Social Media Privacy Protection for Blockchain with Cyber Security Prediction Framework

M. Veni Priya[1], Mrs P. Jasmine Lois Ebenezer[2]

[1]PG Scholar, Department of Computer Applications and Research Centre, Sarah Tucker College (Autonomous), Tirunelveli, Tamil Nadu, India

[2]HOD & Associate Professor, Department of Computer Applications and Research Centre, Sarah Tucker College (Autonomous), Tirunelveli, Tamil Nadu, India

---***---

Abstract - *Human life has become increasingly reliant on social networks. Most social networking sites provide basic features such as online contact, communication, and interest sharing, as well as the ability to build online profiles that other users can view. Unfortunately, many users are unaware that their personal information is being disclosed through their profiles. Leakage of a user's personal information can occur in a variety of ways. This study discusses many of the security issues involved with utilizing social media. Also discussed is the topic of privacy and how it pertains to security. Some crucial points are presented based on these conversations in order to increase a user's privacy and security on social networks. Our investigation will assist readers in comprehending the security and privacy concerns that social network users face, and this research will assist users.*

Key Words: OSN, security, classic privacy threats, modern threat.

1. INTRODUCTION

Social media's growth has ushered in a new age of communication and connection. It has become an integral aspect of our social lives, allowing us to interact with friends, family, co-workers, and others. We've seen how social media platforms like Facebook, Twitter, and WhatsApp have revolutionized the way we use the internet for both personal and professional reasons. [4] social media are a kind of online engagement that allows data senders (data generators) and receivers (end users) to form virtual communities via the usage of online social networks. Because so much of our personal information is stored on the Internet, information security should be a top priority for everyone. Because of the massive popularity of these social networks, which are often used by minors and those who do not value privacy or security, a large quantity of potentially private information is posted on the Internet for others to see. [1] It is important to be cautious about what we publish online in this manner; being careless might result in information being shared that should not be considered.

A significant portion of long-distance interpersonal communication is concerned with security. Aside from the revolution in social networking that Online Social Networks have brought about, its attraction, the ever-increasing number of members, and the vast quantity of personal information they exchange have created new hazards to their users.

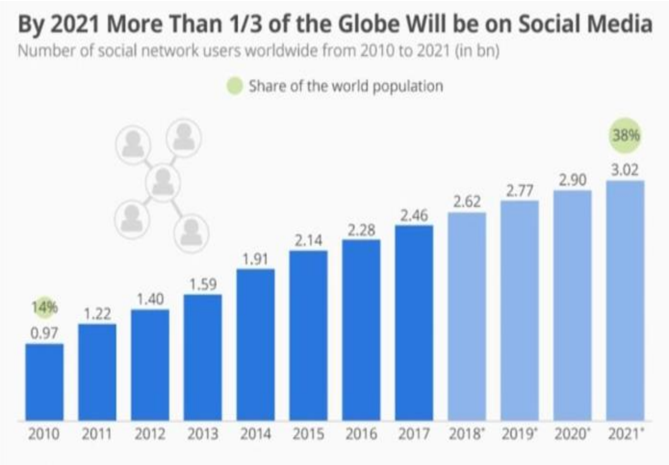


Fig -1: Social network growth from 2010-2021

As they become more integrated into users' everyday lives, online social networks raise additional security issues, particularly due to the possibility for massive quantities of personal data to be exposed. Security and privacy assaults on online social networks, as well as remedies that may be employed to preserve users' privacy and keep shared data safe from various sorts of attacks. Because of the possibility for accessing a great quantity of personal information provided by online social networking users, online social media might present new hazards for its users. Private information of persons or organizations, digital identity, financial assets, intellectual property (IP), and organizational secrets and resources are all vulnerable to assaults in Online Social Networking [5].

2. LITERATURE REVIEW

Recently, the internet has emerged as one of the most efficient and effective means of communicating and exchanging information, particularly in the context of social networking sites. With over billions of users linked via online social networks, and due to the popularity of social networking sites, privacy has become a major worry for many individuals.

