National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

CERTIFICATE NO : NCLIESMH /2024/C0524570

Assessment of the Effectiveness of Privacy Policies for Data Security on Social Networks

Sudipta Das

Research Scholar, Department of Computer Science and Engineering,
Kalinga University, Raipur, Chhattisgarh.

ABSTRACT

These days, social media have a wide-ranging impact on people's daily lives. The benefits of such networks include the opportunity for individuals to communicate with one another in cyberspace, share information, get to know each other, and get alerts quickly. Furthermore, social networks provide a data set for investigating online communities in many scientific domains, which might lead to new insights. Online services, platforms, or sites where individuals express their opinions, display their interests, and discuss them are often referred to as virtual social networks. Investigating online anonymity in social networks was the driving force for the research. In order to improve digital trust and protect personal data, the report stresses the need of tighter regulatory monitoring, more frequent policy audits, and privacy safeguards that are easier for users to understand and implement.

Keywords: Privacy, Social-Media, Communication, Personal data, Information.

I. INTRODUCTION

Even with social media, a person's life becomes quite public. The personal connections made possible by social media platforms enable users to connect with a larger number of individuals. Users all across the globe may find these people and connect with them, even if they'll never meet in person. Good things may come out of this. Still, a lot of privacy issues come up because of this. Unwanted details about an individual could get out in the public domain. The author adds some complexity to the story by saying that there are many who "believe that the desire to participate in public spaces - and, as a rule, any act of showmanship and propaganda - is incompatible with a desire for privacy." Whatever you put out there on the Internet has the potential to reach a wide audience and spread well beyond your initial circle of acquaintances. Many companies now look at a candidate's social media accounts before making a hiring decision.

A lot of individuals now utilize social media to learn about other people's life. Before ever meeting in person, one may learn a great deal about someone via their written works. The process of gaining access to privacy can never cease. To achieve privacy, according to Boyd, one must be able to

manipulate social status via the use of intricate textual clues, as well as be able to finance technological advancements and adapt to social changes. Understanding societal circumstances for privacy is dynamic, just as society itself is.

More and more people are using the Internet to share information, which has led to the proliferation of mobile apps and social media sites. One emerging trend in mobile technology that combines social networking with wireless communication is the mobile social network (MSN). Profile matching is one of the most well-known features of MSNs; it enables users to discover other users who share their interests and preferences, which may be useful in many contexts, including social ones (e.g., meeting new friends). There are a number of things to think about, despite the method's popularity and usefulness in determining users' shared interests.

In order for matching to work, individuals need to share details about themselves, such as their interests and hobbies, with other users. When interacting with other users, some people want to keep certain details about themselves hidden. They are only willing to be completely transparent about their interests when they are certain that the user shares their interests.

The massive amounts of data processed daily by social media platforms give rise to privacy and security concerns. Message, invitation, picture, and open platform application qualities often provide users access to the private information of others. In addition, users' privacy might be compromised by the tools required to handle their data.

User The term "privacy" refers to a user's desire to keep some information about themselves private, whether that desire is conscious or unconscious. There are several ways in which privacy may be described. The most straightforward explanation is that everyone has the inherent right to choose when and how much of their personal information is shared with others. Evaluating and keeping tabs on users' privacy and security in social networks is another crucial part of privacy and security. One way to look at privacy is via the following lenses.

The Surveillance Perspective

Similar to the Facebook and Twitter revolutions in politics and democracy, web-based social media revolutions are frequently discussed and widely used. Internet freedom and information rights movements on a global scale also have a stronger effect on OSN. Concerns about surveillance arise from an insecure Internet, identity theft, abuse, mining of information based on an individual's identification, and the study of an individual's content area.

The Social Privacy Perspective

Economic revolutions are bolstered by examination of an individual's purchasing interests, and society's interests may be further explored by analysis of travel and living data. All these advantages

notwithstanding, social respect and security may be compromised by an individual's likes, dislikes, position, and preferences.

Parameters of Privacy

Basic user privacy information includes user ID, password, date of birth, address, location, etc. Users may deduce necessary information with the aid of data mining and other methods for extracting, analyzing, and drawing networks.

