National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Detection of Attacks in Online Social Networks (OSN)

Prof. Rajesh R M[1], Prof. Prathibha S. B. [2]
[1]Seshadripuram Degree College Tumkur, Karnataka, India
[2]Assistant Professor and HOD Seshadripuram Degree College Tumkur, Karnataka, India

ABSTRACT

Online Social Networks (OSN) attacks are most prevalent and practical attack that cannot be prevented easily. Due to increase in OSN population many users are exposed to many attacks. Attacker uses social media as a channel to launch the attacks. Due to this it is necessary to develop some mechanism to avoid the attacks. So it is essential to do the risk assessment in OSN by assigning the Risk Score to each user in OSN. Risk Score assignment is carried out in two ways. (i) One Phase Risk Assessment based on Group Identification features (ii) Two Phase Risk Assessment based on behaviour features mapping. After calculating the risk score users are categorized as below average (below normal), average (normal), and above average (Malicious) user.

Keywords : OSN Online Social Networks, Risk Assessment, Attacks.

I. INTRODUCTION

Online Social Networks (OSN) is growing field in computer world, it is growing like anything, and it allows users to create accounts in OSN and to share information to other users in the network around the world. OSN also allow user to create both private and public profile encouraging to post the images, videos etc. [1]. The first decade of the twenty first century has witnessed a tremendous growth in the field of communication and information technology, and the penetration of Internet in almost all aspect of our daily life. Within four decades of its introduction in a very crude form called UseNet in 1979, -the Internet has become an integral part of the modern society.

Though there are several popular applications on the web such as E-mail, games, videos, etc., none of these applications make users interested with the Internet the way social media do. The popularity of social media such as Facebook and Twitter has increased several folds in recent years. Social networking sites are attracting a large number of visitors. According to a report, by the Shareaholic website [2], the two social networking sites Facebook and Pinterest attracted over 20% of overall traffic over the Internet, where approximately 73% of adult Internet users access social networking sites as reported in September 2013 (https://blog.shareaholic.com/socialmedia- traffic-trends-01-2014/), and (http://www.pewinternet.org/fact- sheets/social-networkingfact-sheet/).

On social media sites such as Facebook and Twitter some of the users post or tweet and other users, whether- friends or followers may respond to posts by commenting, sharing or re-tweeting, which may be followed by others along the network. These activities constitute online user behaviour and generate a huge amount of data which may be useful in learning models of user behaviour, identifying communities of like-minded users, developing models to understand users' attitudes and predicting future activities of the same set of users. With the ever- increasing popularity of social media, better understanding of users' online behaviour has become critical for the success of many application development and business houses.

As the number of users on social networking sites is increasing rapidly, the amount of data generated by them are also growing very fast. The large amount of highly unstructured data generated by social media poses several challenges to research community in terms of storage, retrieval and mainly analysis. The analysis of user behaviour can be useful to all stakeholders of network traffic; for example, -to ISP providers in optimizing the traffic pattern, to social media sites to create applications as per user behaviour, and to users to understand the behaviour of normal users and malicious users. In order to design an effective model for using social media in teaching and education in general, this paper aims to analyse and model the user behaviour on social media.

In other words, social media is an online interactive platform where users can make online social networks, create contents, discuss and share views. As it is clear from the definition of the social media, users can express their views in different forms and formats. Accordingly, social media can be classified into different categories as described below:

Social Networks: Social network sites can be defined as web-based services that allow individuals to construct a public or semi- public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system [3].

Thus the social network websites allow users to connect with friends, colleagues and other users in order to share media, content and communications. Examples of social networks include Facebook, LinkedIn, and Myspace.

As a result, compromised accounts in Online Social Networks (OSNs) are more favourable than Sybil accounts to spammers and other malicious OSN attackers. Malicious parties exploit the well-established connections and trust relationships between the legitimate account owners and their friends, and efficiently distribute spam ads, phishing links, or malware, while avoiding being blocked by the service providers. Offline analyses of tweets and Facebook posts [4], [5] reveal that most spam are distributed via compromised accounts, instead of dedicated spam accounts.

