An Overview of Social Media Security and Creditability

Pooja Jadon, Assistant Professor,

Department of Computer Science and Engineering, Vivekananda Global University, Jaipur

Email Id- pooja.jadon@vgu.ac.in

ABSTRACT: Although the developing social media with its intrinsic capacities seems to be gaining an advantage in terms of comprehensiveness, variety, and wisdom, its security and trustworthiness problems have grown more severe, requiring immediate attention. The existing research, which include model, protocol, mechanism, and algorithm, are mostly focused on both social media content and user security. Unfortunately, there is a dearth of research into effective and efficient assessments and measures for the security and trustworthiness of different social media tools, platforms, and apps, which has a negative impact on their future development and evolution. To address the problem, this study conducted a review of the current status of social media network security and trustworthiness, with a focus on the rising complexity and diversity of assaults, as well as associated intelligence applications. Then we discussed a novel approach to assessing and measuring those basic and underlying platforms, as well as a hierarchical design for crowd assessments based on signaling theory and crowd computing, which is critical for the social media ecosystem. Finally, we discuss a number of unresolved problems and cutting-edge challenges.

KEYWORDS: Crowd computing, Measurement, Security, Social media networks, Trustworthiness.

1. INTRODUCTION

Modern communication networks technology and information technology have produced revolutionary changes in many sectors, disciplines, and every aspect of society across the globe due to their fast growth and everyday refinement. Web 2.0 and Science 2.0 have now evolved into essential network infrastructure and knowledge platforms enabling all participants in the "Global Village" (man, machine, group, and even brain-like computer) to exchange, share, and contribute vast amounts of data, information, knowledge, and wisdom [1]. The social media ecosystem is concerned with the comprehensiveness, variety, and intelligence of social organization, content medium, and stakeholders. As a result, it makes it easier for new virtual social network and organization types to develop.

The usage of social media has exploded in recent years. LinkedIn, Facebook, and MySpace, for example, have become extremely popular and are now the preferred method of contact for many individuals. The importance of these websites stems from the fact that users devote a significant amount of time to updating their information, interacting with other users, and browsing the profiles of other members.

According to the website statista.com, the total number of social media users worldwide will reach 2.13 billion by 2016, up from 970 million in 2010 [2]. This is a 2.2-fold growth in users from 2010 to 2016. As of April 2016, Facebook ranked #1 in the social media market, with about 1.59 billion members. Tencent QQ, the world's fourth most popular social media platform, now has 899 million members. LinkedIn, which is rated twenty-first in terms of user numbers, has a steady user base of 100 million people. According to the current 38th Statistical Report on Internet Development in China published by the official Chinese Internet Network Information Center (CNNIC), China would have 710 million Internet users by June 2016 and a 51.7 percent Internet popularization rate [3]. According to these statistics, half of China's population is online, with 656 million people accessing the Internet mostly via mobile devices.

1.1. Overview on Social Media Security and Trustworthiness:

A spectrum of the following review works is first described at the beginning of the section in order to more clearly convey the major issues and working directions of a few intriguing and significant works [4]. Model, mechanism, algorithm/protocol, mathematical/logic, engineering, and survey are some of the particular categories.

1.1.1. Various Attacks on Social Media:

The different kinds of social media platforms attract a wide range of assaults aimed at stealing users' identities or jeopardizing their privacy and confidence in the network. In this part, we'll go through some of the recent assaults that have been making the rounds on social media.

- *Identity Theft:*

This is a real-time impersonation of a legitimate user in which the attacker takes control of the target profile and successfully convinces other genuine users that the profile is his [5]. The attacker here utilizes the profile in whatever manner he can, which may have serious consequences for the person whose identity it previously was.

- *Malware Attacks:*

They're getting more popular on social networking platforms these days. The attackers email the genuine user malware-infected scripts [6]. When a malicious URL is clicked, malware may be installed on the attacker's devices, or a false website may be launched, attempting to steal personal information from the target user.

- *Spam Attack:*

The attacker has access to the user's communication information and is able to transmit spam or garbage material as a result [7]. The communication data are not difficult to acquire; genuine user profiles may be used to retrieve them. Spam emails sent in bulk create network congestion, and the expense of sending emails is borne mostly by service providers and sometimes by users.

- *Social phishing:*

It is an attack in which the attacker attempts to acquire sensitive information from a target user by impersonating someone the victim knows or by using a phony website that seems to be genuine [8]. These attacks may be substantially minimized if users are aware of the risks and thoroughly check the data they receive.

- *Hijacking:*

It refers to gaining control of another person's profile [9]. If the attacker is able to break the account's login password, they have succeeded in stealing a genuine profile. Weak passwords are therefore a bad option since they increase the risk of being hijacked because dictionary attacks may acquire passwords. It's a good idea to use strong passwords and change them regularly.

