iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4401

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Security Risk Detection and Prevention in Online Social Networking

[1]Abhiruchi V. Rahatgaonkar, [2]Prof. Dr.Vijay Gulhane, [3]Prof. J. S. Karnewar
[1]*PG Scholar, Dept. of Information Technology, Sipna College of Engineering, Amravati.*
[2]*Professor & Head, Dept. of Information Technology, Sipna College of Engineering, Amravati*
[3]*Assistant Professor, Dept. of Information Technology, Sipna College of Engineering, Amravati*

Abstract: Online Social Networking System plays an important role in both the modern lifestyle and business models, which changes the way we connect with the physical world. It attracts lots of people and hence users drastically enhance day by day. The end users of the online social network increase ultimately. So that privacy issues increased in this site which leads to several legal issues.

The millions of people are facing security issue, such as cyber-crimes, device hacked and so on. The intention of this proposed project is to investigate risks in this social system and used to analyze the attack activity pattern in the social network. In this projects attack detection will be done.

And also attack prevention is done by this project. So that end user gets alter regarding his account which is available on social site. After getting alter user can take action regarding his attack. And also this project will help to block the attack. By using this project, the user can trust on social networking system if in case any attack occurs when the system can evaluate it and get alter to the user.

Keywords*: *cyber-crimes, security, attack.

I. INTRODUCTION

The advancement of technology made man dependent on the Internet for all his needs. The Internet gives man easy access to everything, and he doesn't take efforts for it. Internet is used in almost every sphere with the development of the internet and it's related benefits also developed the concept of cyber-crimes.

Cyber-crimes are committed in different forms. The social network platform affords users both opportunities and risk. Online social networking site is the community-based website where the user creates an account in that site extend their relationships with the other users of the same site.

It is the platform to build social networks among people who have a common interest, attributes and activities. This creates a rising issue of security, trust, and privacy-preserving among users. In our modern lifestyle and business models which are significantly changing the way we used information, interact to others, and even change the business models across the world. In the past year, social network platform, such as Facebook, Twitter, etc. take lots of effort to purge risky social networking practices ensuring users safety on social networks.

The privacy preservation in the social system has been attracting the attention from both academic and industrial communities. This issue draws even more attention in recent years.

The proposed framework is able to help to recommendation system and alike service to identify bloggers; it is unable to do a deeper investigation, such as event tracking, social network forensics, timeline matching which are important for risk evaluations. Attacks including security risk analysis, abnormal activities' detection, cyber-crimes, terrorist attack, etc. Most of the users are unaware of this attack which is done by an attacker on their account

However, when a user profile is compromised the attacker can also spread the scams rapidly. So to avoid all these issues this paper is developed. All the attacks and their causes can be detected and the user can get alter regarding his account. It is clear that a good model of user activity can be very helpful for analyzing the risks and security threats for the activity patterns in social networks.

II. RELATED WORK

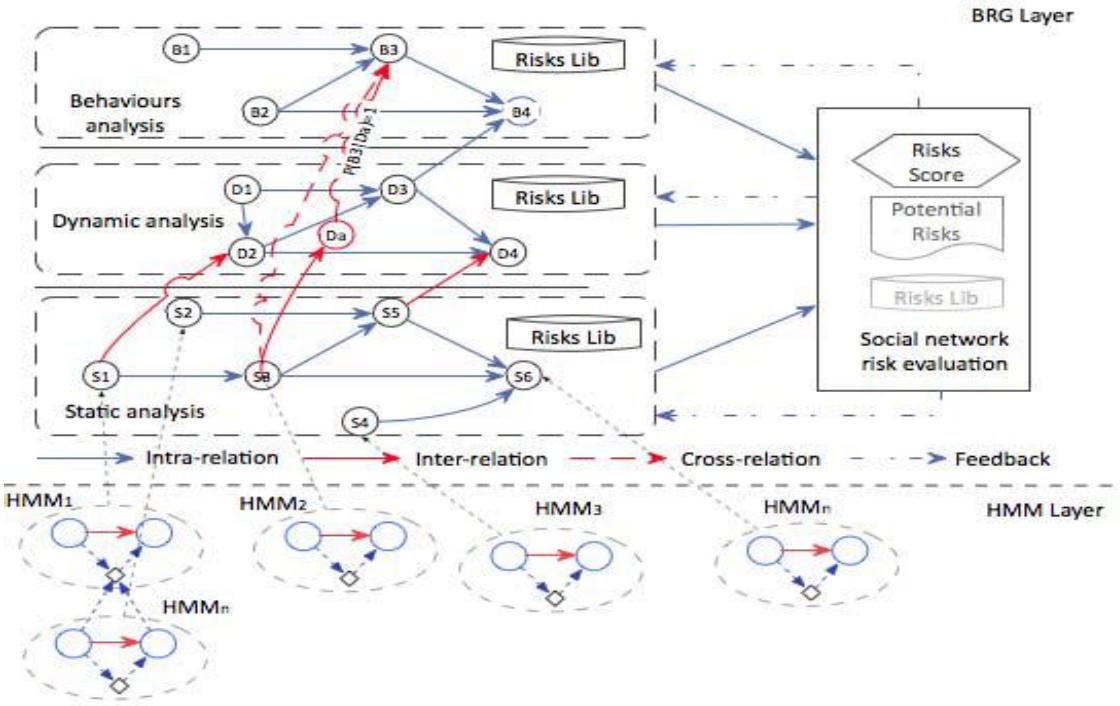


Fig.2.1 Hierarchical Bayesian risk graph model.

