Content Filtering on Social Networking Sites with Fuzzy Logic

Prof. G. N. Purohit
(Dean, AIM & ACT), Banasthali University,
Jaipur, Rajasthan, India

Dr. Priti Singh
(HOD, ECE), Amity University,
Gurgaon, Haryana, India

Praveen Dangi
(Ph.D*) Banasthali University,
Jaipur, Rajasthan, India

DOI: 10.23956/ijarcsse/V7I6/0264

Abstract: Social Networking Sites (SNSs) provide an online platform that is used by people to build social networks or social relations with other people. Many users are not aware of the hidden threats to privacy that exist while using these SNSs. There has been a growing concern regarding these threats in general and among researchers in particular. The present study is a novel attempt to devise a measure to overcome these threats using fuzzy logic and IDPS(Intrusion Detection and Prevention System). This study is helpful in achieving twin objectives -(i) establishing through survey and fuzzy logic, that people are aware of the potential threats in using SNSs and (ii) helping them in securing their accounts by using the IDPS technique. Thus, it is hoped that the current study will be useful to society at large in providing more secure social networking sites.

KeyWords: Social Networking Sites, Security, Privacy, IDPS(Intrusion Detection and Prevention System), Fuzzy Logic.

I. CONTENT FILTERING OF SNS

Content Filtering is the technique which is used to block the contents rather than its source or other criteria. It is most used to filter the email and web access on the internet. Corporations and home computer owners used the content filtering as an Internet Firewall. Some of the famous social networking sites are Facebook, Twitter, LinkedIn, YouTube etc.

1. Risks in Sharing Information with SNS

Viruses: Due to popularity of social networking sites the services provide for them makes easier for the attackers to target those services without less effort.

Tools: The attacker could then access the user’s private data and the data for any contacts that share their information with that user.

Third-party applications: Some social networking services may allow you to add “third-party applications, including games and quizzes, which provide additional functionality.

II. EXISTING TECHNIQUES

It was seen that the techniques and methods proposed by existing studies have some drawbacks. The steganography technique was proposed which is based on the Least significant bit. The Proposed solution protects against spear phishing attack by the use of “SiteKey authentication but SiteKey is ineffective if the users are not properly educated against the phishing attacks and security image attack”. The major drawback of Trustbook is that current social network providers lack mechanisms of determining the authenticity of an account.

So, it was therefore thought of developing some new method to use SNS safely and to provide safety features for using SNS. The main objective of the proposed research are:

- To protects privacy, personal information and provides other related safety features, while using SNS.
- Further to develop measures that can secure the SNSs from hackers and fake users.

Many kinds of attacks are possible on SNS. The major attacks on SNS are characterized as : (i) Uploading Fake profile on Social Networking Sites, (ii) Uploading fake Photos on Social Networking Sites, (iii) Hacking by Unauthorized users, (iv) Third party applications, (v) Users permissions on Social Networking Sites, (vi) Difficult to understand privacy policies on Social Networking Sites, (vii) Misuse of Mobile Network, (viii) Location Based Application.

We discuss each attack in detail in this research.

III. RESOLVING SOME ISSUES IN SNS

The present study provides a more concrete way of finding out the fakeness in relation to selected eight problems. These eight issues have been identified and each questions have eight parts.

3.1. Uploading Fake Profile

Social networking sites also has many fake profiles like other social networks. To attack innocent people fake profile holders use Social Engineering tactics. Facebook has almost 500 Million Users and it is not surprising to have few thousands fake profiles.

RQA. How to identify a fake profile Account on Social Networking Sites?

RA1. If the user hasn’t updated a status for quite a long time. Does it mean the profile is fake?
RA2. Can it be said that the Fake profile of users portraying as girls usually have a contact number in their information?
RA3. If there is only one photo of the individual in the whole profile, does it mean that the account is fake?
RA4. If the user has just been adding people randomly and making them friends, and there are no pages liked or any groups joined. Does it mean that the profile is fake?
RA5. If maximum number of friends are of the opposite gender, can it be assumed that the profile is fake and is used just for casual fun without any social networking aspect?
RA6. If in a user profile, there are no ideal links regarding school or education institutions or workplace, does it mean that profile is fake?
RA7. If there are no local friends added in the profile, does it mean that the profile is fake?
RA8. If someone has a group of friends interacting with each other and vouching for their claims, does it mean the profile is real?
*RA stands for response to question A

3.2. Uploading Fake Photos
In Twitter and Photoshop images are edited, then it can be uploaded and share misleading photos or videos on SNS. It can misrepresented your identity, stolen intellectual property and possibly committed identity theft.