Security concerns on social networking sites are minimal, and users' efforts to make reasonable modifications to their social media security are much lower than other sorts of security operations, according to research. Many social media users, on the other hand, lack technological competence and have occasional security worries. It's one thing to ensure that social networks can execute desirable behaviours, but while sharing a wealth of (personal) data, it's equally important to examine what unwanted behaviour can arise. We'll look at privacy, its significance in social networks, and possible dangers to users' privacy in this part.

As a result, many firms lack a robust social media security policy and program, and are unclear of how to develop effective social media security policies to reduce social media security threats, according to He's findings. Security protection of personal information online has become a substantial and vital study area as social networking services have grown in popularity. This article looked into and examined the privacy and security of social networking sites. We will review how current privacy plays on social network sites, analyse how personal information is influenced by the internet and social networks, and discuss how privacy has become a risk and how to use security awareness to avoid privacy rise, affecting users' self-disclosure of private data in this paper.

The perceived advantage was merged into this study using privacy calculus, and a few characteristics, such as, need change. Data should be managed in a way that does not compromise the privacy of users, and data protection should be thoroughly examined. The first and most important step everyone who uses social media should do is to establish an unwavering standard of privacy. After analysing the literature, the concepts of data sensitivity and perceived advantage were redefined. This research work intends to reduce the level of privacy worry by examining the constructs of privacy concern and self-disclosure.

3. COMMON SOCIAL MEDIA SECURITY RISKS

3.1 Social Media Accounts That Aren't Monitored

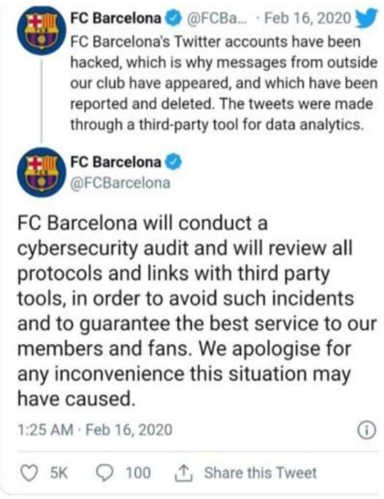
Even if you don't expect to utilize all of your social media platforms right immediately, it's a good idea to reserve your brand's handle on all of them. This makes it simple for others to locate you, but don't forget about the accounts you don't use yet, have stopped using, or don't use often. Hackers may target unmonitored social media accounts and begin sending false messages in your behalf [2].

3.2 Human Error

Everybody makes errors. In today's fast-paced environment, it's all too simple for an employee to expose the organization to internet dangers by inadvertently. According to the EY Global Information Security Survey, "employee vulnerability" was responsible for 20% of cyberattacks. Some online tasks and quizzes might be difficult to complete. Employees may unintentionally cause social media security vulnerabilities by completing them [2].

3.3 Third-Party Apps That Are Vulnerable

It's fantastic to be able to secure your own social media accounts. However, flaws in linked third-party applications may allow hackers to obtain access to protected social media. Hackers gained access to the International Olympic Committee's Twitter accounts. They gained access through a third-party analytics tool. The similar hack happened to FC Barcelona [3].



FC Barcelona @FCBa... · Feb 16, 2020
FC Barcelona's Twitter accounts have been hacked, which is why messages from outside our club have appeared, and which have been reported and deleted. The tweets were made through a third-party tool for data analytics.

