Available online at: https://ijact.in

Date of Submission	06/10/2018
Date of Acceptance	22/10/2018
Date of Publication	31/10/2018
Page numbers	2826-2830 (5 Pages)

ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

PREVENTION TECHNIQUE FOR CREATING FAKE PROFILES AND ACCOUNTS ON WEBSITES

Dr. Adiline Macriga G
Department of Information Technology, Sri Sai Ram Engineering College
adiline.it@sairam.edu.in

Abstract: At present, the social life of everyone has become associated with the online social networks. Also, every online business is linked to users through websites. Users are allowed to create separate personal or official accounts in order to access these websites. The rapid growth of these websites despite being advantageous, it also causes some serious issues. Problems such as fake profiles, online impersonation have become prone these days. The most important issue is that, the websites maintains separate servers with storage area for all the users. Creation of number of accounts by a single user leads to occupying extra storage space in those servers which causes wastage of storage resources. The fake profiles and online impersonation issues are becoming threat to several people like celebrities, businessmen and even to innocent general public. In order to restrict these problems, an idea is suggested to prove the uniqueness of users in these websites and restrict them to create limited number of accounts permitted by the website holders. Like Aadhar in India, most of the countries has unique id and has become mandate. This id's has an advantage of giving uniqueness to every individual. The user's Aadhar card/unique card can be scanned to generate a unique id. Using this unique id, the individuality of users in websites can be identified and a unique username and password can be given to each user. Whenever a user tries to create an account in a registered website, the user will be asked to prove uniqueness and hence can be restricted from creating multiple accounts more than the number of accounts allowed by the website.

Keywords: Social engineering; Unique Identity; Fake Profiles; Multiple accounts; Aadhar card

I. INTRODUCTION

In present era social media has become one of the important medium for communication and for expressing thoughts and even for the business purposes. There are various technological tools in social media which tries to avert users in restricting multiple account creation but fails to reach at an effective solution. Online impersonation almost finds its way impossible to intrude into other person's account without his/her consent. There are various algorithms which are being researched for helping out peoples to ensure security. They also provide number of solutions in averting fake profile creation but these tools makeup a huge sum of money and failed to impress the users.

The existing system uses Naïve Bayes and Decision Tree to classify the legitimate account users and fake account users. The problem with the existing technique is the accuracy. It may give 'false positives' at times and in some cases original account user may be reported as false account holder, if there is even slight anonymity in the behaviour and may end up in losing the original account. The proposed technique of multiple account restrictors in website help the users in a better way as it is the tool which is compact and user-friendly. The one-time registration of users in unique app ensures that the user never violates the policies of the various social media accounts and gives an assurance to the users about the trust worthiness of others holding the accounts to be genuine.

II. Problem Statement

The data-centres that store and process everything from old e-mails and facebook data to tweets, Google searches, and e-commerce transactions suck up two percent of the nation's entire electricity supply. Worse, upwards of 90 percent of that energy is simply wasted. A McKinsey & Company report that the average data-centre uses just six to twelve percent of its electricity for actual computation. Online companies keep their facilities running at maximum capacity round the clock, whatever the demand. This is not sustainable in the long term. Fig 1.1 shows the sample server storage which consumes watts of energy even to run on idle.

Fig 1.1 Storage Wastage

III. Literature Review

Social Engineering in terms of security means the art of stealing confidential information or gaining access to some computer system mostly not by using technical skills but by manipulating people themselves in divulging information.

The social engineering techniques are like Pre_texting, Diversion theft, phishing, baiting, quid pro quo, tailgating, etc.

Examples:

1. Creating a fake profile:

Creating a profile of some person X, by getting information from some online social networking site like Facebook. Adding the friends of the X in Facebook and making them believe that it is the profilele of X. They can get the private information meant for only X by communicating with Xs friends in Facebook.

