Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

Design and Implementation of Privacy and Security System in Social Media

Ramesh Kumar
Research Scholar, Department of Computer Science & Engg, Nims University Rajasthan, Jaipur
Email: rks208@gmail.com
Dr. Parveen Kumar
Professor, Department of Computer Science & Engg, Nims University Rajasthan, Jaipur
Email: pk223475@gmail.com
Dr. Vinay Kumar
Ex-Professor, Department of Information Technology, VIPS, New Delhi
Email: vinay5861@gmail.com

ABSTRACT

Privacy and security are the main concern of any social media networking sites such as Facebook, Twitter Instagram and LinkedIn etc. The primary purpose of these sites is to allow people to share interests, activities, real-life connections. Nowadays social networking sites are the main source of communication and on the other hand these sites are the peak targets for misusing the data and information. This is the fact that the maximum numbers of users are not aware about cyber threats and their lack of knowledge leads to further increase in cyber-crimes is a major challenge. Users should aware in the concerned of security and privacy during creating the account on social media, to read the instruction and follow it. There is some setting in social media platform to secure the message and share to only authorize users. Various governments and businesses are taking a variety of steps to combat cybercrime. Despite many steps, cyber security remains a major issue for many people. This paper focuses on the issues that cyber security faces in the modern era. It also covers the most up-to-date information on cyber security tactics, ethics, and trends that are transforming the face of cyber security.

Keywords - **Data privacy, cyber security, cyber crime, cyber ethics, social media, cloud computing.**

Date of Submission: Dec 07, 2021 Date of Acceptance: Feb 22, 2022

1. INTRODUCTION

Online Social media (OSMs) refer to the platforms of interactions among people in which they can create, share, and exchange information, knowledge and ideas in virtual communities across the networks. The office of communicating and marketing manage the main Facebook, Twitter, LinkedIn, Instagram and YouTube account. Online social media (OSMs) have become a common cultural phenomenon for millions of Internet users. Combining user- constructed profiles with communication mechanisms that enable users to be pseudo-permanently “in contact”, OSMs leverage users’ real-world social relationships and blend even more our online and lives. As of 2021, Facebook has 3 billion monthly active users and it is the third most popular and visited site on the Internet. Twitter, a social micro-blogging platform, claims over 330 million monthly active users and 206 million daily active users on Twitter, who send Tweets in more than 40 languages. OSMs are currently dramatically revolutionizing the way people interact, thus becoming de facto a primary service on the web, today one the impact of this paradigm change on demographic and technical aspects of collaboration and interaction is comparable to that caused by the deployment of World Wide Web in the 1990’s**.** As a result of the popularity, availability, and accessibility of social networking sites (SNSs) during the last decade, people's interactions have gradually transformed. In terms of leisure, information, contact, and communication, social networking sites (SNSs) have changed our life. Because of advancements in automation and Internet usage, nearly everyone now uses social networking sites to share information and communicate with their relatives, friends, partners, and family members. These social networking sites allow people at remote locations to interact with each other very quickly and at minimum cost. On the other side, the security and privacy of SNS users' information has been jeopardized, with the majority of users unaware of this fact. The ratio of cyber attack executed through networking sites is gradually high. It has become a huge problem to find a solution that would give better security for social network members. The goal of this review is to gather information and evaluate all reliable and effective studies that have looked into security issues and solutions on social networking sites. Our goal is to extract and describe the most important security features and methodologies from chosen research publications so that academics and practitioners may get a quick overview of security solutions.

We undertake a secondary study in this review by accessing past studies devoted to SNSs security threats and novel security techniques to protect them from attacks. We conduct thorough evaluation of 84 previous studies, including journal papers and conference proceedings published in high-impact journals, using standard systematic literature review techniques. According to the findings, 2013 was the most popular year for researchers to pay attention to security issues on SNSs, with 23