Online social networks like Facebook, LinkedIn, Orkut and such others are vulnerable to various networking threats. One of the majors is Sybil attack, where attackers create and maintain many fake accounts, called Sybils to inject malwares. Since decade, many social- graph-based Sybil defences have been extensively discussed and proposed in the research community. The social-graph- based Sybil defences rely on multiple assumptions but the underlined truth lays strictly on the limited social connections known as attack edges which form between Sybil and non-sybil users. Here, upper bound of Sybil acceptance still depends on the total number of attack edges which shows that if there is increase in the attack edges then it will evade the Sybil detection. As a result, Sybils may be able to develop many attack edges to real users especially because of those few promiscuous non- sybils who are careless to befriending even with strangers. Existing social graph based detection schemes may show major performance drop while dealing with such kind of situation. To overcome such limitation of social graph based Sybil detection, here proposed its extension version by incorporating user behavioural aspects behaviour profile.

People using such services share tremendous amount of personal and sensitive information on such sites. As a result, these services become vulnerable to different kinds of privacy breaches and attacks where a malicious entity tries to steal user's sensitive information or tries to hack into such services and disrupt its normal working. It has been reported that around 10% of total users registered on popular social networking website Facebook are fake users which amounts to approximately 100 million registered profiles [6]. Also, news has emerged that millions of registered fake accounts were on sale in the market [7]. Rest of Paper is organised as follows. In module 2 discussed the work related to Attack detection techniques based on social graph and user profile behaviour and the attacks related to OSN. In module 3 proposed design is explained in detail. Module 4 discussed the design technique. In module 5 the evaluation factors are discussed.

II. LITERATURE SURVEY

Online Social Networks (OSNs) allow users to create a Public or private profile, encourage sharing information and interests with other users and communicating with Each other. As a result, today's social networks are exposed to many types of privacy and security attacks. Social media are computer-mediated technologies that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks. The variety of stand-alone and built-in social media services currently available introduces challenges of definition. However, there are some common features. [11]

1. Social media are interactive Web
2. Internet-based applications.[12]
2. User-generated content, such as text posts or comments, digital photos or videos, and data generated through all online interactions, are the lifeblood of social media.[12]
3. Users create service-specific profiles for the website or app that are designed and maintained by the social media organization. [11] [12]
4. Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals and/or groups. [13]

Although there is a dramatic increase in OSN usage – Facebook, for instance, has now 1.55 billion monthly active users, 1.31 billion mobile users, and 1.01 billion daily users1 there are also a lot of security/privacy concerns. One of the main sources of these concerns is that OSN users establish new relationships with unknown people with the result of exposure of a huge amount of personal data [14]. Unfortunately, very often users are not aware of this exposure as well as the serious consequences this might have. Also, some users are less concerned about information privacy; therefore, they post more sensitive information on their profiles without specifying appropriate privacy settings and this can lead to security risks [15].

As a result, today's social networks are exposed to many types of privacy and security attacks. These attacks exploit the OSN infrastructures to collect and expose personal information about their users, by, as an example, successfully convincing them to click on specific malicious links with the aim of propagating these links in the network [15]. These attacks can either target user's personal information as well as the personal information of their friends. Another widely used attack is the generation of fake profiles, which are generated with the sole purpose of spreading malicious Content. In addition, there is a growing underground market on OSNs for malicious activities in that, for just a few cents, you can buy Facebook likes, share, Twitter followers, and fake accounts. Although many solutions, targeting one specific kind of attacks, have been recently proposed, having a more general solution that can cope with the main privacy/security attacks that can be perpetrated using the social network graph is missing.

2.1 Types of Attacks

- Sybil attacks.
- Identity clone attacks.
- Compromised accounts attacks.
- Socware attacks.
- Creepers attacks.
- Cyberbullying attacks.
- Clickjacking attacks.

Sybil attacks: - To launch a Sybil attack, a malicious user has to create multiple fake identities.