Limits for Sociality

In terms of social networking and connectivity, there is no system in place to set reasonable boundaries. There is currently no method for a social media user to restrict or conceal postings for certain users; if a person publishes something to their profile, it is accessible to everyone in their network. People on OSN are known to be more than just social media users. In some way, shape, or form, everyone is eavesdropping on everyone else. Now is the moment for the responsible social activist. Social actors need to be governed by some fundamental principles. There is a risk that an expression made on OSN to celebrate an occasion can hurt the person receiving it. In a similar vein, wishing someone well on any occasion may lead to major strife at home.

II. REVIEW OF LITERATURE

Bhattacharya, Munmun et al., (2022) In recent years, online social networks (OSNs) have become more important to people's daily lives. More and more, people nowadays would prefer take part in making content than only consume it. Users are now able to upload audiovisual assets alongside their content, thanks to OSN, among other things. Users of OSNs may participate in online communities where they can express themselves and have meaningful conversations with others. Therefore, the privacy and security concerns linked to OSNs are a major concern for both enterprises and academia. Many studies have been conducted lately to discuss different security and privacy threats associated with OSNs. While several ML-based solutions exist for ensuring the safety of OSNs, no comprehensive assessment has been conducted to date with the goal of classifying and assessing these solutions. In this review, we classify several research on security attacks in OSNs using a thorough taxonomy. After we evaluate and summarize the existing state-of-the-art survey research on OSN security, we will next emphasize their merits and limitations. Following that, we examine all the ongoing initiatives that aim to protect OSNs from security risks via the use of ML-based solutions. At the end of our talk, we'll take a look at what's in store for OSN security in the future, and then we'll go over all the research issues that still need answering, using metrics and possible solutions.

Varalakshmi, Dr. (2020) These days, no one can function without some kind of media technology. The realm of electronic media saw a spectacular ascent. Now more than ever, electronic devices like TVs, cellphones, emails, egames, IOGs, VR games, iPods, IM, social media, esports, and so on are pervasive in the media landscape. Thanks to this, the physical world has shrunk to accommodate current forms of effective communication such as texting, multimedia messaging, video conferencing, virtual meetings, and more. In recent times, social media sites like Facebook, Twitter, WordPress, Whatsapp, LinkedIn, Blogger, Google, Pinterest, Wikipedia, and many more have become important channels for the dissemination of news and information. As the cost of both cellphones and internet connectivity keeps falling, more and more people are able to afford this technology. In addition to providing entertainment, social networks opened up new avenues for business, including sales promotions, marketing research, customer connection development, etc. In this post, we'll look at how social networks impact family ties.

Satyanarayana, Sudarshan et al., (2014) (OSN) open up new vistas of possibility for millions of people by revolutionizing the way people engage with each other. Cybercrimes such as spamming and sending harmful URLs are flourishing on these networks, which is a tragedy because they cause enormous societal and financial harm. Here we take a look at how OSN has become a new target for hackers because to the security holes in the present centralized architecture and the features that drive them. This article gives a thorough review of the current state of these networks with regard to online privacy and security. The article goes on to describe several OSN attack routes and how to defend against them. This literature also discusses the many OSN vulnerabilities and risks. The introduction covers the most common types of dangers, the risks associated with them, and possible solutions to these problems.

Perez Ramos, Marcelo et al., (2011) Sites that allow for online social networking (OSN), such as Twitter, YouTube, and Facebook, are among the most popular websites in the world. When it comes to Mexico, these places are among the best. Users may choose from a variety of features that allow them to read and share information with their contacts and friends, as well as discover others who share their interests. These sites have completely changed the way people meet online. Facebook has 500 million members and Twitter has 175 million users, so it's obvious that both platforms are highly popular. With these kinds of numbers on the rise, we believe there's a great opportunity to study key aspects of online social networks in order to identify the most essential success criteria as seen by end-users. It is possible that identifying such factors may be very helpful for integrating social software features into current information systems as well as for creating new, impactful applications for online social networks. This article details the results of a focus group study that aimed to identify the most important views and concerns about OSN. The results suggest possible lines of inquiry that may be explored further.