The social network platform affords users both opportunities and risk. In the past year, social network platform, such as Facebook, Twitter, etc. take lots of effort to purge risky social networking practices ensuring users safety on social networks. The privacy preservation in the social system has been attracting the attention from both academic and industrial communities. This issue draws even more attention in recent years. The proposed framework is able to help to recommendation system and alike service to identify bloggers; it is unable to do a deeper investigation, such as event tracking, social network forensics, timeline matching which are important for risk evaluations.

Recently, with the research is done in big data analysis a number of research works have been done on the analysis of forensics in social networks. The proposed identification graph can visualize the identify graph based on the social network data without the collaboration of the social network operators.

To analysis the terrorist attack scenario some networks graph is used. However, the proposed methods are unable to dynamically analyze the activity pattern on social networks.

In the previous research, it investigates associated risks in the social networking system and a Hybrid Bayesian Risk Graph(HBRG) model is proposed to analyze the temporal attack activity pattern in social networking. And also to develop hybrid risk analysis model in a cyber-physical social system(CPSS), in which a Hidden Markov Model(HMM) is introduced to model the dynamic user activities that can cause potential risk.

The Bayesian risk graph, which can analyze risk faced by both apps and mobile phone systems analyze that user activity patterns by using Markov model methods based on the observed data, and a clustering algorithm is proposed that can group users according to the interaction behaviors. However, the proposed methods are unable to dynamically analyze the activity pattern on social networks.

III. PROPOSED WORK

Online social networking site gives the user freedom to work in that. So that the risk problem regarding the site is increased. The main purpose of developing this project is to analyze this problem. There are several attacks on social networks such as Fake followers, fake plugin, Malware, Identify theft, etc. If any fake follower attack on the authorized user profile then to detect it, in this project behavior tracking algorithm is used. This algorithm can track the suspicious patterns which are available in the user's history data set. Along with suspicious patterns, our system will be considered time wise behavioral changes of users using social

activities tracked. So that in case of attack the user behavior is track and authorized user get alteration regarding it. In our proposed work, we will consider the previous but recent behavior to track suspicious activities which are more helpful for the user, and for the system to generate alter.

The Artificial Neural Network (ANN) algorithm is also used to detect the suspicious activity of the user. The inner activity wises neural network to find out whether the activity is suspicious or not? For example, if the attacker trying to share a private document with any user, we will check whether the user is an authorized user to share a selected file using ANN. If there is no possibility that the file can be shared to the selected user, the activity can be considered as suspicious activity. So that system can generate alteration to the authorized user. The objective of this project is the enforcement of a strong password policy. This strategy used to defend against a targeted attack based on the fact that an attacker will use an automated tool that tries all possible combinations of letters, numbers and special characters. The length of the password must be at least 6 characters (the longer password, the more difficult to be broken by brute force). The password must include letters (uppercase and lowercase) and numbers. So that it will be difficult for the attacker to guess the password.

Then the Advance Encryption Standards (AES) work for fake attacker is account lockout after 3 failed attempts. If the server detects that a user has provided an incorrect password attempt three times since his last login for the same email, the server will temporary lock the account and then gives the user another chance to prove his/her identity by displaying a new form acquiring the user to answer his/her security question to unlock the account and back again to the login process.

However, if a user failed to enter the correct answer for the security question three times, the server will decide that the account is under brute force attack and will lock it for one day.

REFERENCE

[1] [Bohme and Moore, 2016] M. Riek, R. Bohme, and T. Moore, “Measuring the influence of perceived cybercrime risk on online service avoidance,” IEEE Trans. Dependable Secure Comput., vol. 13, no. 2, pp. 261–273, Mar. 2016.

