July - 21-22
22-23

IIETA International Information and Engineering Technology Association

International Journal of Safety and Security Engineering
Vol. 12, No. 4, August, 2022, pp. 507-518
Journal homepage: http://iieta.org/journals/ijsse

Comprehensive Analysis of Privacy Attacks in Online Social Network: Security Issues and Challenges

Sandip A. Kahate[1*], Atul D. Raut[2]

[1] Research Centre P. G. Computer Science Department, SGBA University, Amravati 444601, Maharashtra, India
[2] CSE Department, P. R. P. P. College of Engineering, and Management, Amravati 444601, Maharashtra, India

Corresponding Author Email: sandipk_joe@bkc.met.edu

https://doi.org/10.18280/ijsse.120412

Received: 18 July 2022
Accepted: 20 August 2022

Keywords:
online social network, security, privacy issues, malicious user, machine learning, decentralized technique

ABSTRACT

Nowadays, users value their privacy of information is more than money but the Online Social Network is creating new platforms for cybercrime to intimidate innocent users of countries because of the privacy pitfalls in the present traditional centralized architecture like Facebook, WhatsApp, and Twitter, Instagram, and many more. Third-party apps and malicious attackers breach innocent users' private information, especially adolescent users for their personal purpose. Many Asian countries have no special data protection laws like a European. The main objectives of this research paper are to study the different types of privacy attacks for data confidentiality in the Online Social networks with analyzed mitigation techniques and discussed future proposed work on how to control and detect the user's private information from unreliable people. Even then, few privacy destructions are unresolved!

1. INTRODUCTION

Online social networks are becoming tremendously popular among young as well as old people just too virtually interconnect with each other for the purpose of exchanging information and entertainment while supporting various new apps that are launching day by day.

Michael Fire et al. survey the OSNs, those apps which stand as a demanding rank in the youth of society, such as Facebook, Google+, Twitter, Instagram, etc., as listed in Figure 1.

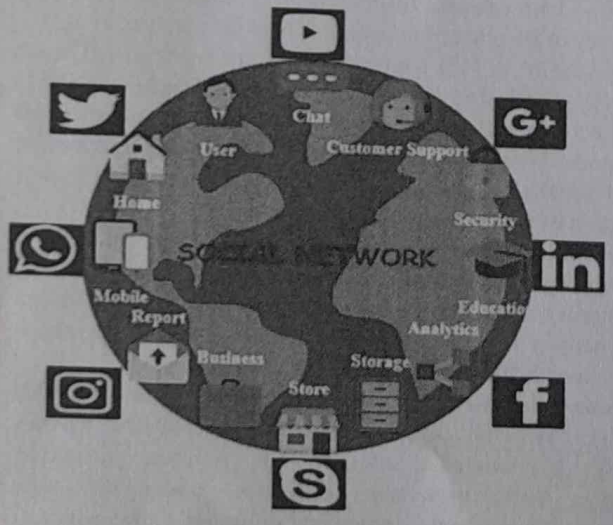

Figure 1. Online social network

It has more demanding apps in society, primarily from young people [1]. Worldwide, there are over 2.9 billion monthly active Facebook users as of the first quarter of 2022 which is a 13 percent increase year over year. YouTube has 2.5 billion monthly active accounts, while WhatsApp has 2 billion. Instagram, the fourth-most popular photo sharing app, with over 1.4 billion users and 436 million monthly active Twitter users globally. Global internet users spent an average of 147 minutes each day on social media, so, in 2022, over 4.26 billion individuals used social media globally, with that figure predicted to climb to over six billion by 2027 [2].

Through his or her profile, an OSN user creates his or her own identity in the social network, which is accessible to their friends in a transitive manner. OSN also has the ability to create links between different users. He/she can form these connections with various users known as "friends," "mutual friends," and "friends-of-friends," and even accepts friend requests from strangers who may turn out to be good friends. If both the users are successfully connected with each other then it is considered as a neighbor. Chewae et al. examine how the high demand for and regular use of OSN causes security and privacy issues in cybercrime. Non-secure private information in OSNs will result in the open entry of attacks for susceptibilities or malicious users for destructive intentions, especially by teenagers [3]. Nowadays, in the area of OSNs, many researchers are working on security and privacy aspects that make the OSN systems more appropriate to society at large in the future [3-6]. Privacy setting also provided by many OSNs to allow users to avoid other users' access. As survival is one of the important criteria, intervention of advertising agencies, political parties during election prevent the providers to breach information (theft identity) to third parties.

The main purpose behind all of these in the picture is to show the centralized infrastructure of OSN under the control of a single administrator. Hence, users have no options without believing in the OSN provider to protect all their confidential data. Even though the user does not know whether their confidential data is actually protected from attackers who may breach and theft from the provider's server or not. Therefore,