RQB. How to figure out the fake photos on SNS?
RB1. You will consider place, date and approximate time to determine fake photo.
RB2. The fake profiles photos are open to everyone.
RB3. If the photograph is altered by hacker, you will consider the accuracy of the image like weather conditions, background and the position of the sun at the time of the event.
RB4. If the photograph is altered then observe colour consistency and whether different parts of the human body having the same skin colour, is to be checked.
RB5. The Image manipulation often requires filling areas to replace removed objects.
RB6. Hackers can steal a lot of pictures from someone else’s profile, will it be hard for them to tag all the people.
RB7. If the image is manipulated then examination of the light and shadows of similar of objects in the photograph is to be ascertained.
RB8. Is it correct to say that the photos of celebrities used by people in Social Networking Sites are fake?
*RB stand for response to question B

3.3. Unauthorized Users Hack Personal Information
Hacking personal information means to change or destroy information by installing dangerous malware without user’s knowledge, by computers hackers or unauthorized users.

RQC. The unauthorised users are hacking the personal information and damaging the sensitive data.
RC1. This is possible if the email account, mails are marked as read, trash or permanently deleted without persons notice and forwarded to a third party email address without person’s consent.
RC2. The multiple unsuccessful login attempts from another computer suggest that the account has been hacked.
RC3. The application and system logs on a windows computer are corrupt, it implies that an attempt has been made to change the log files.
RC4. Does the unexplained modifications of users personal file storage suggest hacking?
RC5. If one or more systems start behaving erratically, does it mean that hacking exploits are being run on them?
RC6. The sudden deterioration in performance, corruption of data or new windows unexpectedly popping up suggests hacking.
RC7. Repeated lock outs in a single user account indicate password guessing attempts.
RC8. Activity by hackers will change the time and data stamps of files in various directories of affected computer.
*RC stands for response to question C

3.4. Third Party Applications
In addition, third-party sites can rapidly distribute their services via social-networking sites to keep in touch with users while they are on these sites.Sometimes using a relatively unknown software may minimize the risk of hacking.

RQD. Does the third party applications are safe for users on SNS?
RD1. A Third Party application includes the social network’s privacy policy.
RD2. The Social Networking Sites take responsibility of Third Party Application to be secure.
RD3. The Social networks take the responsibility of Third-Party Applications interacting with their sites.
RD4. Does the tracking sites track the online activity through Third Party Application?
RD5. The Third Party Applications are designed only to gather information about users.
RD6. The Third Party Application contain malware designed to attack the user’s computer.
RD7. The Third-party developer report users’ actions back to the social networking platform.
RD8. Some social networks have agreements with certain websites and applications that allow them the access to personal information of all users of the social network.
*RD stands for response to question D
3.5. Users Permission
User permission in social networking sites is very important to control or access their own data. Users have the right to block the person who is secretly extracting their personal information from the profile.

RQE. Does a user has access to any application without the permission of SNS?
RE1. A user chooses to post information as “public” without restricting access through available privacy settings.
RE2. A user has an option to change the privacy settings to make the information “private” so that only approved users can view it.
RE3. A social network change its privacy policy at any time without the permission of the user.
RE4. Approved contacts copy and repost information including photos without a user’s permission, potentially bypassing privacy settings.
RE5. Can a Third-party Application that has been granted access, is able to view information of a user or users contact, post privately.
RE6. The Social networks guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private.
RE7. A user has the discretion to permit or to deny any permission.
RE8. A malicious software is placed in a computer without the knowledge of the owner for harassing individuals, or to infect computers.
*RE stands for response to question E

3.6. Issues in Understanding Privacy Policies
When people join any social networking site they skip the privacy policy. Some privacy policies are very long and difficult to understand. Many times users do not read out the privacy policy because the SNS do not have clear statements, so it’s very difficult to understand them.

RQF. Is the Privacy Policy of SNS is difficult to understand for users.
RF1. The Privacy Policy of a Social Networking Site can be easily located on the homepage.
RF2. The language of the Privacy Policy seem excessively vague or incomprehensible.
RF3. The privacy policy mentions only, what happens to personal information if a user dies?
RF4. The marketers use the data posted by the users without their explicit consent.
RF5. A Privacy Policy mentions the grievance redressal mechanism when the user gets the response from the site via the email or the phone number mentioned therein, when the user interacts for some grievance resolution.
RF6. A Social Network sites notify users about changes in the Privacy Policy and the same is communicated properly to the user personally on email as well as on the homepage of the site.
RF7. The Privacy Policy of a Social Networking Site discloses about the certification of third party applications, which always respect user’s privacy and security.
RF8. The Social Networking Sites always mention the important portions of a privacy policy at the very end.
*RF stands for response to question F

3.7. Misuse through Mobile Network
Today mostly users use their mobile phones and access Internet services. For mobile users it is very difficult for them to know where and how their information is used and who is authorised to use it.

