Chapter 12
Evolving Cyber Threats, Combating Techniques, and Open Issues in Online Social Networks

Sanjeev Rao
https://orcid.org/0000-0001-7338-1930
Thapar Institute of Engineering and Technology, India

Anil Kumar Verma
Thapar Institute of Engineering and Technology, India

Tarunpreet Bhatia
Thapar Institute of Engineering and Technology, India

ABSTRACT

Online social networks (OSNs) are renowned powerful web tools that allow worldwide users to connect with their friends, families, professional groups, and social circle through social interaction for sharing common interests. With the proliferation, ease, and efficacy of OSNs, these are becoming an essential tool for communication. But many OSN users innocently uncover their personal information such as their home address, phone numbers, email id, etc. that can be used by the malicious user to perform various kind for cyber-crimes like cyber-bullying, spamming, click-jacking, identity theft, phishing, distrust, fake profiles, spreading malicious content, etc. This chapter presents a review of various privacy and security threats/attacks associated with OSN users and recommended combating techniques based on data-mining and machine learning algorithms. Also, the future directions for upcoming researchers in this field are suggested.

DOI: 10.4018/978-1-7998-5728-0.ch012

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

From the last few years, the usage and popularity of OSNs have increased at a tremendous rate. It becomes a necessary tool to facilitate communication for every online social user (Boyd & Ellison, 2007). Some of the very popular OSNs are Facebook, Twitter, Google+, Myspace, Tumblr, Sina-Weibo, Snapchat, Pinterest, and Instagram, etc. have millions of daily active users. As of the first quarter of 2020, Facebook has a maximum, i.e., more than 2.5 billion monthly active users (Statista, 2020). The preliminary characteristics of social networking are based on 3C's, i.e., creation, curation, and consumption. OSNs generally have synonyms like Online Social Media (OSM), Social Network Sites (SNS) that were used interchangeably in many research papers. Social media is like a vehicle for communication. It's a place that can be used to transmit information to other people like newspaper agencies publish and spread the news in the form of a newspaper to many people. But with the advent of the internet, media is no longer static and can be used as blogs, apps, websites, videos, etc. Social media is a broader term, and the OSN is part of Social Media. OSN allows users to connect with their friends, families, professional groups and social circle through social interaction for sharing common interests by first connecting with other members through sending and receiving friend request, later in the form of posts, comments, likes, dislikes, tags, sharing posts, followers, following, etc. OSNs are helping many other business sectors like marketing, advertising, promotions, product reviews, knowing public opinion in political elections, online learning, growing business reputation, disaster management, healthcare, professional network, and recommender systems, etc. (Fire, Goldschmidt, & Elovici, 2014; Penni, 2017). The challenges associated with OSNs are an ever-increasing amount of users' leads to the accumulation of Bigdata in the form of textual data, data related to their connections, multimedia data that they share, and personal information (Persia & D'Auria, 2017). These further give rise to issues such as data storage, data management, and data analyses. Users trust these OSNs and users within these social networks that lead them to make their social network by sending and receiving friendship requests from people whom they know and don't know or but having some friends in common. By accepting these friend requests, users innocently reveal their personal information (age, religion, income, relationships, location, phone numbers, sexuality, habits, financial details, etc.) and professional in-formation like (company, project, work-culture, team, reports, earning, etc.) to strangers. This information could be exposed and abused maliciously and hurting the users both in the cyber and in the real world (Bilge, Strufe, Balzarotti, & Kirda, 2009; Gangavarapu, Jaidhar, & Chanduka, 2020). The vast Number of OSN users and huge volumes of personal details have attracted malicious people, hackers, computer criminals, and third-party companies, etc. These malicious users conduct illegal practices such as data stealing, ransomware, false accounts, spamming, invading viruses, phishing, cyber-bullying and sexual assault, and fake reviews, etc.(Persia & D'Auria, 2017). These challenges give rise to new research directions to secure the privacy of OSN users that is at stake due to misuse of personal information, spreading viruses, fake news, rumors, and spam by malicious users and hackers. The success of any OSN is influenced by the number factors like Number of active users, design, privacy and security of users, other useful features like searching, profile tagging, messaging, calling, photo and text editing options, etc. OSN developers give much emphasis on design and features, and decidedly less focus is given to the security and privacy of OSN users. So studying, analyzing, and combating OSN's privacy and security issues have now become a wide area of research. The motive of this chapter is to provide useful information regarding privacy and security threats/attacks in the OSNs. In this chapter, a survey of some paramount cyber threats associated with

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/evolving-cyber-threats-combating-techniques-and-open-issues-in-online-social-networks/261732

Related Content

A Quantum Secure Entity Authentication Protocol Design for Network Security
Surjit Paul, Sanjay Kumarand Rajiv Ranjan Suman (2019). *International Journal of Information Security and Privacy (pp. 1-11).*
www.irma-international.org/article/a-quantum-secure-entity-authentication-protocol-design-for-network-security/237207

CSMCSM: Client-Server Model for Comprehensive Security in MANETs
Hatem Mahmoud Salama, Mohamed Zaki Abd El Mageed, Gouda Ismail Mohamed Salamaand Khaled Mahmoud Badran (2021). *International Journal of Information Security and Privacy (pp. 44-64).*
www.irma-international.org/article/csmcsm/273591

Corporate Social Responsibility and Corporate Governance: Analysis across Industries in Mexico
Andrée Marie López-Fernández (2017). *Business Analytics and Cyber Security Management in Organizations (pp. 163-182).*
www.irma-international.org/chapter/corporate-social-responsibility-and-corporate-governance/171845

Data-Embedding Pen
Seiichi Uchida, Marcus Liwicki, Masakazu Iwamura, Shinichiro Omachiand Koichi Kise (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data (pp. 396-411).*
www.irma-international.org/chapter/data-embedding-pen/70298

Cyber Defense Maturity Levels and Threat Models for Smart Cities
Ali Amur Al Shidhani (2019). *International Journal of Information Security and Privacy (pp. 32-46).*
www.irma-international.org/article/cyber-defense-maturity-levels-and-threat-models-for-smart-cities/226948