FC Barcelona
@FCBarcelona

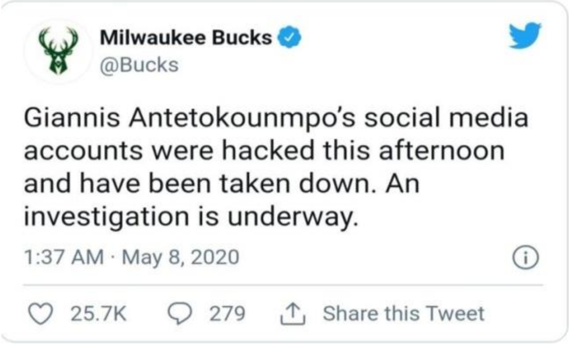
FC Barcelona will conduct a cybersecurity audit and will review all protocols and links with third party tools, in order to avoid such incidents and to guarantee the best service to our members and fans. We apologise for any inconvenience this situation may have caused.

1:25 AM · Feb 16, 2020

Fig -2: Twitter tweet hack example

3.4 Malware and hacking attacks

Hackers who obtain access to your social media accounts might severely harm your band's reputation. Hackers allegedly acquired access to NBA MVP Giannis Antetokounmpo's accounts. His crew had to undertake damage control when they tweeted racist insults and other profanities.



Milwaukee Bucks
@Bucks

Giannis Antetokounmpo's social media accounts were hacked this afternoon and have been taken down. An investigation is underway.

1:37 AM · May 8, 2020

Fig -3: Twitter Accounts Malware Attack

4. METHODOLOGY

4.1 Predicting Social Media Users' Behaviour

Users often link from e-commerce websites to social networking sites like Facebook and Twitter in the age of social commerce. However, there have been few attempts to study the links between consumers' social media accounts and their online shopping habits. This study describes a method for predicting a user's e-commerce buying behaviour based on their social media profile. We are particularly interested in determining if a user's profile information on a social network (such as Facebook) will be used to forecast which product categories the user will purchase (for example eBay Electronics). The article examines how users' Facebook profile information connects to eBay transactions, as well as the efficacy of different feature sets and learning algorithms on the job of predicting buy behaviour.

4.2 Privacy Concerns and Issues

Adolescents might experience both good and harmful impacts from electronic media. When utilized for education, access to good health information, and creating and maintaining social relationships, electronic media may be beneficial. Despite these advantages, electronic media may be hazardous and cause health problems. The authentication techniques of P2P backup and storage systems were examined for the study of password-based authentication in decentralized systems. Following the investigation, new methods for password-based authentication and a new encryption-based access control mechanism were designed to address the privacy issue without losing speed. Lightweight custom simulators were created by Facebook to assess design efficiency. The suggested architectures' security features were carefully examined, but no formal security proofs were provided.

4.3 Potential Threats in Social Networking Sites

The main needs of social networking sites are security and privacy concerns. However, many of the worst crimes continue to exist in all of these social networking sites, and protecting prospective users from these terrible acts has been a difficult issue for many social analysts and engineers. The most common security attacks are divided into three types.
1) Data Breach: Determine the connectivity between nodes and edges, as well as the relationship between them.
2) Passive Attacks: These might be completely undetected and anonymous.
3) Active Attacks: Attempt to connect to opposing nodes and get access to the other nodes by forming new nodes intrinsically.

4.4 Privacy Settings on Social Media Sites

Destinations on social networking platforms attempt to protect privacy settings. As part of their default settings, Facebook and other long-range social communication destinations weaken safety. Clients must go via their client settings to change their protection according to their freedoms. These sites, such as Facebook, allow users to hide personal information such as their birth date, email, phone number, and company status. For those who choose to include this information, Facebook allows users to restrict access to their profiles to just those they identify as "companions." Even this amount of anonymity, however, cannot prevent one of those companions from downloading a snapshot to their own computer and uploading it elsewhere. Regardless, fewer social networking site users have restricted their accounts at this moment.
Take, for example, how users may restrict the display of their profiles to others on a variety of social networking sites: Facebook: Facebook's new user privacy option is set to Friends Only.

To do so, go to Settings
Settings > Privacy > Who will be able to view your future posts?
Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets on Twitter.
To change this, go to Settings > Account > Helpful Links > Edit your public profile on LinkedIn.
To change this setting on Google+, write the name of a Circle in the "To" space underneath your post before publishing it.