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

important security issues uncovered. Researchers frequently site Facebook and Twitter as examples of SNSs platforms with security issues. We discovered that the two main drivers of today's security and privacy vulnerabilities on SNSs are people (users) and the social networking sites themselves. To summaries, security and privacy issues on social networking sites are still an unsolved problem, and there is now no firm and complete solution for completely eliminating those issues on the sociability of social networking sites, which could jeopardize user privacy. Due to the prevalence of security and privacy issues on social networking sites, social service providers have attempted to address these issues for their users by improving privacy settings and restricting privacy levels [1]. The security metrics or goals, on the other hand, are not totally met. The recent Sony photo data breach [3] and the Heartbleed vulnerability [2] provide compelling evidence of this. Similarly, security issues are encountered more frequently on SNSs as the number of SNSs increases. These difficulties inspire us to investigate a variety of Social networking site security risks and security approaches using systematic literature reviews (SLRs) [4] to establish why security issues on Social networking sites are still a problem and why researchers' efforts have not entirely succeeded.

There are many effective ways to protect your personal information when using the social media platform such as unique and secure password and taking advantages of two-factor authentication. If two –factor authentication is configure to your mobile the hackers cannot login if they do get hold of your password. As a user we should keep the password at least 16 character long with alphanumeric and special character. In social media platform generally you have seen the friend request, before accepting your friend request you have to check the user account authentication. Because most of the account could be fake and you don't click on the unknown link. If you click the unknown link it will create a problem and there is probability to hack your account.

On the other hand Education and awareness play the key role to defend against the social engineering attacks and there are many examples of good practice in deploying such operation. Specially, In this case Internet service provider (ISPs) play the important role and engagement with users to help and build a innovative ideas, knowledge base around incident and threats encourage consumers to proactively protect themselves. These activities can improve security not just for the end user and the ISPs but for the online ecosystem as a whole world.

Users should aware about the latest malware and cyber attacks: As we know that, every day new malware and the new concepts of cyber crime is appearing across the network. The reason to appear the new malware and new concepts of cyber attack is, hackers are continuously experiment the new concepts of attack and spread across the network for money and damaging the assets. So, that as a users and ISPs provider both has the accountability to look at the new cyber attacks and malware to protect itself.

ONE-TIME password can minimize the unauthorized access: Social engineers are introducing various new techniques, methods for phishing attacks, honestly individual users and organizations are suffering from such types of attacks. Without knowing, the user personal account, banking account, social media account, any digital platform accounts are hacked or access by hackers and same things happening with the organization. If we apply the ONE-TIME password for login verification then unauthorized users can not access the other account without his or her permission.

Protect users by default from worldwide cyberattacks and act collectively to identify and respond to known threats: Internet Service Providers (ISPs) can play a major role to identify and help to prevent or mitigate worldwide cyber attacks before they reach the user's machine. If ISPs provider should be fully active and monitoring all user's related networks then the attacks rate could be dramatically reduce. ISPs provider can deploy the security tools to monitoring the incoming and outgoing packets across the networks and it should define what should and should not be blocked from reaching customers. Efforts are underway in a number of countries to explore criteria for how to decide what should and should not be blocked, and to ensure transparency on processes undertaken and oversight.

2. LITERATURE REVIEW

Das et al. [5] presented a report on cyber security challenges for social networking sites (SNS). Also covered were the risks and lack of understanding of users that lead to cybercrime, as well as the applications of Social Networking Sites such as digital marketing, social e-commerce, and branding. Jang and Julian[6] gave an overview of the security threats present in current hardware, software, and network layers. They also talked about new attack patterns in areas including social media, cloud computing, smart phone technology, and critical infrastructure. A survey of consumers' views on security and privacy of popular social networking sites was done by Jabee and Afshar [7], and privacy enhancement in Facebook is also discussed. Soumya and Revathi [8] talked about network threats and provided strategies to combat them.

ElMrabet et al[9] looked at security needs, described serious cyber-attacks, and presented a cyber-security strategy to detect those cyber-attacks. Senthil Kumar and Sathish Kumar [10] presented a study on cyber security awareness among students in Tamil Nadu institutions, as well as a discussion of various security dangers on social networking sites. Kirichenko et al. [11] offered a brief overview of cyber-threat detection approaches. In relation to social networks, graph theory and data mining are also studied. It also includes the JEL Classification: C38, 45, 55, 61, 63. Kayes et al. [12] gave an overview of new

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

privacy and security concerns in online social networks. Attacks on privacy and security, as well as their responses, are briefly discussed. Fire et al [13] offered an overview of available solutions that can provide improved safety, security, and privacy for online social networking users, as well as a detailed evaluation of numerous security and privacy risks. They also made a few recommendations for users to improve social networking site security and privacy.