RQG. Mobile Network is misuse through malicious application.
RG1. When users opt a password or PIN, they often choose that can be determined or remembered easily. This increases the risk when phones are stolen or lost.
RG2. People are often unaware of the nature and extent to which their information is collected, since the apps are installed on smartphones.
RG3. Having too much dependence on a mobile device for the authentication protocol can lead to greater risk due to device theft.
RG4. The mobile devices firewalls can protect the user from the intruder, who obtains sensitive information and tries to misuse it.
RG5. The privacy gets compromised in e-commerce because of the risk involved in disclosing personal information such as email addresses, phone numbers or credit card information.
RG6. The Mobile consumer securely access the data via the social networking sites.
RG7. With the widespread use of mobile devices, highly accurate sensor data is collected and often shared without the user’s knowledge.
RG8. The hacker mishandles the bank account and get the PIN and other sensitive information on the SIM card through Internet Banking.
*RG stands for response to question G

3.8. Location based Application
Location-based social networks like Foursquare, Gowalla, Brightkite and Google Buzz are among the currently fastest growing new mobile services. These applications share the current location of the user. From these the user has to accept the risks.
So, the new ways of detecting fakeness are highlighted, which are different from the existing measures. These new ways will work as a basis for developing the practical methods for ascertaining, to be implemented in Java in order to detect fakeness.

RQH. Is it safe to use Location Based Application on SNS?
RH1. The tracking of user’s behaviour and details could be beneficial for creating targeted services tailored to the user needs and personalities.
RH2. The users sharing their location with the public on the networking sites invites chances of robbery and theft.
RH3. It is easy for hackers to locate potential victims through Location Based Application.
RH4. In most commercial location based services, the users have the ability to control their data.
RH5. Location Information also raises child safety concerns as more children access mobile devices and location-based services.
RH6. Criminals can use location data to steal identities when location data are disclosed, particularly when they are combined with other personal information.
RH7. Decentralized approaches create triggers, instead of relying on a centralized server.
RH8. User’s personal data are usually collected and stored differently across a multitude of services.
*RH stands for response to question H

IV. IMPLEMENTATION AND ANALYSIS

4.1. Introduction
Some issues have been raised and for each issues Eight Queries were identified. The answers of these queries are opinion based but they are not very crisp. It may vary from Absolutely False to Absolutely True. In this situation Fuzzy Approach is very suitable approach for their analysis. Even for using Fuzzy Logic approach two types of experimental work has been done. One is Machine based while the other one is based as usual survey based methods. Results can be obtained based on opinion of an individual. For the other method, a questionnaire was circulated among a sample size of 100 persons. For each question, it was decided to have only four possible answers from Respondents. These answers can be False, Partially True, True and Absolutely True. These four answers were given fuzzy numbers between 0 and 1 as provided in Table 4.1. From these allotted fuzzy numbers, it is easier to arrive to a conclusion.

<table>
<thead>
<tr>
<th>Possibilities</th>
<th>Fuzzy Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td>0.0 - 0.299</td>
</tr>
<tr>
<td>Absolutely False</td>
<td>0.299-0.499</td>
</tr>
<tr>
<td>Partially True</td>
<td>0.499 – 0.899</td>
</tr>
<tr>
<td>True</td>
<td>0.89 – 0.999</td>
</tr>
<tr>
<td>Absolutely true</td>
<td>0.99-1.000</td>
</tr>
</tbody>
</table>

4.2 Queries and Answers Fuzzification
While opting an opinion about any query there are possibly many types of answers for the sake of simplification, in this study these have been characterised as False, Partially True, True and Absolutely True. In the scale of fuzzy numbers between 0 and 1 these have been allotted numbers as given in Table 4.1. For the values between 0.0 to 0.299 the Fuzzy Possibility is False, for the values between 0.299 to 0.499 is Absolutely False, for the values between 0.499 to 0.899, the Fuzzy Possibility is Partially True for the values between 0.899 to 1.00, the Fuzzy Possibility is Absolutely True for the value 0.99-1.00.

In this work, users choose one possible condition according to their understanding, after that we calculate the Fuzzy possibility and find out the fakeness.

4.3. Data Collection
A survey was conducted using the questionnaire method to collect data regarding people’s perception about security and privacy of SNSs. In total there were 100 respondents. For each question there were eight responses. For each response there were four options i.e. Absolutely True, True, Partly True and False. Respondents were requires to tick one of the option according to their understanding. After collecting the data, section wise analysis of the questionnaire is done. On the basis of the values ticked by the respondents, average of all the 8 responses given by an individual in each section is calculated. On the basis of the average of each respondent, the Group average value is also calculated. From this the final possibility is ascertained. Since all the responses are converted into a value, the data analysis therefore confirms the validity of the questions that has been asked in each section.

So, after collecting the data from the respondents, average and group average was calculated and from group average, find the fuzzy possibility of each question. If the outcome is True, then it validates the issue that has been raised. However, if the final result is False, then it shows that issue raised is an erroneous issue.

V. SECURING SNSs BY IDPS
Social networking websites are not only to communicate or interact with other people but also an effective way for business promotion. The hackers can steal personal information of users of social network, upload fake photos and fake
profile, misuse of their mobile networks, and also other issues mentioned in previous chapter. To address these security issues, IDPS is used to stop malicious activities. The IDPS can be used to secure the data from attackers, as these can search out the malicious activity, block and stop it and report to the administrator. So IDPS is very helpful to secure the data and also provide security for SNS.

VI. FUTURE WORK
Social Networking sites can be secure by several methods. It is planned to use Soft Computing for prevention of attacks at run time without compromising network performance. It is hoped that SNS can be secured using ANN.

REFERENCES