National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

III. RELATIONSHIP BETWEEN PRIVACY AND SOCIAL NETWORKS

The proliferation of social media platforms like Meta, Twitter, and Instagram has normalized the sharing of personal information, making online privacy an increasingly pressing issue in the modern day.

Many individuals' private details are among the mountains of data collected by social media platforms. Many people's private details are among the mountains of data collected by social media sites. One positive aspect of data collection is that it helps social networks tailor users' browsing experiences by showing them content, advertisements, and suggestions that are more pertinent to their interests. This makes users' experiences more engaging and cohesive. Also, it makes people wonder about their privacy, especially when it comes to issues like data security and user permission. Some of the most crucial aspects of the privacy-social-network dynamic are as follows:

Collection and Use of Data

- Users' personal details, interests, online activity, and interactions with one another are among the many types of data collected by social networks;
- These networks often utilize this data to tailor the user experience, provide more relevant advertisements, and conduct market research. Concerns over openness and consent are warranted by the amount and nature of the data gathered.

User Consent and Control

- Users should be able to readily find and understand privacy rules that explain the collection and use of data;
- Social networks should provide users the ability to manage the visibility of their data and sharing choices.

Data Security

- Social networks are prime targets for cyberattacks due to the large amounts of data they gather; protecting users' personal information is crucial;
- Using modern security techniques, including encryption, is essential to prevent unauthorized access to user data.

Transparency and Responsibility

- Social media platforms have a duty to be forthright about the data they gather and how they plan to use it, as well as to own up to any mistakes or abuses that may occur.

National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

Compliance with Regulations

- GDPR and other global privacy standards have an effect on social network activities all across the globe, even if privacy laws differ by area.

Emerging Issues

- Biometric data processing and the use of artificial intelligence for behavior analysis are two examples of new privacy concerns brought about by the proliferation of new technology.

IV. SOCIAL NETWORKING PRIVACY ISSUES

Their many uses, notably in sharing and instant chatting, are well-received. But many people are wary of social media because of privacy issues. A lot of individuals are worried that the social media companies' employees would exploit the personal information they have given them against them. In reality, there have been repeated assertions that individuals at all levels of the company may, for various reasons, reveal sensitive information, such as customer data. When that happens, some employees may attempt to obtain customer data by passing the information on to others. This could explain why, even with good security, some people's social media accounts and business websites get compromised.

Concern that total strangers could use their details to contact them is a real concern for some social media users. These two researchers found that among college students, 22% were worried that complete strangers may find out their home address and 40% said the same about social media, namely that it could reveal their class schedules. On their Facebook profiles, the majority of students disclosed both their home address and when they had classes. The pupils said there had to be some kind of protection that would restrict access to their information to just those individuals with whom they have established connections on their profiles. Most students remained worried that complete strangers may access their personal information, even though this is easily fixable by adjusting the privacy settings.

There are social media companies that have taken advantage of its users by using their personal data. Attempts to make money off of Facebook were a top priority in 2007. To that end, Facebook built a software that recorded what its users purchased and shared that data with other websites so that consumers might be notified when the same things become available for purchase. They should have asked people for the information beforehand to avoid violating their privacy. Several commercial and social media websites have allegedly been found to deploy spyware that allows them to access users' private data. Even customers can't share some information on social media, so they may use it to their advantage.

The Single Security Access Sign-On, implemented by the majority of social networks in 2012, is another major privacy risk. People may now access a variety of websites, including social media and business sites, using a single set of login credentials. The majority of users are worried about the potential harm that may come from someone else gaining access to their many login credentials for various websites, which is why they utilize this service. What some individuals would do with this knowledge is unbelievable. The fact that third parties may access a user's information on several sites makes them more likely to attempt to utilize the same data on commercial and even payment sites. Customers may see a message that says they have made a payment using their payment wallets when in fact they have not.