Albladiet.al[14] provided a novel approach for determining user susceptibility based on several online user characteristics. The authors demonstrate that main user attributes have a direct or indirect impact on an online user's security danger. Senthil Kumar et al. [15] conducted a comprehensive survey on privacy and security problems in social networking sites, analyzed the main causes of security issues, and provided some policies and suggestions for online users. Wajeb and Maha [16] looked at cyber dangers on social networking sites and offered anti-threat methods.

Kumar et al .al[17] The history of online social sites, their types, and potential threats and methods to address these concerns were presented. Different cyber risks are reviewed by Omar [18], as well as possible cyber security measures to improve security and privacy. Canongia et al. [19] introduced the topic of cyber security, its current importance, and the challenges of the emerging Information Society, whose critical development determinants include technological revolution and innovation. This article provides an overview of national cyber security strategies in developed countries, such as the United States and the United Kingdom, as well as a study case, Brazil, which is taking its first steps toward cyber security, and concludes by proposing a model for developing a Brazilian cyber security strategy.

According to a survey conducted in the United Kingdom, Facebook's security settings are confusing to its users. Almost half of Facebook users don't keep track of changes to their privacy and security settings on a regular basis (Tahseen, 2011). Facebook's privacy policies have been updated eight times, including one that automatically notifies users where they are and another that allow third parties to access users' phone numbers and addresses (Tahseen, 2011).

According to The Montreal Gazette, a University of British Columbia investigation exposed Facebook's security mechanism after it failed to thwart a large-scale attack that collected personal information from Facebook users' profiles. Bots, or computer-generated phoney Facebook profiles controlled by programming, were used to acquire 250 gigabytes of data from Facebook users, according to the researchers (Shaw, 2011). The bots gathered this information over the course of eight weeks, starting with buddy requests. From the phoney account to roughly 5,000 random Facebook users, an exploratory study of a user's Facebook security and privacy settings was conducted. When people accepted the requests, the bot used Facebook services like Friend-Finder to send friend invites. If a network contains fraudulent or phished Facebook users, users may be subject to data theft and misinformation operations (Shaw, 2011).

Many users are concerned about the security of their Facebook account due to Facebook's constant changes to privacy and security settings. In December 2011, Facebook founder Mark Zuckerberg was hacked when 14 private photos of Zuckerberg leaked to photo-sharing sites with the caption: "It's time to solve those security holes." Facebook later stated that the attack was the product of a recent code update and that it was only active for a short time, affecting thousands of user accounts in addition to the founder's (Burnham, 2011).

Facebook and other social media platforms is "rewriting the norms" of social participation, according to Sheryl Sandberg, Facebook's Chief Operating Officer (Consumer Reports, 2012). Facebook has teamed up with the Department of Labor and other organizations to help job seekers and companies by building technologies that make job posts go viral. The network, for example, keeps active-duty soldiers in touch with their families and enables for the easy posting of severe weather warnings. Millions of people use Facebook to share their opinions on government and industry, extending their aggregate impact in ways never imagined before (Consumer Reports, 2012).

Alessandro Acquisti and Ralph Gross of Carnegie Mellon University conducted extensive research in the area of Facebook security, including Imagined Communities Awareness, Information Sharing, and Privacy on Facebook. In 2006, when social networking was just beginning to become a global phenomenon, these authors conducted a poll of fellow university students who used Facebook. The researchers investigated for an underlying demographic or behavioral difference between members and nonmembers of the network, as well as the influence of privacy concerns (Acquisti and Gross, 2006).

The study discovered that an individual's privacy concerns are just a marginal predictor of network membership. Indeed, people who are concerned about their privacy join the network and reveal a considerable deal of personal information. Some people dealt with their concerns about privacy by believing in their power to control the information they share and who has access to it. However, researchers discovered that some members have considerable misconceptions regarding the online community's reach and the visibility of their profiles (Acquisti and Gross, 2006).