Identity clone attacks: - In this type of attack, malicious user creates similar or even identical profiles to impersonate victims in an OSN.

Compromised accounts attacks: - Compromised Accounts Are accounts where legitimate users have lost complete or partial control of their login credentials.

Socware attacks: - In this type of attack, an adversary creates malware items, called Socware, in the form of applications, Pages or events containing malicious links to be propagated in the OSN.

Creepers attacks: - Creepers are real users they might send friend requests to many strangers or posting spammy advertisements by selling the accounts temporarily.

Cyberbullying attacks: - Attackers harass their Victims (usually children and teenagers) by posting sexual Remarks, threats, or repeated hurtful messages.

Clickjacking attacks: - In this kind of attacks, attackers. Trick users into clicking some items different from what they intended to click. Then, the attacker can manage the User's account by posting spam messages and performing Likes on some items.

III. DESIGN TECHNIQUE

We recall that the aim of the first.

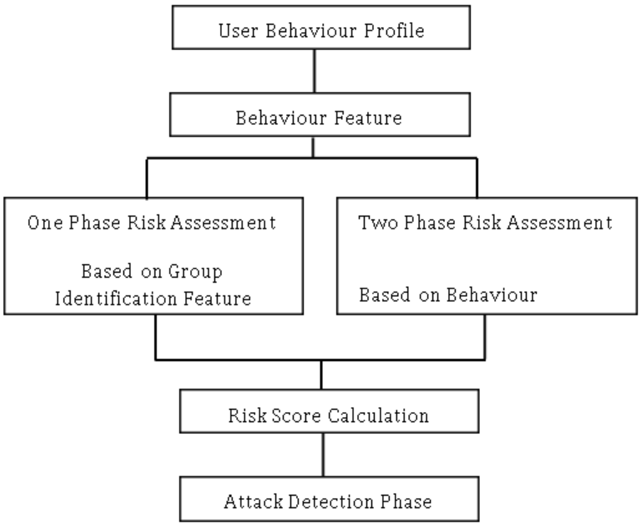

Fig: 3.1 Architecture for Attack Detection Phase

Clustering is to group users for which similar behaviours are expected. At this purpose, group identification (GI) features should be those that are greatly discriminating, likes age, gender, but also those that impact the possible users' behaviours, like, education and nationality. In addition to these features, we have to take into account that even if in the real world people with similar background usually behave in similar way, in an OSN this might be impacted by the users' attitude towards online social networks that might be different even for similar users. For this reason, in addition to profile information (i.e., age, gender, education, nationality), in order to measure users' attitude in online socialization, GI features also include the following:

Fig 3.1 shows the Architecture of the proposed system, input for the system is the Behaviour Profile, based on this the Behaviour Features (BF) are calculated after this BFs are used to do the Risk Assessment. Here Risk Assessment is carried out in two phases. One Phase Risk Assessment and Two Phase Risk Assessment. Based on this output the attacks are categorized and in attack detection phase attacks are detected and reported to Admin.

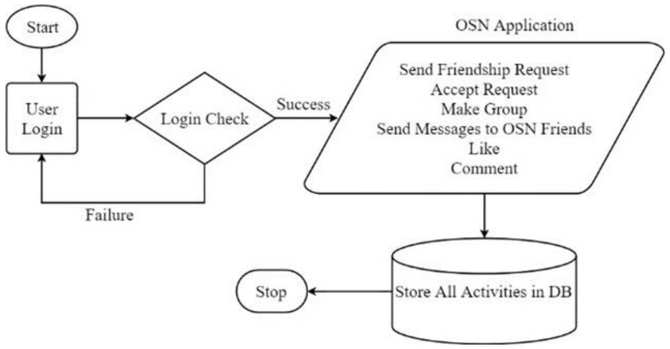

Fig 3.2 User activity Flow Diagram

Figure 3.2 shows the A flowchart is a graphic illustration showing the flow of stages in a program, individuals in an Organization. A flowchart specifies arrangements and choice points as well as initial and ending points. Meanwhile it is easier to hold associations in a pictorial form than in a verbal picture, flowcharts can avoid the oversight of stages in a procedure. Flowcharts are predominantly useful for instructional designers who are beginner or infrequent programmers.