2. Online impersonation to defame a person:

The other reason why people create fake profiles is to defame the persons they do not like. People create profiles in the name of the people they don’t like and post abusive posts and pictures on their profiles misleading everyone to think that the person is bad and thus defaming the person.

3. Social Bots:

Social bots are semi-automatic or automatic computer programs that replicate the human behavior in Orbit Showtime Network (OSN). These are used mostly by hackers now-a-days to attack online social networks. These are mostly used for advertising, campaigning purposes and to steal user’s personal data in a large scale.

These social bots communicate with each other and are controlled by a program called botmaster. The botmaster may or may not have inputs from a human attacker. The social bots look like human profiles with a randomly chosen human name, randomly chosen human profile picture and the profile information posted randomly from a list prepared from before by the attacker. These social bots send requests to random users from a list. When someone accepts the request, they send requests to the friends of the user who accepted the request, which increases the acceptance rate due to existence of mutual friends.

Recently a researcher made a social botnet of 103 bots in Facebook and added 3000 friends in just eight weeks. He was able to extract around 250 GB of personal data of users. This shows the extent of the applications of social bots by the attackers.

4. Facebook imune system

When we consider Facebook, it has its own security system to protect its users from spamming, phishing, etc. and this is called Facebook immune system (FIS). FIS does real time checks on every single click and every read and write operation done by it. This is around 25 Billion checks per day and as high as 620,000 checks per minute at peak as of May, 2011

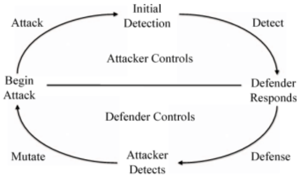


Fig. 1.2 The Adversarial Cycle

IV. System Analysis

4.1 Automatic Detection of Fake Profiles in Online Social Networks

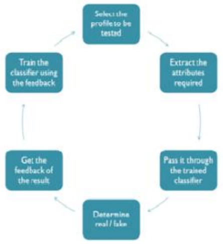

Select the profile to be tested
Extract the attributes required
Pass it through the trained classifier
Determine real / fake
Get the feedback of the result
Train the classifier using the feedback

Fig. 1.3 Framework for detection of fake profiles and learning

The proposed framework in the fig. 1.3 shows the sequence of processes that need to be followed for continuous detection of fake profiles with active learning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by the social networking companies.

1. The detection process starts with the selection of the profile that needs to be tested.
2. After selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.
3. The attributes extracted is passed to the trained classifier. The classifier gets trained regularly as new training data is feed into the classifier.
4. The classifier determines whether the profile is fake or real.
5. The classifier may not be 100% accurate in classifying the profile so; the feedback of the result is given back to the classifier.

For example, if the profile is identified as fake, social networking site can send notification to the profile to submit identification. If the valid identification is given, feedback is sent to the classifier that the profile was not fake.

6. This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles. Fig. 1.4 explains the concept.

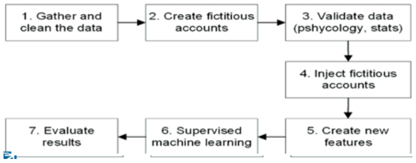

1. Gather and clean the data
2. Create fictitious accounts
3. Validate data (pshycology, stats)
4. Inject fictitious accounts
5. Create new features
6. Supervised machine learning
7. Evaluate results

Figure 1.4: Research Steps

4.2 Finding Deceptive Accounts

The process of identifying the deceptive accounts is managed by humans using the training data technique. Here the data or information is collected as raw data. This raw data is cleaned, mined and the stored in a database. Then it is applied to supervised machine learning models for training. The trained data is verified for its effectiveness.

The following metrics are followed to evaluate the effectiveness of each model.

Accuracy–From the trained data the fake and correct accounts are identified and verified.