One of the most important subjects at the moment is "security and privacy measurements in social networks." According to this topic, the study team can see how important it is to explore these issues. This one is relevant to today's society, which is why the group chose it as the subject of their group investigation. Many researchers

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

have conducted study pertinent to the topic. Many researchers have conducted study pertinent to the topic. "Security and privacy in online social networks" is one of Levcio Antonin Cutillo's research projects on the subject. Online social networks that are centralized pose a threat to their users' privacy since social network providers have unrestricted access to personal data, according to study conducted by the Royal Institute of Technology. [20].

3. MAJOR SECURITY ISSUES ACROSS THE SOCIAL NETWORKING SITES

User created information and personal information, such as private data, images, and basic information, will be included in a user's online activity on any social networking site (name, place, location). Maintaining social identity while jeopardizing social privacy is a difficult issue for any social network user. According to estimates, the number of social networking site users will reach 3 billion in 2021, accounting for one-third of the global population. Through unauthorized access, malicious people obtain access to the user's private information and other useful information from social networking sites and launch attacks. Unauthorized users with information obtained from social networking sites may engage in undesired and criminal actions such as hacking, spoofing, and phishing, among others, endangering the privacy and security of online social network members.

Security and privacy difficulties on social networking platforms are entirely related to user behaviour, rather than a technology issue. The more personal information consumers reveal, the greater the risk of a security breaches. Posting sensitive and secret content increases the danger of vulnerabilities, and those contents are seen by a large number of people, making it easier for malevolent users to exploit a flaw and get access to a private account or network. Because threats change over time, security must evolve to keep up. Even if user security settings are properly setup, there is no guarantee that new settings will not be added. Changes may occur on your computer or other Internet-connected devices, as well as on the websites themselves.

4. ATTACKS AND CHALLENGES IN SOCIAL NETWORKING SITES

Phishing - To track user information, this cyber-attacker uses e-mails and websites. Disgusting e-mails target sensitive information such as credit card details and passwords. Unauthorized purchases, identity theft, and money looting are all concerns that arise as a result of phishing. In a commercial setting, phishing can have negative consequences such as a loss of market share, consumer trust, and reputation.

Hacking - It's when someone gains unauthorized access to a computer system or a network. Hacking is never considered unethical. Computer specialists that hack for personal benefit are known as black hat hackers. Grey hat hackers alert the network's administrator about the network's security flaws.

Spam - Spam nowadays uses social networks and tries to degrade the network by advertising, introducing dangerous code, and gathering sensitive information, whereas spam previously solely targeted e-mails. Instant Messaging spam, Forum and comment spam, and mobile phone spam are all examples of today's spam.

Identity Theft - Unauthorized individuals attack using an application that asks for permission to access the information in a social networking site's profile. When a user consents, they gain access to all of the information and can use it without the user's awareness.

Virus - Any malicious software that tries to gain access to the user's computer system. When software or files are transferred across a network, viruses propagate. Viruses have the ability to infect system resources, software, modify applications, and the system's fundamental functions.

Spoofing - By impersonating a trusted entity, fraudulent users get access to a user's account or system. Email spoofing and IP spoofing are examples of this. Email spoofing entails seeking private sensitive data and financial information from a trustworthy sender via e-mail. These spoofing e-mails could also contain trojans and other malicious software. The majority of IP spoofing attacks target the entire network. To impersonate the originating entity, malicious users choose an IP address and change the packet headers transmitted from their own system.

Password Sniffing - Malicious programming that examines network data in order to trace usernames and passwords. To prevent these types of attacks, many encryption standards have been established for protocols.

Worm - Malicious code that replicates and spreads over the network. These worms can be found in spam e-mails or instant messages as attachments. Worms have the ability to alter and corrupt user files, as well as introduce malicious code. Furthermore, these worms clog up the shared network and take up hard disc space.

5. WAY TO MANAGE YOUR SOCIAL MEDIA PRIVACY SETTINGS ON SOCIAL NETWORKS

Every major social media sites, like Facebook, Twitter, LinkedIn and Instagram, offers how to protect privacy in a better ways, but it’s up to users to use and customize them:

Facebook Privacy Settings

1. **Log on Facebook and click on "Settings"**
2. **Then Select “Privacy Settings”**

You can change the profile access to control who view your posts and who cannot. You can choose to share your posts and contact information with your Facebook friends, and not for general public. That will stop the hacker from viewing your Facebook account.