In this application user login to the application first if it is success OSN allow user to do the activities such as user can send Friendship request, accept request, like, comment, post the images, create groups, send messages and do replay to the messages. All these activities are recorded in the database.

3.1 ONE PHASE RISK ASSESSMENT

In One Phase Risk Assessment Phase the Group Identification (GI) Features are considered to detect the attacks in the OSN. GI feature includes the following

- Number of Friends: Here the popular user is accepting request form strangers than the normal or private user. This is one of the features that can be considered in attack detection phase.
- Activity Level: This activity features like, comment and posts by the user and other item for which this user does like, comment and sharing of the posts.
- Percentage of Public item in OSN: Some posts in the OSN are public items. These items can be accessed by anyone in the OSN, so attacker makes use of this thing to propagate the malicious items. So that we need to consider these items too.

3.2 TWO PHASE RISK ASSESSMENT

In Two Phase Risk Assessment Phase Behaviour Feature mapping is done based on the attacks. In this phase I considering the attacks so that need to map the Behaviour Features to the Sybils attacks. The BF's that are to be considered for mapping in done in two ways

- Attack Detection (Dense Graph) in this the Behaviour Features like Comment Rate, Started Comments, Post Rate, Post Propagation Speed, Like Propagation Speed, Comment Feedback Ratio, Post Feedback Ratio, Out In Ratio, Like Rate Like Propagation Ratio and Post Rate Post Propagation are considered to calculate the risk score.
- Attack Detection (Sparse Graph) Group Identification Features, Friendship Ratio, Mutual Friend Ratio, Comment Rate,

Started Comments, Post Rate, Post Propagation Speed, Like Propagation Speed, Comment Feedback Ratio, Post Feedback Ratio, Out In Ratio, Like Rate Like Propagation Ratio and Post Rate Post Propagation are considered to calculate the User risk score.

3.3 Calculation of risk score

This section aimed with some significant procedures of spreading such as mean deviation, variance etc., of the user in the OSN and finally analysis of frequency distributions.

Mean deviation for ungrouped data: For n observation of user u1, u2,..un, the mean deviation about their mean of user u is given by

$$\text{M.D}\ (\overline{u}) = \frac{\sum |ui - \overline{u}\,|}{n} \qquad (1)$$

Mean deviation about their median M is given by

$$\text{M.D (M)} = \frac{\sum |ui - M\,|}{n} \qquad (2)$$

Mean deviation for discrete frequency distribution Let the given data consist of discrete observations u1, u2... un occurring with frequencies f 1, f 2 , ... , fn , respectively.

$$\text{M.D (M)} = \frac{\sum fi\,|ui-\overline{u}\,|}{\sum fi} = \frac{\sum fi\,|ui-\overline{u}\,|}{n}$$

$$\text{M.D (M)} = \frac{\sum fi|ui-M\,|}{n} \qquad (3)$$

Once the mean, median, and deviation is obtained the risk score is calculated as shown below.

3.4 Clustering of Users.

An Expectation-Maximization (EM) algorithm is an iterative method for finding maximum likelihood or maximum a posteriori (MAP) estimates of parameters in statistical models, where the model depends on unobserved latent variables. The EM iteration alternates between performing an expectation (E) step, which creates a function for the expectation of the log-likelihood evaluated using the current estimate for the parameters, and a maximization (M) step, which computes parameters maximizing the expected log-likelihood found on the E step. These parameter-estimates are then used to determine the distribution of the latent variables in the next E step. Filtering and smoothing EM algorithms arise by repeating the following two-step procedure.

E-Step

Operate a minimum-variance smoother designed with current parameter estimates to obtain updated state estimates i.e. the mean and variance of the obtained value is given as input.

M-Step

Use the filtered or smoothed state estimates within maximum-likelihood calculations to obtain updated parameter estimates.

