Impacts of Big Data on Privacy and Security of Social Media Users

Introduction

In the world of ever-changing technology, many companies have started to adopt Big Data to keep to the pace of technology. Despite Big Data presenting wide arrays of benefits to companies, studies have shown that there are numerous issues of Big Data that revolves around the privacy and security of the users. Individual activity on social media is increasingly collected by social media providers even without the consent of the users. Although companies might be using those user activities for a right purpose such as to predict future behavior, purchase choices, or other sensitive subjects, it breaches the users' privacy. The purpose of this paper is to investigate how inherent characteristics of Big Data impacts on the privacy and security of the users of social media.

Problem Description

Privacy breaches have nearly become a norm in social media [1]. In the recent past, there have been various cases where social media providers leverage customers' information for wrongful purposes. Facebook was recently accused of colluding with Cambridge Analytica to advance political campaign. In the scandal, Facebook is believed to have aided Cambridge Analytica with personal information of "Up to 87 million people" [5]. The case of Facebook depicts how Big Data exposes users to privacy breaches and violation. Twitter was also accused of selling public data access to Cambridge Analytica to support its campaign.

Hacking of social media accounts is aided by Big Data. Although users often feel a sense of privacy when they are interacting in social media, Big Data uses user's search behavior to harvest or gather information. This information is used for wrongful purposes. Studies have shown that Big Data intrusions often leave members of underrepresented groups to become more vulnerable [3] and [5]. Although social media users are fully aware of security breaches, they can do nothing because in most cases security breaches are aided by social media providers.

The huge explosion in the Big Data available has made users information more vulnerable. Cyber attackers have devises new ways of attacking social media users' data. As a result, it has increased the risk of data and privacy breaches. The security of customers is at risk because their critical information such as location and financial position are exposed to attackers. Studies have demonstrated that a lack of awareness of social media use has contributed to security breaches. According to [1], the majority of social media users are not aware of the dangers of using social media on privacy. This has made them more vulnerable to data breaches.

The effects of Big Data on social media users are often considered unethical. This is because social media providers sometimes manipulate the data for wrongful purpose without considering the negative impacts on the customers. Studies have directly linked data and security

breaches on social media to depression and anxiety [1]. Some social media users have developed signs of symptoms of anxiety and depression whenever they are attacked. This depicts the dangers of Big Data not only on privacy but also on the health of individuals.

Objectives of the Proposal

The prime objective is to examine the correlation between Big Data and privacy breaches. This is achieved by looking at how Big Data exposes the data of social media users to attackers or hackers. Studies conducted in the past act as a source of information in understanding the underlying facts of the study [4]. The second objective is to identify and semantically link multi-lingual and diverse cross-sector information sources that contribute to privacy breaches in social media. This is achieved by looking at risk-areas in social media. Although it is common knowledge that weak passwords and users are prime causes of hacking in social media, the study will look at other vulnerabilities that increase data breaches.

Furthermore, the proposal is to identify sources of vulnerabilities in social media and measures that can be used to thwart them. This is achieved by looking at past cases on how human errors, weak passwords, malware attacks, unsecured mobile phones, and privacy settings contribute to privacy breaches in social media [3]. Identifying the measures to curb social media hacks can be achieved by scrutinizing past records. Finally, the proposal will investigate the correlation between security awareness and privacy breaches in social media. This is achieved by using a formal questionnaire to extract data from users for analysis.

The significance of the Research

The proposal is important in understanding the security issues posed by Big Data on social media and measures to thwart them. It helps users to appreciate the use of strong passwords and usernames in their social media accounts. It also acts as an eye-opener because it enlightens users on sources of vulnerabilities in social media [2]. In addition, the research broadens users regarding privacy within an evolving technology environment. It also addresses the datafication model which emphasizes on post-collection data. Moreover, it increases knowledge of how Big Data gather information on social media user’s search behaviors.

References

[1]C. Changchit and K. Bagchi, "Privacy and Security Concerns with Healthcare Data and Social Media Usage", *Journal of Information Privacy and Security*, vol. 13, no. 2, pp. 49-50, 2017. Available: 10.1080/15536548.2017.1322413.

[2]T. Ring, "Your data in their hands: big data, mass surveillance and privacy", *Computer Fraud & Security*, vol. 2016, no. 8, pp. 5-10, 2016. Available: 10.1016/s1361-3723(16)30061-6.

[3]W. Chung, "Social media analytics: Security and privacy issues", *Journal of Information Privacy and Security*, vol. 12, no. 3, pp. 105-106, 2016. Available: 10.1080/15536548.2016.1213994.

[4]M. Kantarcioglu and E. Ferrari, "Research Challenges at the Intersection of Big Data, Security and Privacy", *Frontiers in Big Data*, vol. 2, 2019. Available: 10.3389/fdata.2019.00001.

[5]F. Panvelwala and A. G., "Data Protection Guidelines for Protecting Privacy of Users on Social Media", *International Journal of Computer Applications*, vol. 182, no. 2, pp. 7-12, 2018. Available: 10.5120/ijca2018917449.