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

For most cases, you can choose to share items with Everyone, Friends of friends, and Friends. You can control various things, including:

- Who can check your posts (past and future)
- If you want to review anything you are tagged in before it posts
- You can limit the audience for things you have previously shared with friends of friends or the public

You can also control in your settings how people find and connect with you, such as:

- Who can send you friend requests
- Who can see your friends list
- Who can look you up using the email you provided
- Who can look you up using the phone number you provided
- If you want search engines outside of Facebook to link to your profile

3. **You can also change various Facebook settings in the "Security and Login" section of Settings and monitor your usage: In this section users can monitor periodically what he / she have using and check the suspicious account.**

4. **If you visit the "Apps and Websites" section, you can monitor if and what apps are able to access your Facebook data or information.**

Twitter Privacy Settings

To update privacy settings on Twitter, log on and click on "Settings and privacy" in the menu: In this section users can set the account privacy.

In the main "Account" settings, you'll be able to:

- Review your login verification methods (set up two-factor authentication)
- Select if you want to require personal information (email/phone number) for a password change
- Request your Twitter archive

2. The "**Privacy and safety settings**" in Twitter are where users will be able to allow the general public to view your Tweets or to have your Tweets protected.

In the Twitter privacy page, just check the box next to "Protect my Tweets" to wall of strangers from your Twitter feed. You can also select to avoid including your location in the time of tweeting. That gives you an extra measure of protection if you're traveling or are away from home for an extended length of time.

3. The "Passwords" section in Twitter's settings allows you to change your password.

4. **The Twitter "Apps" settings** section lets you see what if any apps are connected to your Twitter account and lets you 'Revoke Access' to any you want to remove.

LinkedIn Privacy Settings

Basically, professionals create a profile to connect with group of people with same and different profile. This social media is the way of communicating and exchange the information, ideas in groups.

1. Once you are logged in to your account you select the "Privacy & Settings". Users can set the privacy of various activities i.e. account, Ads and communication.
2. **In "Account" settings, you can also view "Partners and Services"** to see who you've shared access to your LinkedIn Account with and who can access your LinkedIn data.
3. **The "Privacy" settings** let you select what others see and how LinkedIn uses your data. You can choose for updates to be seen only by you, your connections, or the general public. You can also download your LinkedIn data here as well.

6. TECHNIQUES TO PREVENTION OF CYBER ATTACKS ON SOCIAL NETWORKING SITES

6.1 Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls

To keep your computers and information safe, use strong passwords and use separate passwords for various accounts. A "brute force attack" is when a hacker uses readily available software tools to try millions of character combinations in an attempt to gain access to a system without permission. Passwords should be at least twelve characters long, but larger passwords are more difficult to guess because there are more characters to decipher. Immediately after installing new software, and on a frequent basis thereafter, change all default passwords, especially for administrator accounts and control system devices. Other password security features, such as an account lock-out that occurs after a certain number of incorrect passwords have been entered should be implemented. Multi-factor authentication, which includes users proving their identity – via codes delivered to previously registered devices – whenever they attempt to sign in, is another option.

6.2 Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates

The majority of vendors work carefully to produce patches for vulnerabilities that have been identified. Many systems remain vulnerable long after patches and upgrades have been provided because businesses are either unaware of or choose not to implement these solutions. Verizon discovered in its 2016 Data Breach Investigations Report that only three patterns cover three quarters of events and breaches in most sectors. These patterns were cyber espionage, crimeware, and denial of service for utilities. Understanding the components of an attack (for example, a kill chain) can aid in the construction of defenses and the detection of a breach, according to the report. Because the top ten cyber vulnerabilities accounted for 85 percent of successfully exploited traffic, effective patching can also stop a big amount of attacks.

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

6.3 Develop and Enforce Policies on Mobile Devices

In the workplace, the growth of laptops, tablets, smart phones, and other mobile devices poses substantial security risks. Because of their mobility nature, these devices are vulnerable to external, hacked applications and networks, as well as hostile actors. The growing tendency of firms enabling employees to use their personal electronic devices for work reasons, known as the "Bring Your Own Device (BYOD)" phenomenon, is adding to this difficulty.