3.5 Gaussian Mixture Model

A Gaussian Mixture Model (GMM) is a parametric probability density function represented as a weighted sum of Gaussian component densities. GMMs are commonly used as a parametric model of the probability distribution of continuous measurements or features in the Risk Assessment Phase. The below formula is used to calculate the risk score i.e. the probability value using the below formula.

$$p(x) = \sum_{i=0}^{k} \pi_i f_i(x)$$

Where p(x) is the probability value is called the risk score of a user.

After calculation of the user risk score the user are clustered, clustering means users are grouped together based on their risk score. In order to do this the threshold value is fixed to do clustering. If the user is below the threshold value, they are called below average user if value is above threshold value users are grouped as a malicious user in case of One Phase Clustering. In Two phase clustering Behaviour Features are mapped to calculate the Risk Score. If the score obtained above the threshold, then it is considered that Sybil attacks may be launched by the user. Here everything is based on the user behaviour profile. The input is the user risk score and output is the detection alert to the admin. Once the attack is detected the admin will take an action.

IV.CONCLUSION

In this paper, One Phase Risk Assessment and Two Phase Risk Assessment is discussed. These approaches are based on risk estimation of the user based on the User Behaviour Features in the OSN by calculating risk score to each user in the network. If the user behaviours are diverged from normal behaviour it is grouped as below average, normal, and abnormal behaviour based on the threshold value.

V. REFERENCES

[1]. N. Laleh, B. Carminati, and E. Ferrari, “Risk assessment in social networks based on user anomalous behaviour,” IEEE Transactions on Dependable and Secure Com- puting, 2016.

[2]. A. M. Kaplan and M. Haenlein, Users of the world, unite! the challenges and opportunities of social media," Business horizons, vol. 53, no. 1, pp. 59-68, 2010}.

[3]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, Detecting and char- acterizing social spam campaigns," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, pp. 35-47, ACM, 2010.

[4]. C. Grier, K. Thomas, V. Paxson, and M. Zhang, @ spam: the underground on 140 characters or less," in Proceedings of the 17th ACM conference on Computer and communications security, pp. 27-37, ACM, 2010.

[5]. J. Jiang, C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai, and B. Y. Zhao, “Under- standing latent interactions in online social networks,” ACM Transactions on the Web (TWEB), vol. 7, no. 4, p. 18, 2013.

[6]. J. R. Douceur, The sybil attack," in International Workshop on Peer-to-Peer Systems, pp. 251-260, Springer, 2002.

[7]. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, “Sybilguard: defending against sybil attacks via social networks,” in ACM SIGCOMM Computer Communication Review, vol. 36, pp. 267- 278, ACM, 2006.

[8]. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, Sybillimit: A near-optimal social network defense against sybil attacks," in Security and Privacy, 2008. SP 2008. IEEE Symposium on, pp. 3,17, IEEE, 2008.

[9]. D. N. Tran, B. Min, J. Li, and L. Subramanian, “Sybil-resilient online content voting.," in NSDI, vol. 9, pp. 15-28, 2009.

[10]. G. Danezis and P. Mittal, “Sybilinfer: Detecting sybil nodes using social networks”, in NDSS, San Diego, CA, 2009.

[11]. L. Jin, X. Long, H. Takabi, and J. Joshi, “Sybil attacks vs identity clone attacks in online social networks,” Pittsburgh: University of Pittsburgh, 2012. international conference on World wide web, pp. 551-560, ACM, 2009.

[12]. M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: threats and solutions” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019, 2036, 2014.

[13]. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, “All your contacts are belong to us: automated identity theft attacks on social networks,” in Proceedings of the 18th

[14]. B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, “An analysis of social network-based sybil defenses,” ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 363{374, 2010.

[15]. V. Dave, S. Guha, and Y. Zhang, “Catching click-spam in search ad net- works,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & com- munications security, pp. 765{776, ACM, 2013.

Cite this Article

Prof. Rajesh R M, Prof. Prathibha S. B., "Detection of Attacks in Online Social Networks (OSN)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 187-193, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194735