REQUIREMENTS

- Platform : JDK 1.7
- Front End : JAVA (Servlet,JSP)
- Back End : MySQL
- IDE : Net Beans 7.3.1
- Operating System : Microsoft Windows 7

III. ARCHITECTURE DIAGRAM



IV. MODULES

- Login
- Hide data
- Profile Matching
- Altered Profiles

LOGIN:

The Login Form module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on your website. Which additional resources they will have access to can be configured separately. Once logged in, the Login Form module presents the user with a Logout button. Logged in users who are inactive for a predetermined period of time will be automatically logged out. The Login Form module will appear in whatever module position it is assigned to in the current template. It is also possible to have a Login Form that will appear in place of regular content when a Menu Item is clicked.

HIDE DATA

In this module, it consists of a new stenographic algorithm for hiding data in images. Here we have also used a Steganography algorithm. Steganography is the practice of hiding secret message within any media. Most data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. Here we have tested few images with different sizes of data to be hidden and concluded that the resulting steno images do not have any noticeable changes. In this module, the concern user who uploads the image will have an id that will be hidden within the image. Once another user

who downloads the image cannot see the image as it is hidden. We have also used water mark techniques that will not be visible even for the users. Steganography technique finds its main application in the field of secret communication. The main advantage of this algorithm is to keep the size of the cover image constant while the secret message increased in size. It can be used by intelligence agencies across the world .Hence this new stenographic approach is robust and very efficient for hiding data in images.

PROFILE MATCHING:

In this module, If the user who uploads the entire image can be viewed by the another user. The another user can downloaded the image but they cannot upload the same image this can be checked by the hidden id. The profile will be checked if the third party who upload the same image, this will be checked by the database. If the profile matches with the another profile, the another user cannot upload the same it consists of a new stenographic algorithm for hiding data in images. Another user can, Use the Image or else can upload the Image internal entry criteria matching system that checks for a primary match based on hard-coded, Already some data inside is there are not check. This profile matching module will check if another user who uploads the image which is in exists with the another user. There by this can avoids the fake user.

ALERTED PROFILES:

If the profiles match, then the concern user will be alerted by the alert message. The user will be notified as their profile image has be tried to upload by the another user and the user can block the person or else allow its user wish. User will also be notified with the fake users name, mail id, uploaded image, uploading time and system MAC Address. criteria match fails, no further weighing point match is attempted and the profile is either created newly or rejected based on parameter settings for this interface ID in fake profile. So finally give a some. Alert Message to the original User.

IV. CONCLUSIONS

We solved Entity Resolution with our system and used it to compare online user profiles from social networks in order to identify matches. Our systems are comparing the two images and identify that fake or not. We are using Steganography Algorithm and that algorithm hides the information inside the image. In this way new images upload in our profile and that image compare to existing user profile. If the image is fake when send notification to original user. The original user allows the uploading notification that images was uploaded otherwise blocked.

V. REFERENCES

[1]. K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and Evaluation of a Real-Time URL Spam Filtering Service," in IEEE Symposium on Security and Privacy, 2011.

[2]. W. Xu, F. Zhang, and S. Zhu, "Toward worm detection in online social networks," in Annual Computer Security Applications Conference (ACSAC), 2010.

[3]. C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in ACM Conference on Computer and Communications Security (CCS), 2010.

[4]. F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting Spammers on Twitter," in Conference on Email and Anti-Spam (CEAS), 2010 Computer and Communications Security (CCS), 2010.

[5]. G. Stringhini, C. Kruegel, and G. Vigna, "Detecting Spammers on Social Networks," in Annual Computer Security Applications Conference (ACSAC), 2010.

[6]. T. Jagatic, N. Johnson, M. Jakobsson, and T. Jagatif, "Social Phishing," Comm. ACM, vol. 50, no. 10, pp. 94–100, 2007.

[7]. K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots + machine learning," in International ACM SIGIR Conference on Research and Development in Information Retrieval, 2010.

[8]. H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards Online Spam Filtering in Social Networks," in Symposium on Network and Distributed System Security (NDSS), 2012.

[9]. S. Lee and J. Kim, "WarningBird: Detecting Suspicious URLs in Twitter Stream," in Symposium on Network and Distributed System Security (NDSS), 2012.

[10]. M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Compa: Detecting compromised accounts on social networks," in Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, February 2013.