As a result, it's critical to establish standards in your office and on your networks about the reasonable use of mobile devices. These policies should be rigorously followed by all employees and contractors. Password-protected devices should also be used to ensure that only authorized individuals may access them. Otherwise, an unauthorized user can utilize an authorized user's device to obtain access to restricted networks and files. Employees should also avoid or exercise caution while using devices that do not belong to them because they cannot be certain that they are properly protected or adhere to existing rules. These devices may be contaminated, and using them puts the information and networks you use at risk.

6.4 Firewall

It is a piece of hardware or software that acts as a barrier between an organization's network and the internet, shielding it from risks such as viruses, malware, and hackers. It can be used to restrict who has access to your network and who can send you information.

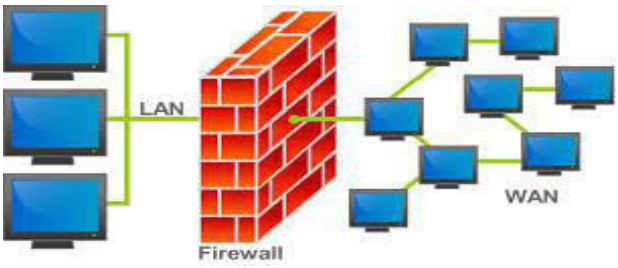

Figure-1: Firewall

In an enterprise, there are two types of traffic: inbound traffic and outbound traffic. It is possible to configure and monitor the traffic of the ports using a firewall. Only packets from trusted source addresses are allowed to enter the organization's network, while blacklisted and unauthorized addresses are denied access. Firewalls are necessary to protect the network from illegal access, but they cannot guarantee this unless they are configured correctly. A firewall can be built using either hardware or software, or a combination of the two.

- **Hardware Firewalls:** Routers, which connect the network to the network outside the business, such as the Internet, are an example of hardware firewalls.
- **Software Firewalls:** These firewalls are deployed on both the server and client devices, and they serve as a gateway to the company's network.

6.5 Anti-virus software

Anti-virus is a protection tool that you install on your computer or mobile device to prevent malware from infecting it. The term "malware" refers to any malicious software, including viruses, worms, Trojan horses, and spyware. Malware is derived from a combination of the phrases malicious and software. A cyber attacker can collect all of your keystrokes, steal your papers, or use your computer to target others if your computer is infected with malware. Any operating system, including Mac OS X and Linux, can be infected, contrary to popular belief.

Anti-virus software detects malware in one of two ways: signature detection or behaviour detection. Signature detection works in the same way as the human immune system does. It looks for features or signatures of harmful programmers on your computer. It accomplishes this by using a malware dictionary. The programme tries to neutralize something on your machine that matches a pattern in the dictionary. The dictionary approach, like the human immune system, requires updates, such as flu shots, to protect against new malware strains. Anti-virus software can only protect you from what it considers to be hazardous. The issue is that cyber criminals are generating new malware at such a rapid pace that anti-virus firms are unable to keep up. As a result, no matter how recent your anti-virus software has been updated, there is always a new form of malware that can potentially defeat it.

6.6 Avoid linking personal and business accounts

Hackers' task is made considerably easier by linked accounts, which provide access to several accounts if one account is accessed. Different usernames and passwords are required for each account. Provide only the administrative privileges that are required, and limit any excess privileges that could lead to a cyber attack.

6.7 Avoid clicking on unnecessary links

These fake links may contain viruses or spyware that can harm a user's computer and get access to personal information such as usernames, passwords, account numbers, and credit card details. Spoofing might occur when you click and download an unexpected communication from someone.

6.8 Securing home network

The first step is to keep a problem-free machine and to make sure that any internet-connected devices are running the most recent operating system, web browser, and security software. Mobile devices that connect to your wireless network are included in this. Review security options on a regular basis, use a firewall, verify that all devices connected to the internet are protected, plug and scan before starting work, and store backups. Public wireless networks and hotspots are insecure, and they can monitor your activity while you're connected. When using public Wi-Fi, keep your online activity to a minimum and avoid logging into accounts like email and banking.