[2] [Mulazzani, Huber et al., 2017]M. Mulazzani, M. Huber, and E. Weippl. Social Network Forensics: Tapping the Data Pool of Social Networks. Accessed: Mar. 31, 2017. [Online]. Available: http://www.sba research.org/wp-content/uploads/ publications/socialForensics-preprint.pdf

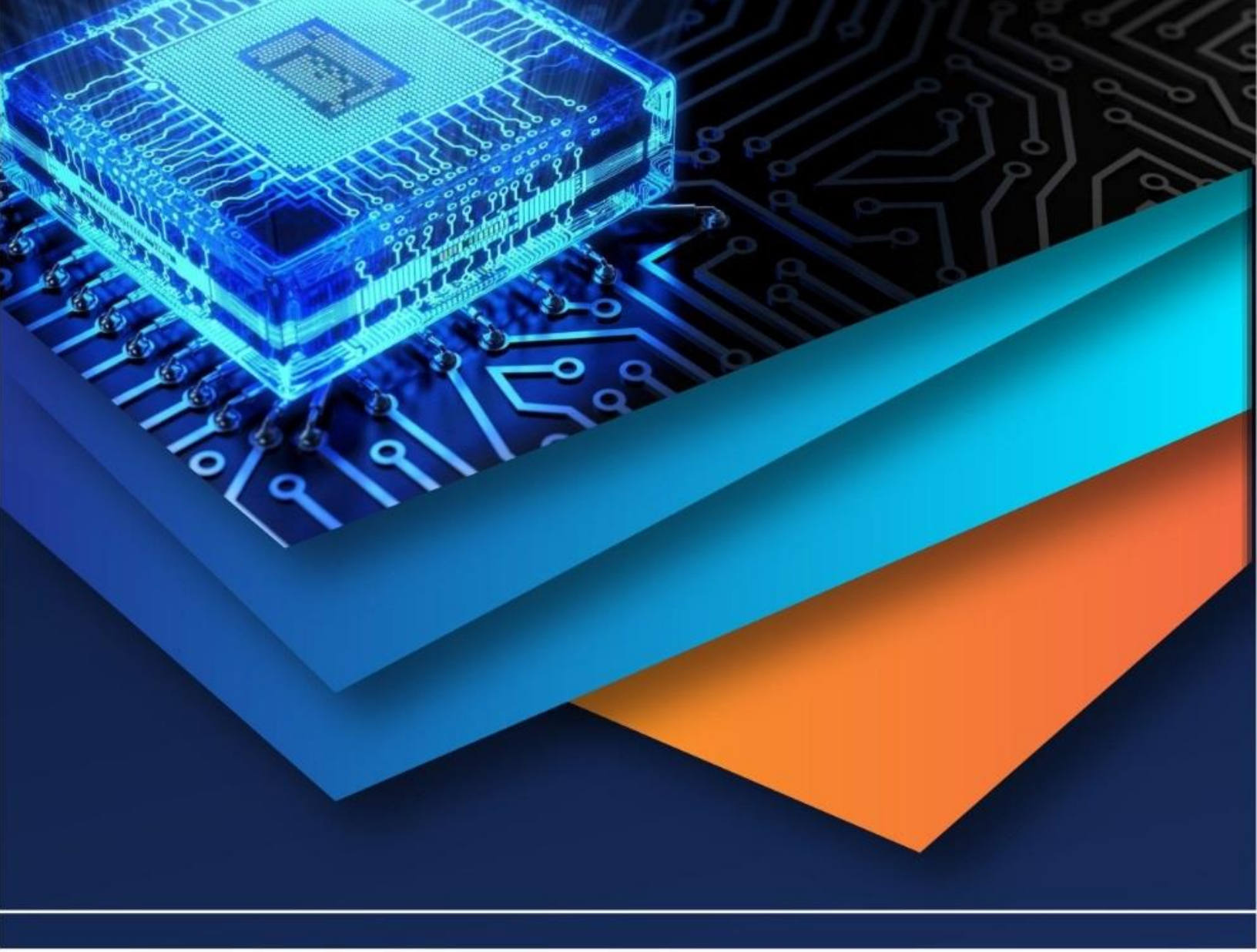
[3] [Weth, Abdul et al., 2017] C. Von Der Weth, A. M. Abdul, and M. Kankanhalli, “Cyber-physical social networks,” ACM Trans. Internet Technol., vol. 17, no. 2, 2017, Art. No. 17.

[4] [Raghavan, Steeg et al., 2014] V. Raghavan, G. V. Steeg, A. Galstyan, and A. G. Tartakovsky, “Modeling temporal activity patterns in dynamic social networks,” IEEE Trans. Comput. Social Syst., vol. 1, no. 1, pp. 89–107, Mar. 2014

[5] [Raun and Qian et-al] M. Li, N. Ruan, Q. Qian, H. Zhu, X. Liang, and L. Yu, “SPFM: Scalable and privacy preserving friend matching in mobile cloud,” IEEE Internet Things J., vol. 4, no. 2, pp. 583–591, Apr. 2016.

[6] [Singh, Pattipati et al., 2006]H. Tu, J. Allanach, S. Singh, K. R. Pattipati, and P. Willett, “Information integration via hierarchical and hybrid Bayesian networks,” IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 36, no. 1, pp. 19–33, Jan. 2006.

[7] [Tao, Liu et al., 2017] Y. Guo, D. Tao, W. Liu, and J. Cheng, “Multiview cauchy estimator feature embedding for depth and inertial sensor-based human action recognition,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 47, no. 4, pp. 617–627, Apr. 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY