Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.8 No.2, 2019, pp.6-8

DOI: https://doi.org/10.51983/ajcst-2019.8.2.2149

A Survey on Online Social Networks: Applications, Threats and Solutions

K. Jayabalan[1] and B. Subramani[2]
[1]Research Scholar, Department of Computer Science, KSG College of Arts and Science, Tamil Nadu, India &
Assistant Professor, Department of Computer Science, Dr. N.G.P. Arts and Science, Tamil Nadu, India
[2]Research Supervisor & Principal, Shri Nehru Maha Vidyalaya College of Arts & Sciences, Tamil Nadu, India
E-Mail: gkjayabalu@gmail.com, subramaningp@gmail.com
(Received 5 February 2019; Revised 23 February 2019; Accepted 23 March 2019; Available online 3 April 2019)

***Abstract* - Online social networks (OSNs) are playing crucial role in digital world today. OSNs are web applications that allow users to share their personal information, digital images and videos, and to inform others about online or real time world activities and events with people in their network. OSN's are decentralized and distributed computer networks where users communicate with their friends and relatives through Internet services. The Smartphone has increase the situation for hacker's to attacks end user data from OSNs. Behaviors of OSN users has been monitored for data analytics[1]. In this paper, we represent full review of the applications, different security level threats and privacy issues, which threaten the well-being of OSN users in general, and children in particular. In addition, we present an overview of existing solutions that can provide better protection, security, and privacy for OSN users[2]. We also offer few recommendations for OSN users, which can improve their security and privacy when using the online social networks.**
***Keywords:* OSN, Security, Privacy, Threats, Knowledge**

I. INTRODUCTION

Online Social Networking (OSN) service is an online platform which people use to build social networks or social relationship with others who are interested to share their personal, career things, activities and real-life connections. In the digital world, digital gadgets are playing vital role to enrich the social networking applications to the people. But sometimes the digital gadgets are not fulfill the requirements due to remote areas with poor wireless coverage and hence unreliable Internet access, vehicular networks in which network situations are highly dynamic and information transfers are sensitive to time latency, or disaster scenarios where the communication infrastructure has been damaged.

Social networking sites allows users to share a variety of technical features to each other[3]. The success of online social networking services can be seen in their dominance in society today, with Face book having massive users and career-oriented social-networking service. As of the third quarter of 2018, Face book had 2.27 billion monthly active users. With rapid development of online social network, few questions are raised to increase the integrity: How social media have been used? Which are related to online social network utilization? Which are the factors affect the online social media support?[4]

II. APPLICATIONS OF OSN

The following sectors are widely utilized OSN to share their knowledge, brand their products and taking survey from people in easiest way.

1. Government
2. Business
3. Medical and Health
4. Education
5. Political
6. Research

A. Government

Social media applications offer a fast and easiest platform for the government to get the opinion of the public and to keep the public updated on their activities. Police departments are presenting crime prevention procedure, time sensitive information and using social media channels to ask information on wanted criminals from the people. Online Social Medias will help to municipalities and health department to communicate important safety information to the affected areas in a short amount of time.

B. Business

Social media can be a good way to attract the new customers and business owners. Social networks give you the opportunity to interact directly with customer and fans give them chance to describe the features of the particular product. Customer service and support is very easy in business sector. Social media contents have been shared and liked by women's compare than men's[4] to increase the business to attract the customer.

C. Medical and Health

Health professionals have been using social media to benefit the patients, enhance professional networks, and advance understanding of individual and contextual factors influencing public health. Daily Strength is the site contains online communities that deal with different medical conditions or life challenges. Patients Like Me is also the social networking site to offers patients connect with others who have the same disease or condition and track and share their own experiences with the goal to improve outcomes.

Fitocracy is an online gaming portal and social media that aims to use gamification to help patients to improve their fitness. There has been a tremendous development in the use of online social media to expand the view of various specialties in medicine field[4]. Increased usage on online social network, medial awareness has increased over the past few years. Experts are exchange their knowledge in social media networking to enrich the medial education filed[5].