7. CYBER ETHICS

"Character is what you do when no one is looking," says an old saying. The same is true with the Internet. People

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

can feel invisible and capable of doing things they wouldn't do in person or in public, even if they know they're wrong, when they're online. As the Internet becomes a more vital part of daily life, it's more important than ever to resurrect the concept of "citizenship" and apply it to the online world. "Cyber citizenship," "cyber ethics," and "netiquette," all relatively new words, refer to appropriate cyber social behaviour. When no one else is looking, these terms apply to what people do online. As our children spend more time online, teaching them about cyber ethics is essential, especially since bad e-habits can begin at a young age. Unfortunately, we are realizing all too well that children with computers can be harmful and cause serious damage and harm, whether they are attempting to be mischievous or committing cybercrime on purpose. To assist enforce ethical online behaviour [21], the Computer Ethics Institute publishes the Ten Commandments of Computer Ethics.

- Do not use your computer to cause harm to others.
- Interfere with other people's computer work as little as possible.
- Snooping through other people's computer files is not a good idea.
- Using a computer to steal is not a good idea.
- Do not use a computer to testify falsely.
- You must not replicate or use proprietary software that you have not paid for.
- Do not utilize another person's computer resources without their permission or payment.
- Do not plagiarize the intellectual outputs of others.

8. FUTURE WORK

According to the survey and literature review on social media platform and different types of cyber attacks, password authentication required for users login. The server can verify the users' authentication through OTP (one-time-password).

9. CONCLUSIONS

In today's digital world, social networking websites are increasingly disclosing user private information, corporate information, and other sensitive stuff. On the other hand cyber security professionals continue to upgrade and expand security measures for social media accounts, security threats and vulnerabilities continue to rise at an alarming rate. This survey focused on how to protect user's social network personal information. It examined users' awareness of the risks and threats to their personal information privacy, and highlighted the need to develop a new privacy system supported by mobile internet devices. Because most of the users use their mobile phones for internet services, privacy settings should be compatible with mobile phones need to be developed. The method of selecting privacy settings should also be simplified to provide users with a clear picture for the data that will be shared with others. Users should accountable to aware about the latest malware and cyber attacks and the other hand Internet Service Providers (ISPs) can play a major role to identify and help to prevent or mitigate worldwide cyber attacks before they reach the user's machine. If ISPs provider should be fully active and monitoring all user's related networks then the attacks rate could be dramatically reduce.

REFERENCES

[1] Aimeur, E., Gambs, S., & Ho, A. (2010). Towards a Privacy-Enhanced Social Networking Site. *International Conference on Availability, Reliability and Security*. pp. 172-179

[2] Labs, V. (2014). Majority of Global 2000 Organizations Have Not Remediated Heartbleed, Remain Vulnerable to Cyber Attacks. Venafi Labs Q3 Heartbleed Threat Research Analysis.

[3] Walker, D. (2014). Experts take inventory of Sony Pictures data leak, potential costs. Available at: http://www.scmagazine.com/experts-take-inventory-of-sony-pictures-data-leak-potential-costs/article/386991/

[4] Kitchenham, B. (2004). Procedures for performing systematic reviews. Joint Technical Report, 33(2004), pp. 1-26.

[5] Das, Rituparna, and Mayank Patel. "Cyber Security for Social Networking Sites: Issues, Challenges And Solutions." *International Journal for Research in Applied Science & Engineering Technology* (IJRASET) 5.4,833-838 (2017).

[6] Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences 80.5 (2014):* 973-993.

[7] Jabee, Roshan, and M. Afshar Alam. "Issues and challenges of cyber security for social networking sites (Facebook)." *International Journal of Computer Applications 144.3 (2016):* 36-40.

[8] Soumya, T. R., and S. Revathy. "Survey on threats in online social media." 2018 *International Conference on Communication and Signal Processing* (ICCSP). IEEE, 2018.

[9] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). "Cyber-security in smart grid: Survey and challenges." Computers & Electrical Engineering, 67, 469-482.

[10] Senthilkumar, K., &Easwaramoorthy, S. (2017, November). "A Survey on Cyber Security awareness among college students in Tamil Nadu." In IOP Conference Series Materials Science and Engineering (Vol. 263).