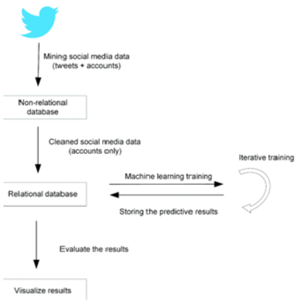

Mining social media data (tweets + accounts)
Non-relational database
Cleaned social media data (accounts only)
Iterative training
Machine learning training
Relational database
Storing the predictive results
Evaluate the results
Visualize results

Fig. 1.5 The flow of data to detect identity deception

V. PROPOSED SYSTEM

The multiple accounts preventer mainly aims to curb the creation of account creation beyond the bound limit which is specified. This also ensures that there is zero possibility of creation of fake profiles and even the person involved in impersonation may easily caught hold. This also mainly ensures that the storage space in servers are also not wasted which may use for new account holders thereby ensuring space optimization.

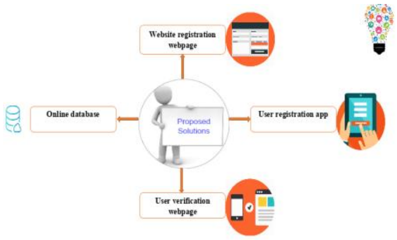
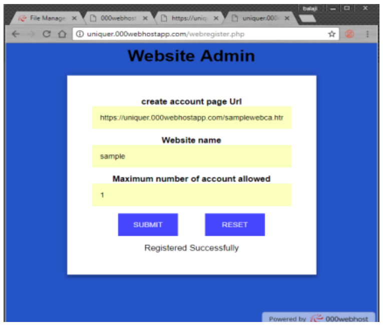


Fig.1.7: Proposed Solution

The website holder registers the website along with maximum number of accounts a user can hold. Database will be updated with a column value as the website URL and rows as maximum number of accounts. The user registers him/her through the app by scanning his Aadhar card and giving unique username and password and also mobile number. If already registered then another account cannot be created through that app. When a user clicks create account from that website, he will be redirected to unique identifier page where he has to enter his unique username and password. The username and password are checked in the database. If available, the maximum number of accounts available will be checked and if it is greater than 0 then he will be redirected back to the create account page of that website. If the maximum number of accounts count is 0, then he cannot create another account in that website. If username is not available, he has to create his unique account through the app to proceed creating account in that website.

1. **Website registration webpage** is for the website owner to register his website URL and maximum accounts a user can have in that website.



Website Admin

create account page Url

https://uniquer.000webhostapp.com/samplewebca.htr

Website name

sample

Maximum number of account allowed

1

Registered Successfully

Fig. 1.8: User Verification webpage

2. User registration app scans Aadhar card of user and gets unique username, password and mobile number from the user and registers those information to the database.

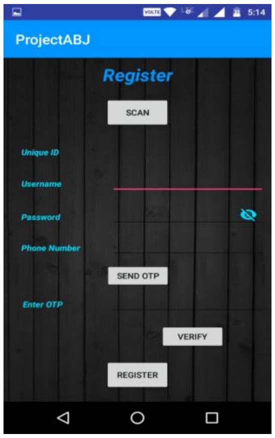
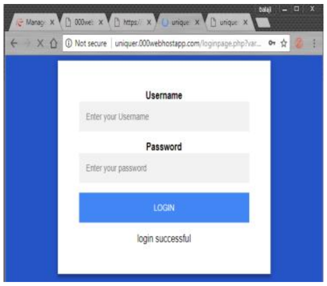


Fig. 1.9: Unique Identifier Page

3. User verification webpage (fig. 1.8) verifies the registered users username and password from the database before creating an account in the registered website.



login successful

Fig. 1.10 Login Page

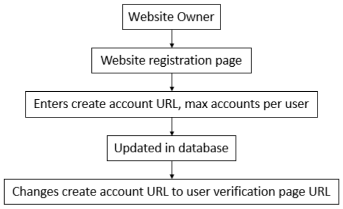
VI. Operation & Technical Feasibility Study

The website holder registers the website along with maximum number of accounts a user can hold. Database will be updated with a column value as the website URL and rows as maximum number of accounts. The user registers himself through the app by scanning his/her Aadhar card and giving unique username and password and also mobile number. If already registered then another account cannot be created through that app. When a user clicks create account from that website, he will be redirected to unique identifier page (fig. 1.9) where he has to enter his unique username and password. The username and password are checked in the database. If available, the maximum number of accounts available will be checked and if it is greater than zero then he will be redirected back to the create account page of that website. If the maximum number of accounts count is 0, then he cannot create another account in that website. If username is not available, he has to create his unique account through the app to proceed creating account (fig.1.10) in that website.