Governments and security experts have not been fond of the idea of merging many social networking sites and using one login credentials. The plans to combine customer data have put Google, the internet communications behemoth, in the spotlight lately. As part of this strategy, which is part of Google's updated privacy policies, users will be able to log in once and access over sixty different Google products—including, but not limited to, YouTube, Gmail, Google Plus, Library, Google Scholar, and books. Google is being smart here as it will spare customers the trouble of remembering a bunch of different login credentials. Additionally, the business may simply identify customers who have violated the terms and conditions among its millions of customers. Although it is a sound technique, many industry insiders worry that it may compromise sensitive data. Many users are worried that social media companies disregard their feedback on privacy settings. The reality is that customers have little influence over the privacy policies that govern their information.

The proliferation of both personal and business websites has coincided, says the Federal Bureau of Standards, with a corresponding spike in cybercrime. Malicious coders all across the globe are slaving away at devising systems that may remotely access sensitive customer information. Among the several strategies used are baiting, phishing, malware, doxing, farming, and phreaking. Large, reputable websites, such as social media platforms, often have minor apps installed. Hackers steal sensitive information, including as login credentials to a website and financial data stored on a user's computer, when they visit websites that have little programs installed by the hackers.

The social media companies are all too aware of the fact that malicious coders from all over the globe are hell-bent on gaining access to user information. There have been recent allegations that an unknown number of PCs throughout the globe were infected with key logger malware. More than two million accounts on various social media platforms were allegedly compromised, impacting some of the most popular websites. The hackers stole login credentials and other personal information from over 250,000 Twitter accounts in early 2013. For the purpose of exposing Facebook's security holes, a Palestinian information systems researcher named Khalil Shreateh broke into Facebook founder Mark Zuckerberg's account in August 2013. He boasted that he could secretly publish anything on other people's accounts.

Many are concerned about their privacy as a result of the widespread security holes found on social media services. Many people, including experts, wonder why social media companies can't take better measures to secure their websites and prevent unauthorized access to user data. Even if sharing on social media sites may need certain personal information, the vast majority of users still believe that service providers should take reasonable precautions to keep their data secure. Google Plus is one of the social media platforms that has taken additional precautions to safeguard user information. As a result, prominent social media platforms have been under intense pressure to beef up their security measures, particularly Twitter and Facebook.

Over the last decade, social networking sites' use has skyrocketed. These websites allow up to 1.3 billion individuals, both young and elderly, from all over the globe to exchange photos and information with one another. Politicians are also promoting their ideology to potential voters via social media. The next decade should see this tendency accelerate even more. To be sure, customer confidentiality is a major issue. Ethical hackers and renegade programmers have exposed major security holes in the majority of social media platforms. Improving the safety of customer data necessitates immediately fixing the existing security holes.

It is the obligation of social media companies to safeguard their users' personal information by using robust security measures, such as robust encryption. Also, these businesses should make sure that no one person has access to customer information on an individual basis. There is a chance that the government may use its power and resources to force social media companies to improve the security of their customers' personal information.

Privacy Leaks and Privacy Measures in OSNs

Users' personal information being leaked is another major concern. Leakage of user privacy occurs as a result of identity theft attacks. Unique identifiers that may lead to the disclosure of additional information are limited to email IDs. There are few privacy concerns as pressing as the revelation of one's location. Smartphones not only have cutting-edge Internet access, but they also give location data derived from GPS and other online sources. Upgraded social network software that allow for real-time communication and information sharing are also available on these smart phones. In order to fix the issue of location sharing in mOSNs, the mobile share architecture was implemented. Some suggestions for better location data collection are made.

Using the kanonymity approach, the authors advocated for the categorization of information sources as either trustworthy or untrustworthy. When it comes to group communication, users rely on OSNs. Inviting spammers to do the basic four tasks are:

(i) controlling entity of the entire OSN
(ii) well-defined interactions

(iii) user Identity
(iv) multiple interfaces of OSN providing different views.

On OSNs, spams propagate with the purpose of gathering user data and actions, which in turn leads to privacy leaks. To protect oneself against Identity Theft, one might use both traditional and technology means of coping.