[11] Kirichenko, L., Radivilova, T., & Carlsson, A. (2018). "Detecting cyber threats through social network analysis: short survey. " arXiv preprint arXiv:1805.06680.

Volume: 13 Issue: 04 Pages: 5081-5088(2022) ISSN: 0975-0290

[12] Kayes, I., &Iamnitchi, A. (2017). "Privacy and security in online social networks: A survey." Online Social Networks and Media, 3, 1-21.

[13] Fire, M., Goldschmidt, R., &Elovici, Y. (2014). "Online social networks: threats and solutions." IEEE Communications Surveys & Tutorials, 16(4), 2019-2036.

[14] Albladi, S. M., & Weir, G. R. (2020). "Predicting individuals' vulnerability to social engineering in social networks." Cyber security, 3(1), 1-19.

[15] Senthil Kumar, N., Saravanakumar, K., & Deepa, K. (2016)." On privacy and security in social media–a comprehensive study." Procedia Computer Science, 78, 114-119.

[16] Gharibi, Wajeb, and MahaShaabi. "Cyber threats in social networking websites." arXiv preprint arXiv:1202.2420 (2012).

[17] Kumar, Sunil, and Vikash Somani. "Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques." International Journal of Advance Research in Computer Science and Management 4.4 (2018): 125-129.

[18] Al Mushayt, Omar Saeed. "Threats and anti-threats strategies for social networking websites." *International Journal of Computer Networks & Communications* (IJCNC) Vol 5 (2013).

[19] Canongia, Claudia, and Raphael Mandarino. "Cyber security: The new challenge of the information society." Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions. IGI Global, 2012. 165-184.

[20] Zanero, S, D Keromytis , " Security and privacy measurements in social networks". Available:http://nsl.cs.columbia.edu/papers/2014/lessons.badgers14.pdf [Accessed: 25 July 2016]D Gunter , Solomon S, "The Danger of Data Exfiltration over Social Media Sites" , Western International University, Available: https://media.blackhat.com/bh-us-12/Briefings/Gunter/BH_US_12_Gunter_Sonya_SNSCat_WP.pdf [Accessed: 19 July 2016

[21] http://www.cybercitizenship.org/ethics/.

Biographies and Photographs

Ramesh Kumar is a Ph.D Scholar, Nims University Rajasthan, Jaipur. He completed BCA and MCA from Central University IGNOU and M.Tech in Computer Science & Engineering from NIMS University, Rajasthan, Jaipur. He has 15 years of experience in Academic, Research and Industry with different organization. He started his career as a software developer when he joined TOQSOFT Technologies, Bangalore. He worked three years and then joined CMC Pvt. Ltd. as a Sr. Faculty in 2008. After, he worked with NIMS University as Sr. Lecturer from 2009 to 2013. He worked five years as Sr. faculty with Mahan Institute of Technology, New Delhi from 2015 to 2019. His research area is Privacy and Cyber Security, Cloud Computing.

Dr.Parveen Kumar did his Ph.D from Kurukshetra University, Kurukshetra. Before that he completed Master of Science in Software System from BITS Pilani, MCA from Kurukshetra University and B.Sc. (Non-Medical) from Kurukshetra University Presently working as Professor in the Department of Computer Science & Engineering, NIMS University Jaipur, Rajasthan since 4.11.15. Worked as HOD (CSIT), Chairperson (BOS, CSIT), Dean (Student Welfare), actively involved in NAAC Accreditation. Guiding PhD Scholars. Worked as Professor and Head, Dept of Computer Sc & Engineering, Amity University Gurgaon, from 9.5.14 to 7.7.15. Also remained Member (Board of Studies), Member (Flying Squad, Exams), and Chairperson (Library Committee).

Dr. Vinay Kumar worked as scientist in National Informatics Centre (NIC), Government of India for approximately 21 years. He also worked with Vivekananda Institute of Professional Studies (VIPS), affiliated to GGSIPU, as Professor and Dean of the IT Department and Department of Research and Publication. He has extensively contributed to the knowledge arena through his books and research publications. He has published over 100 research papers in refereed journals and authored a book of Discrete Mathematics and a memoire *Killed Instinct.*

He is a LMCSI and past Chairman of CSI Delhi Chapter for year 2020-21.