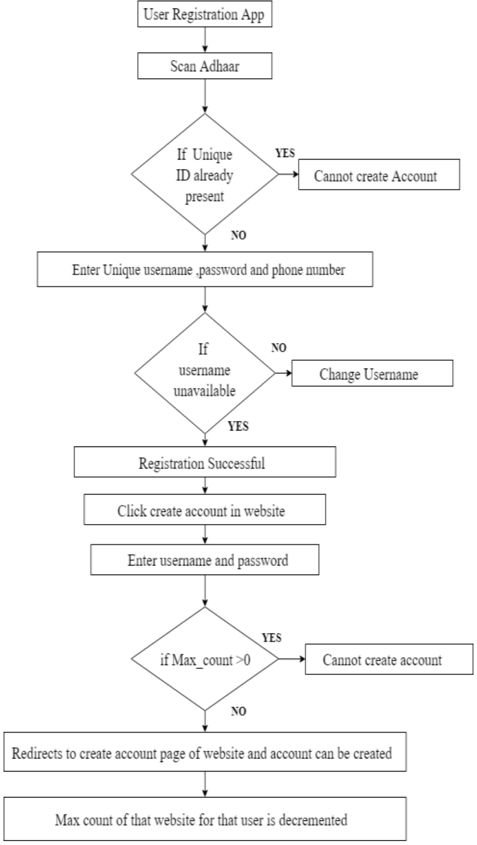
Feasibility Study:

Since Aadhar card is issued to every individual of India and same way unique id's are issued for different countries, it will be easy and feasible to use that as a unique identifier of individual users. If any website desires to avoid multiple accounts from same user it can use this project to register itself and avoid those problems. Any website can register itself and get benefitted from this. It is simple and easy to implement but very efficient. For this project purpose, we have generated a unique id from the Aadhar number scanned from Aadhar card of the user because storing of Aadhar number directly in databases is illegal based on Aadhar law of India.

Website Admin Flow diagram:


Website Owner
Website registration page
Enters create account URL, max accounts per user
Updated in database
Changes create account URL to user verification page URL

User Flow diagram:


User Registration App
Scan Adhaar
If Unique ID already present
YES
Cannot create Account
NO
Enter Unique username ,password and phone number
If username unavailable
NO
Change Username
YES
Registration Successful
Click create account in website
Enter username and password
if Max_count >0
YES
Cannot create account
NO
Redirects to create account page of website and account can be created
Max count of that website for that user is decremented

VII. Conclusion

The proposed system cannot confirm to the credibility of the user and so in our methodology we can restrict the unauthorised persons to pertain the creation of fake account and use them. This is possible only if the websites care about this issue of multiple fake accounts and are willing to bring a solution to it. This proposed system does not allow any user to create new multiple accounts but already available multiple accounts are not identified. The future enhancement will be based on providing uniqueness in current available accounts. Also age restriction can be provided for users for some web sites that require age authorization.

VIII. References

[1] T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems, SNS, volume 11, page 8, 2011.

[2] C. Wagner, S. Mitter, C. K ̈orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. In Proceedings of the WWW, volume 12, 2012.

[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93–102. ACM, 2011.

[4] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21–30. ACM, 2010.

[5] Estee Van Der Walt. T and Jan Eloff, Using Machine Learning to Detect Fake identities: Bots vs Human, Department of Computer Science, University of Pretoria, South Africa.