D. Educational

Social media is helpful for education sector to enrich the academic settings ranging from elementary and secondary school to post-secondary education. Social media tools can be misused for cyber bullying or sharing inappropriate content. As result, cell phones have been banned from some classrooms, and some schools have blocked many popular social media websites. YouTube is most of people accessed social media portal in the classrooms to demonstrate the lecture in digital mode. Students can watch videos, answer questions, and discuss content. Additionally, students can create videos to share with others to enrich the digital skills.

E. Political

Social media platforms including Face book, Twitter and You tube are allowing the politicians to speak directly to peoples without spending a dime. Election commissions can be publish the awareness of voters' content and broadcast it to millions of people instantaneously within stipulated time. Voters are able to connect directly to politicians to engage in political activities in new method. Politicians are able to present their opinions and ideas to the people. Politicians are asking for feedback from voters or constituents can be a good thing in the digital world.

F. Research

Researchers are very much enthusiastic to develop and find their problems in OSN due to end users are very high. Also massive amount of data has been accumulated in social media to analyze the data[5]. Data science and big data analytics have been rapidly developed based on high demand research in social media network areas. Researchers are also very much interested to review the multi-disciplinary within the social media[6]. Social network analysis is also growing in the world due to millions of users having different behavior aspects in their research. OSN is providing opportunities for cyber bullying methods. Cyber bullying method is harassing or insulting the people by sending messages of hurting or threatening nature using digital communication[7].

III. THREATS IN OSN

The OSN security and efficiency of maintain data integrity is important challenging issues in the information sharing systems. End users of online social networks are spontaneously publishing and sharing their social network data with third party consumers. The stored social network data contains very sensitive information about users and their relationships[8]. However, the OSNs service provider is generally a semi-trusted server who will honestly follow the designated protocol, but might collect the OSN credential and share them with others for benefits without users' knowledge or consent[9]. Majority of OSN users are providing their behaviors in their accounts. So the attackers can easily identify the end-users behaviors. Most part of research works on privacy issues in OSN focuses on the general way of cumulated data, while our work can be enriched in another branch of research that focuses on formatting, measuring and preventing privacy measures in OSN.

A. Privacy Breach Attacks

Most of users in OSN are providing their images, phone numbers, email id and date of birth in public mode. In this case, all the personal information's can be attacked by hacker easily. Online Social Networks are the crucial targets for worm creators due to the following things : contact list and personal information[10].

B. Malware Attacks

Attackers can get some information from OSN users while they are sending some email and file sharing through spreading some malicious software's. Malware can propagate over social networks via profile, interaction, and third-party applications[11].

Koob face is the example of social network worm which targets to social network users. There are several such worms are created by hackers to get social network users privacy data. Online Social Network worms have to send worm mails or push messages that containing malicious code or hyperlinks to open the particular indirect webpage's.

C. Fake Profile Creations

OSN users can create fake profiles under different identities to hack and get sensitive information from other users. So far many OSN media do not have the secure authentication techniques. Adding friends and reliable photos are crucially updated by the hackers to motivate the social media users to accept the friend request.

D. Phishing

Attackers use fake websites and emails to fool the end users to surrender their personal and sensitive information. The OSN users will be directed to websites where they will be asked for information like password, credit card details[12]. When the recipients opened the unwanted invitations, they were redirected to third party web portal to ask the identical information.

E. Fake Online Advertising

Online Social Network advertising, the word of the "free" content on the web has crucial marketing business in recent years by insist the new opportunities for advertisers to reach potential customers[13]. Whenever customers are interested to get free products, attackers are insist the users to provide their bank account details to send the product. After getting the bank details from the social network users, attacker made misbehavior to the account. Online advertising is better tool to attract the customers and industries are very much interested[13].

IV. PROTECTING USER DATA FROM OSN

We are delight enjoy utilizing OSNs to interact with other end users through the sharing of our experiences. We advise OSN end users who are in need to better control themselves in these applications to implement the following few recommendations in each of their OSN credential mechanism [14]. Nowadays it has been informed that wireless technology networks have evolved in a tremendous way offering the way for new paradigms such as Internet of Things (IOTs), smart cities, location-based mobile applications and context-aware systems[15]. Cookies information's are stored in your computer that is easily hacked by hackers. So we are in the critical situation to safe guard our data from attackers. There is a need for a security mechanism that secures users activities and operates the main purposes of OSN at the same time, because almost all of the available Smartphone's don't support all privacy issues[16]. So we recommended that the following things to be configured in OSN users account settings.