V. PRIVACY CONCERNS ASSOCIATED WITH OSN USERS

In terms of the formation and shaping of social ties, many people's lives have been changed by the adoption and use of OSNs. One major issue that has arisen as a result of this expansion is the issue of personal privacy. Privacy is not a novel idea, but the SLR uncovered new privacy risks due to the widespread use of OSN, which are detailed below:

Data Leakage

A concern about privacy in online social networks is the possibility of abuse and disclosure of users' profiles and personal information. As the number of posts made by users increases, there is a greater amount of data that might be used maliciously. Particular bits of personally identifiable information and the unique identifiers of OSN users were among the material was leaked. Using Request-URIs, Referrer headers, and cookies, OSNs routinely show that user identification information is leaked to at least one third party. Information leakage and location leakage were added to the original concept of data leakage in OSN.

The core concept of social media is freely exchanging and sharing information with peers. Such sensitive and private information may have unintended consequences for OSN users, as some users even provide health-related data. Concerning location-leakage, it's worth noting that most OSN user's access social networks using mobile devices. This fact alone could persuade individuals to disclose their exact whereabouts. As a result, cybercriminals might use users' geolocation data to commit crimes on social media.

Disclosure of Sensitive Information

"Personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent" is how Dinev defines information sensitivity. Evidence suggests that consumers' perceptions of danger are heightened when dealing with sensitive material.

Therefore, a major worry for OSN users is the leaking of sensitive information. Despite the fact that OSN profiles had the ability to reveal a lot of personal information, users were only making around a quarter of their profile information public, which may be seen as an intentional attempt to keep crucial details hidden.

Research has shown that consumers' privacy concerns are heightened when dealing with sensitive information. Data leaks or malicious third-party apps might be to blame. Theft of the identity of an unwary OSN user is another potential consequence of the exposure of sensitive information.

Third-Party Applications

To facilitate the development of third-party apps that may run on their platform, a number of OSNs provide an Application Programming Interface (API). Since these apps store codes somewhere other than the OSN, which is outside the authority of the users, there are legitimate privacy issues. In order to obtain data on social network users for advertising and commercial interests, third-party apps may either monitor their activities or provide access to ad partners.

When it comes to the collection and use of personal data, OSN customers don't have much say over the matter. Previous research has also shown that although third-party apps are widely utilized for harmless reasons, they are often used by malicious actors to get access to many accounts and spread spam and malware on open social networks (OSNs).

Identity Theft

The reason for this is because OSNs include a lot of personally identifying information, such actual name, birthdate, and location. The frequency of identity theft is also the most often mentioned worry among OSN users, according to research. The results demonstrated that both internal and external sources may launch such an assault on OSNs. Accepting friend requests from strangers, giving up account information, or clicking on links to other websites are all potential causes of this issue for OSN users.

Control Over Personal Information

The lack of proper control over personal information retained by social media sites is a problem for many OSN users. The timing, method, and scope of data collection, use, and disclosure are all aspects of user privacy that should be customizable. Users remain dubious about the security of their shared information, even if OSNs provide data owners a limited degree of control over access via customizable settings, which means that some contents may be concealed from unwanted access.

Further, people often want greater say over how and when their data is shared (i.e., they'll be more forthcoming with sensitive information if they can decide which bits of data will be shared). Users of OSNs are often in the dark about how their data is being used, or at least not involved in the process, and the widespread gathering of personal information is seen as intrusive.

VI. STRATEGIES TO PROTECT USERS' PRIVACY

To address consumers' privacy concerns, many approaches have been proposed. Typically, these are the methods or resources that people use to keep their data secure and reduce the likelihood of a privacy breach.