- *Impersonation:*

The attacker's goal is to build a false profile and effectively mimic a real-life individual. This attack is extremely dependent on the authentication methods that users encounter when creating a new account. These assaults have the potential to do severe harm to the impersonated victim.

- *Fake Requests:*

To expand their network, the attacker makes a false request using their own profile. If the users accept the fraudulent request, the attacker gains more rights and has access to more information from the victim profiles. Because it is impossible to avoid fraudulent requests, users should exercise more caution while using social media.

1.1.2. Motivations of the Attacks on Social Media:

Attackers, often known as hackers, carry out social media assaults for a variety of reasons. Revenge/emotions, financial gain, amusement, hacktivism, espionage, and cyber warfare are only a few examples.

- *Financial Gains:*

This is the most frequent and significant cause for social media attacks. Cyber thieves get sensitive information about users' bank accounts and maliciously access their accounts in order to achieve financial benefit. It may involve stealing business-related information in order for a competing firm to benefit.

- *Revenge:*

Due to their rage, disagreement, or any sort of vengeance, dissatisfied or unhappy users, or even an organization employee, may launch a cyber-attack on social media. These types of hackers attempt to tarnish the target organization's image by preventing genuine users from using their services. Victim organizations may suffer significant financial losses as a result of such assaults.

- *Expertise for Job:*

Because the majority of IT professionals lack experience in cybersecurity and hacking, there is a strong need for cybersecurity and hacking skills. These occupations have a burgeoning employment market these days. Hiring hackers and cybersecurity experts may assist businesses in better evaluating their security and combating cyber criminals. It is much easier to defeat a criminal if we have someone on our side who can think and function in the same manner as them.

- *Entertainment:*

Some hackers love the adrenaline rush of social media hacking. They carry out attacks in order to earn acclaim for their hacking skills or to achieve reputation among other hackers. They do it for the sake of amusement, not for financial or political benefit. Some guys, it is said, just want to watch the world burn.

- *Hacktivism:*

Hacktivism is the use of computers and computer networks for political purposes, primarily to promote free speech, human rights, and information ethics. This also involves publicizing a political community or religion's goals and viewpoints in order to organize demonstrations in favor of their political/religious convictions. Vandalism of websites with political/religious themes is also included.

2. DISCUSSION

2.1. Social Media Security and Privacy:

Social media has been created by the relationships between users and bodies on the basis of current Internet technology and platform carriers as a form of presentation and typical use of Web 2.0 technology [10]. The initial issues with Internet platforms' secrecy, completeness, and availability persist in social media platforms. Practical application issues linked to security control mechanisms, individual privacy protection, and digital copyright protection have been developed in relation to new platforms, new scenes, and new applications of social media ecosystems.

2.2. Social Media Security and User Behavior:

The never-ending security breaches on social media have given businesses the right to protect information shared over the internet. Any breach of security impedes the organization's ability to develop economically. The behavior of its users, which may be a person or a group, can be studied to evaluate social media. Internet users must be well-informed about the dangers that their personal and financial information may face. They should be able to act in a safe manner and depend on trustworthy security measures to assist them. Their actions are determined by their actual realization and their social media experience. Users who have been victims of identity theft or cyberbullying, for example, will have a completely different perception of security and trust than those who have not.

2.3. Social Media Trust and Evaluations

Another major and important element in the steady existence and effective application of the social media ecosystem is the issue of trustworthiness among social media users, content (service) suppliers, platform owners, and third-party supervisors. Both security and trustworthiness issues are inextricably linked and overlap, and the security of social platforms may influence the trustworthiness concerns of the stakeholders listed above. Users will be more conscious of their safety if trustworthiness is built and strengthened.

2.4. Social Media Security and Reliability:

The quantitative and qualitative examination of security and trustworthiness in social media research is still lacking. They are ill-equipped to cope with today's security and privacy threats. This paper addresses the direction, which is a quantifiable assessment and measurement for trustworthiness and security of social basic platforms, by defining the platform's availability, transparency, and quality assurance as evidence-driven work. To achieve the aim of building a trustworthy, security-preserving social media ecosystem, the research should concentrate on how to assess, measure, and improve (optimize) trustworthiness and security.

2.4.1. Crowd Evaluation:

Stakeholders in social media ecosystems include SMPOs (Social Media Platform Owners), GUs (General Users), CISPs (Content Information Services Providers), ISPs, and SMMs (Social Media Marketing) (Social Media Monitor). The paper discussed a multi-layer architecture for crowd evaluation and measurement based on signaling theory in economics, information management, and crowd computing, including the Featured Signals Layer, the Evaluation/Measurement Layer, and the Enhancement/Optimization Layer, as well as two types of signals and their feedback loops. The multi-layer, which represents the entities and their signal-based operations, as well as data flow between levels.