1. Adjust Privacy and Security Settings
2. Do Not Accept Friend Requests From Strangers
3. Install Antivirus and Internet Security software's
4. Do Not Trust your Network Friends
5. Monitor Your Kids from OSN
6. Un-Install Third-Party Applications
7. Remove Cookies information's periodically
8. Create Strong Password in OSN

V. CONCLUSION

Privacy preservations in online social network is an active area of research with many opportunities are remaining to be addressed. OSN providers should incorporate high level of encryption methods in their servers to ensure the data integrity and confidentiality of OSN end users. In this paper, we have presented basic knowledge of online social networks and how threats are passed in the online networks. Also we recommended few steps to overcome the threats. We hope that this survey will offer very good understanding of review of OSN and creates new research interests and developments in this field.

REFERENCES

[1] T. A. Trinh and N. E. Group, "Measuring User Behavior in Online Social Networks," No. October, pp. 26–31, 2010.

[2] Y. Asim, A. K. Malik, B. Raza, W. Naeem, and S. Rathore, "Community-Centric Brokerage-Aware Access Control for Online Social Networks," *Futur. Gener. Comput. Syst.*, 2018.

[3] K. Ghazinour and J. Ponchak, "Hidden Privacy Risks in Sharing Pictures on Social Media," *Procedia Comput. Sci.*, Vol. 113, pp. 267–272, 2017.

[4] J. E. Indes, L. Gates, E. L. Mitchell, B. E. Muhs, and N. Haven, "Social media in vascular surgery," *J. Vasc. Surg.*, Vol. 57, No. 4, pp. 1159–1162, 2013.

[5] G. B. Colbert *et al.*, "The Social Media Revolution in Nephrology," *Kidney Int. Reports*, Vol. 3, No. 3, pp. 519–529.

[6] S. Ghani, S. Member, B.C. Kwon, and S. Member, "Visual Analytics for Multimodal Social Network Analysis : A Design Study with Social Scientists," *IEEE Trans. Vis. Comput. Graph.*, Vol. 19, No. 12, pp. 2032–2041, 2013.

[7] B. S. Nandhini and J. I. Sheeba, "Online Social Network Bullying Detection Using Intelligence Techniques," *Procedia - Procedia Comput. Sci.*, Vol. 45, pp. 485–492, 2015.

[8] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy preserving social network data publication," *IEEE Commun. Surv. Tutorials*, Vol. 18, No. 3, pp. 1974–1997, 2016.

[9] Q. Huang, Z. Ma, Y. Yang, X. Niu, and J. Fu, "Improving security and efciency for encrypted data sharing in online social networks," *China Commun.*, Vol. 11, No. 3, pp. 104–117, 2014.

[10] S. Wen, S. Member, W. Zhou, and J. Zhang, "Modeling Propagation Dynamics of Social Network Worms," *IEEE Trans. Parallel Distrib. Syst.*, Vol. 24, No. 8, pp. 1633–1643, 2013.

[11] T. Saikumar and P. Sriramya, "Security issues in social networks," *Int. J. Pharm. Technol.*, Vol. 8, No. 4, pp. 20835–20841, 2016.

[12] I. No, "Available Online at: www.ijarcs.info Comparative Study Of Threats And Solutions In Online Social," Vol. 9, No. 1, 2018.

[13] J. Estrada-jiménez, J. Parra-arnau, A. Rodríguez-hoyos, and J. Forné, "Online advertising : Analysis of privacy threats and protection approaches," Vol. 100, pp. 32–51, 2017.

[14] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Commun. Surv. Tutorials*, Vol. 16, No. 4, pp. 2019–2036, 2014.

[15] A. M. T. Ali-Eldin, "Trust prediction in online social rating networks," *Ain Shams Eng. J.*, Vol. 9, No. 4, pp. 3103–3112, 2018.

[16] R. Ajami, N. Al Qirim, and N. Ramadan, "Privacy issues in mobile social networks," *Procedia Comput. Sci.*, Vol. 10, pp. 672–679, 2012.