National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

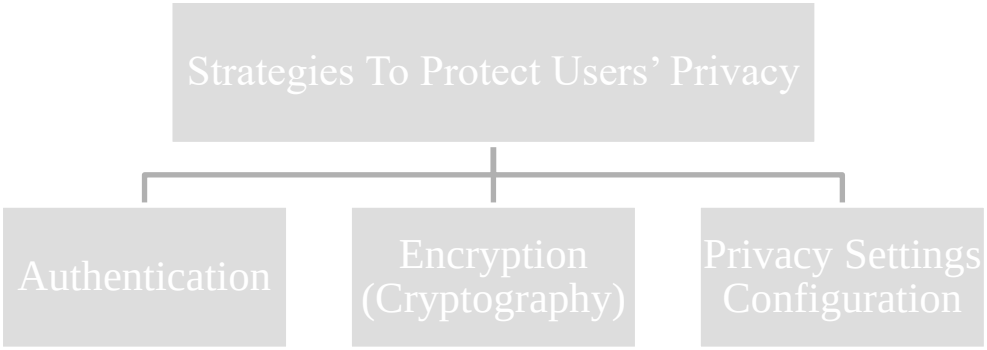

Figure 1: Strategies to Protect Users' Privacy

Authentication

Attributing messages to their senders and establishing user authentication are prerequisites for achieving privacy, security, and access control. In an effort to ensure that each user is a genuine person, Facebook, for one, has implemented authentication mechanisms like CAPTCHA. Furthermore, OSN users should enable secure browsing and any other available authentication methods, such two-factor authentication, wherever practicable. An additional measure to mitigate consumers' privacy concerns is the implementation of numerous firewall levels of security.

Encryption (Cryptography)

There are thousands of attacks on social media platforms every second. To prevent impersonation and phishing attacks, which can have a significant impact on users, it is recommended that data be protected using cryptographic keys, which can be computationally expensive. Social media platforms like Facebook and Twitter have used SSL encryption to safeguard user information. Thus, OSN users may also employ stronger encryption techniques to offer secrecy and, in certain cases, secure parts of their profile and instant messages exchanged via these platforms, since integrity is the foundation for both.

Privacy Settings Configuration

With privacy settings, users may hide information from friends or groups and prevent other users from illegal access to their data. According to research, many OSN users do not make use of the privacy options that are accessible to them. Users on OSNs are often less private than ideal when they refuse to adjust their privacy settings. The majority of the time, people employ privacy settings on OSNs for their own convenience. Protecting one's private information from prying eyes is a breeze with the many user privacy options offered by OSNs. Users do not make advantage of the elaborate privacy settings because they are perplexed by them and do not want certain audiences to be able to see their information. It has been noted that a small percentage of users are routinely checking their privacy settings, although a larger percentage are aware of the availability of these options.

So, it's highly recommended that OSN users maintain their individual privacy settings and make full use of the privacy-protection features offered by their OSNs. In a same vein, users are encouraged to often adjust their privacy settings to a more stringent state, as several OSNs do so with each update.

VII. PRIVACY POLICIES ON OSN

When it comes to exchanging information, one area where OSNs aim to satisfy user expectations about privacy protection is paramount. Users of OSNs should be able to easily and adaptably communicate their privacy choices to one another, outside parties, and OSN service providers via the rules in place. Essentially, consumers need reassurance that privacy rules are easy to find. Consequently, the question of how to stop the abuse of user data must be addressed by privacy rules and other privacy preservation procedures. There was a correlation between users' familiarity with privacy regulations and the likelihood that they would disclose personally identifiable information, particularly regarding the sharing of their information. Even when consumers do read privacy policies, they often fail to fully grasp their contents. For example, customers may assess the pros of using a service against any possible privacy misuse worries, determining that the advantages exceed the costs of reading complex privacy regulations in their entirety.

According to another finding, many users don't bother to read the rules because they think they're too lengthy and tedious. As a consequence, users aren't informed, which might affect their actions negatively. This is supported by previous studies that have shown that privacy rules are difficult to comprehend for many users due to issues with readability, format, usage of legalese, special idioms, and unique terminology. Because the rules aren't written in a way that the typical, non-technical user can comprehend, the OSN provider may change them without the users knowing, which greatly increases the danger of privacy breaches. When users expressed serious concerns about data sharing practices and a lack of trust in the privacy policy, a data privacy risk emerged.

If privacy policies are shown by default, users could be prompted to evaluate them and might even spend a considerable amount of time reading them. This would imply that privacy rules should ideally be simple, easy to understand, thorough, and easy to read. Even though people who use OSNs may be concerned about their privacy, they may still choose to reveal personal information because of the advantages they may get from using these services. On the one hand, OSN users express legitimate privacy concerns, while on the other, the platform does nothing to address these issues. Many people find this policy-breaking quite offensive, and they frequently point to it as an example of the "privacy paradox"—the situation in which users say they care about privacy but really don't give it any thought.