2.5. Open Issues and Challenges:

Researchers and practitioners in the area of social media networks are still dealing with different assaults from or against social networks and social platforms, and are attempting to deal with the security, privacy, and measurement issues that these attacks provide. We primarily confront the following major open issues and challenges in light of the three elements discussed:

- Because of the numerous, varied, and dynamic characteristics of social media platforms, the formulation of social platform featured signals is an essential step for future crowd assessment and measurement. We need to figure out how to properly describe the common characteristics of platform trustworthiness and security that have been categorized and extracted, especially the development of an ontology formalism for platform behavioral traits.
- Social media allows us to share our knowledge with individuals all over the world. However, it allows companies in charge of our data access to our personal information. People also use social media to disseminate false news in order to create chaos and terror. User trust can only be established by enhancing perceived user control and reducing such dangers, thus these problems must be addressed.
- Finding an efficient technique for building the full dynamics (mathematical) model is required before we can develop the social platform trustworthiness assessment model. This approach should not only evaluate the execution efficiency and computational complexity of the model, but also important aspects of the platform's key trustworthiness from the three highlighted signal sources of services availability, transparency, and quality assurance of social platforms.
- Real-time proxy security solutions need frequent software updates. Furthermore, the problem of an OSN user having no control over the information that other users reveal about him has not been addressed.
- Varied social media users, including both general users and information (content) service providers, have different security requirements depending on the kind of social media, time, place, and situation. The platforms' security and privacy protection standards are essential and relatively constant. As a result, based on the formalism of platform security crowd measurement and the temporal logic of security rules, the optimization of social platform security policy has emerged as an open problem for ensuring fundamental social platform security and obtaining a generally optimized security policy that is common to two types of users. These goals may be accomplished via the use of conflict-free security principles and the development of an optimal approach (model).
- The majority of the defensive methods we've looked at utilize encryption to protect user text from malevolent users, but these strategies fail to effectively encrypt images.
- Companies that handle our personal and financial data; therefore, contact between organizations and consumers is critical for ensuring transparency and trust. Liability is reduced and public confidence is increased by making security warnings and features readily available.
- OSN users' security awareness should be enhanced by giving frequent updates on OSN threats, defensive measures, user responsibilities, and preventive tools.

3. CONCLUSION

This paper primarily provides a state-of-the-art overview of social media security and trustworthiness, followed by a discussion of a new social media security and trustworthiness path. The never-ending security breaches on social media have given businesses the right to protect information shared over the internet. Any breach of security impedes the organization's ability to develop economically. The behavior of its users, which may be a person or a group, can be studied to evaluate social media. Internet users must be well-informed about the dangers that their personal and financial information may face. They should be able to act in a safe manner and depend on trustworthy security measures to assist them. The direction is theoretically important for achieving safe interaction, sharing, and digital rights management of social media material, as well as for continually increasing platform trust and security and creating a trustworthy and secure social media ecosystem. It also offers a more relevant vision and practical application value for the industry's healthy, normal, and fast growth. Users will be more conscious of their safety if trustworthiness is built and strengthened.

REFERENCES:

[1] J. S. Turner, “Global village,” *Rijksmuseum Bulletin*. 2018, doi: 10.52476/trb.9749.

[2] “Statista.” statista.com (accessed Sep. 28, 2018).

[3] “Statistical Report on Internet Development in China,” 2016. https://www.cnnic.com.cn/IDR/ReportDownloads/201611/P020161114573409551742.pdf (accessed Sep. 28, 2018).

[4] D. Tayouri, “The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages,” *Procedia Manuf.*, 2015, doi: 10.1016/j.promfg.2015.07.181.

[5] S. Irshad and T. R. Soomro, “Identity Theft and Social Media,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, 2018.

[6] A. Kumar, N. Ojha, and N. K. Srivastava, “Factors affecting malware attacks: An empirical analysis,” *Purushartha*, 2017, doi: 10.21844/pajmes.v10i02.10569.

[7] I. Inuwa-Dutse, M. Liptrott, and I. Korkontzelos, “Detection of spam-posting accounts on Twitter,” *Neurocomputing*, 2018, doi: 10.1016/j.neucom.2018.07.044.

[8] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Commun. ACM*, 2007, doi: 10.1145/1290958.1290968.

[9] S. R. Veil, J. Reno, R. Freihaut, and J. Oldham, “Online activists vs. Kraft foods: A case of social media hijacking,” *Public Relat. Rev.*, 2014, doi: 10.1016/j.pubrev.2014.11.017.

[10] N. Senthil Kumar, K. Saravanakumar, and K. Deepa, “On Privacy and Security in Social Media - A Comprehensive Study,” 2016, doi: 10.1016/j.procs.2016.02.019.