5. SOLUTIONS ON SOCIAL MEDIA THREATS

1. The most effective way to guarantee the privacy of your data is to use strong passwords.
2. Use complicated passwords that include upper- and lower-case letters, digits, and special characters. It should be remembered rather than written down.
3. We should be cautious about what we post/share on social media sites, and avoid publishing personal information such as dates of birth, social security numbers, phone numbers, names, and family photos.
4. Only connect our smartphones to allowed Wi-Fi networks, utilize the privacy features given by different mobile operating systems, use auto-lock features, and only download software from authorized app shops.
5. Keep the operating system up to date with the latest patches, enable the firewall, and stay away from cracked applications.
6. Make sure our antivirus is up to date and that we run regular scans.
7. When using the internet, we must be cautious and avoid accessing untrustworthy sites; referral links

to websites should never be clicked; instead, put in the browser's URL address.

8. It's important to only accept friend requests from individuals we know, and to ban anyone who publish offensive information or remarks.

5.1 Advantages

- Individual users may easily communicate with friends and family. You'll pay attention to what other people do and also let them know what's going on in your life via words, photographs, and other media.
- Users may connect with others who share their interests. Social networking makes it simple to join organizations and establish friends with others who share your interests, no matter how odd they may be.
- People can connect with one other across vast distances and across international borders.
- Social networking has the potential to boost voter turnout and assist political change. Elections, boycotts, rallies, and marches may all be organized and carried out via social media.
- In the case of a disaster, such as a storm, wildfire, or terrorist attack, a large number of individuals will be notified rapidly.

5.2 Disadvantages

- Users cannot be certain that their personal information will be kept secure. It should be stolen or, in certain cases, sold by the site itself.
- Social networking sites are used for scams, computer infections, fraud, and identity theft.
- Students utilize social networking sites to cheat and copy their homework.
- People may squander a lot of time on social networking sites for no apparent reason. As a consequence, their professional careers, education, social lives, and even physical health will suffer.
- Companies that use networking face the risk of making a blunder or worse, harming their brand.

6. CONCLUSIONS

In this article, we go into the specifics of social media privacy and security. The majority of this investigation shows that interpersonal organizations pose significant security and protection risks. Organizations must take proper steps to prevent cybercrime, and consumers must safeguard their personal information to prevent abuse. Because cyberspace is becoming a major arena for criminal activity, there is a need for broad coordination across governments to tackle the growing threat of social network security and social media cyber-attacks. All of this research indicates that social networks pose significant security and privacy threats.

REFERENCES

[1] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Comm. ACM 50(10), 94–100 (2007

[2] Mahmood, S.: Online social networks: The overt and covert communication channels for terrorists and beyond. In: IEEE HST, 2012.

[3] Mahmood, S.: New privacy threats for Facebook and Twitter users. In: IEEE 3PGCIC, 2012.

[4] Dey, R., Tang, C., Ross, K.W., Saxena, N.: Estimating age privacy leakage in online social networks. In: INFOCOM, pp. 2836–2840, 2012 70 S. Mahmood.

[5] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), October 2007.

[6] Warren, S.D., Brandeis, L.D.: The right to privacy. Harv. Law Rev. 4(5), 193–220 (1890)

[7] Chaabane, A., Acs, G., Kaafar, M.: You are what you like! Information leakage through users' interests. In: Proc. Annual Network and Distributed System Security Symposium, 2012

[8] Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Comm. ACM 24(2), 84–88 (1981)

[9] Chaum, D.: Blind signatures for untraceable payments. In: CRYPTO, pp. 199–203, 1982

[10] Cooper, B.: Italian drugs fugitive jailed after posting pictures of himself with Barack Obama waxwork in London on Facebook. Mail Online February 14, 2012

[11] Westin, A., Blom-Cooper, L.: Privacy and Freedom. Bodley Head, London (1970).