VIII. CONCLUSION

The study highlights that while online social networks have transformed global communication and connectivity, they also expose users to unprecedented privacy and security challenges. The assessment of existing privacy policies reveals that most social networking platforms have

established extensive policy frameworks to address data protection; however, the effectiveness of these measures remains limited by gaps in implementation, user awareness, and regulatory oversight. Many users continue to accept default settings without fully understanding the implications of data sharing, reflecting a mismatch between policy intent and real-world practice. The findings underscore the need for privacy policies that are not only legally comprehensive but also user-centric, transparent, and easily comprehensible. Social media companies must strengthen enforcement mechanisms, simplify privacy controls, and communicate policy changes clearly to ensure informed consent. Governments and regulatory bodies, in turn, should play a proactive role in enforcing compliance and ensuring accountability. Safeguarding privacy in social networks requires a collaborative approach involving platform providers, policymakers, and users. A balance between innovation and privacy protection is essential for maintaining user trust, securing personal data, and fostering a safe and responsible digital environment.

REFERENCES

1. G.-J. A., S. Mohamed, and A. S., "Security and privacy in social networks," *IEEE Internet Comput.*, vol. 15, no. 3, pp. 10–12, 2011.
2. M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 4, pp. 2019–2036, 2014.
3. D. Singh, R. Sinha, P. Songara, and R. Rathi, "Vulnerabilities and attacks targeting social networks and industrial control systems," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 133–142, 2014.
4. K. S. Rook, "Social networks in later life," *Curr. Dir. Psychol. Sci.*, vol. 24, no. 1, pp. 45–51, 2015.
5. M. Al-Qurishi et al., "SybilTrap: A graph-based semi-supervised Sybil defense scheme for online social networks," *Concurr. Comput.*, vol. 30, no. 5, pp. 1–10, 2018.
6. J. Song, N. Jamous, and K. Turowski, "A dynamic perspective: Local interactions driving the spread of social networks," *Enterp. Inf. Syst.*, vol. 13, no. 2, pp. 219–235, 2019.
7. S. R. Sahoo and B. B. Gupta, "Classification of various attacks and their defence mechanism in online social networks: A survey," *Enterp. Inf. Syst.*, vol. 13, no. 6, pp. 832–864, 2019.
8. N. Dakiche, F. B. S. Tayeb, Y. Slimani, and K. Benatchba, "Tracking community evolution in social networks: A survey," *Inf. Process. Manage.*, vol. 56, no. 3, pp. 1084–1102, 2019.
9. S. R. Sahoo and B. B. Gupta, "Fake profile detection in multimedia big data on online social networks," *Int. J. Inf. Comput. Secur.*, vol. 12, no. 2–3, pp. 303–331, 2020.
10. M. Ghosh, S. Das, and P. Das, "Dynamics and control of delayed rumor propagation through social networks," *J. Appl. Math. Comput.*, vol. 68, no. 1, pp. 3011–3040, 2021.
11. M. P. Ramos and J. Gomez, "Why do people use social networks?," *Commun. IIMA*, vol. 11, no. 2, pp. 41–50, 2011, doi: 10.58729/1941-6687.1162.

12. H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Social network security issues in online social networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, 2011, doi: 10.1109/MIC.2011.50.
13. S. Satyanarayana, K. Sood, Y. Tao, and S. Yu, "Security and privacy in online social networks: A survey," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 1, no. 1, pp. 1–12, 2014, doi: 10.4108/inis.1.1.e3.
14. Varalakshmi, "Influence of cybersecurity on social networks," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 7, pp. 43–46, 2020, doi: 10.35940/ijitee.G4863.059720.
15. M. Bhattacharya, S. Roy, S. Chattopadhyay, A. K. Das, and S. Shetty, "A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges," *Secur. Privacy*, vol. 6, no. 1, 2022, doi: 10.1002/spy2.275.