Flaws in Privacy and Security of Facebook

Akhil Kumar[1*], Sapna Jain[2], Rajkumar Yadav[3]

[1]Master of Technology Computer Science and Engineering, MRKIET College, Rewari
[2]Department of Computer Science, MRKIET College, Rewari
[3]Department of Computer Science, I.G.University Meerpur, Rewari

Corresponding Author: akhil123401@gmail.com

Abstract *-* In today's era the massive online social networking places like Facebook, WeChat and WhatsApp, etc where are different-different working background peoples including students linked/connected to each other through a social networking media, and sharing of our thought, picture, videos with our family and friends. The main motive of this study is to highlight the default privacy setting and security of Facebook is breach due to the fake account, fake news and third parties on these sites. Facebook is a virtual online meeting space for the world where a huge volume of information is shared. Every second user of Facebook doesn't have any knowledge about privacy setting. Privacy matter is strongly related to third parties to access Facebook user information. The risk with this platform is that it may fall within the wrong hands and people become a victim of hacking, identify theft, cyberstalking, child soliciting, and Abuse, etc.

Keywords: Social media, Hacking, Facebook, Fake Account, cyberstalking.

I.   INTRODUCTION

In the recent few years, Facebook strongly establishes ownself on the social networking world. Facebook is an effective path of communication between friends and others. Behind the fast and sudden growth of Facebook is that Facebook gives permission to use to build a new own online identity profile under the limited area. According to the new report on Facebook, Worldwide the number of one-month active users of Facebook is over 2320 million. In every single second approx 5 new user profiles are built. There are 84million fake profiles on Facebook. 4.75 billion content on facebook shared daily. In nowadays the life of youth without Facebook is out of think. The goal of social media users is to build a profile/connection and keep the relationship. Now the generation is changed people use social media for our fun and sharing unnecessary data. In Facebook, there are many privacy and security considerations that need to be noticed. The Internet is written with permanent ink, not with granite. The figure-1 showing the progressive countries depending on the amount of Facebook users. Facebook has 260 million active users in India. The amount of users only in India is 25% in Aisa Region.
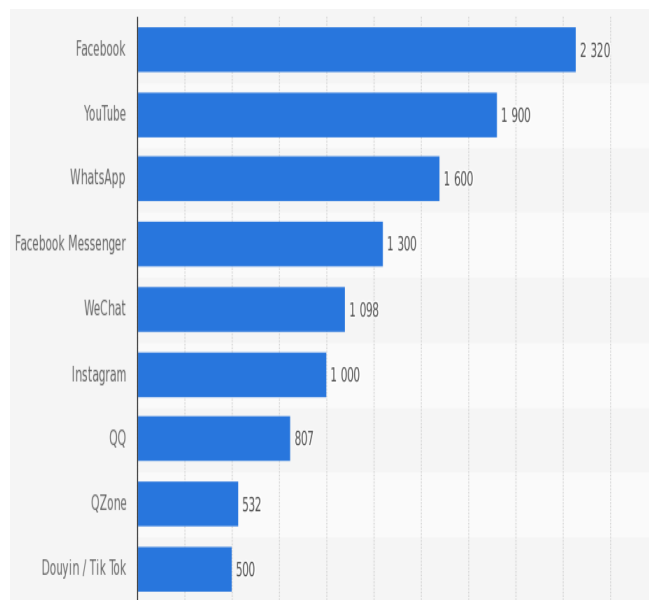

Figure 1. Facebook users (April 2019 in millions)

Many users upload and share themselves private Details on online social media and this information is accessible and hackable by the unknown person. It means it helps to increases the flaws in Facebook privacy settings and security. But many Facebook users have no knowledge about its privacy setting and its usages. User information sharing process on Facebook has shown below in (figure 2).
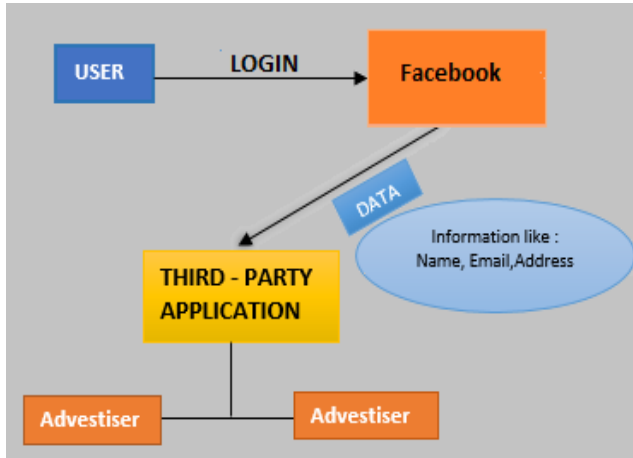
Figure 2. Data sharing model.

II. LITERATURE REVIEW

Facebook is a popular social network in every age of peoples especially in teenagers and younger adults. Most of the user share and upload personal details online on Facebook, which means sharing information with the user who has same Taste like as photos, like, dislike, relationship, status, current home town details, etc. Unfortunately, most of the Facebook user is not aware of privacy risk. According to customer security risk survey (in 2014 by Kaspersky lab) showing the risk when the user used a mobile/tablet device for accessing social networking websites. 78% of the Facebook user did not a problem with their information to be managed and intended by online cyber-crime. The survey also found that 1/10 of Facebook user can share and converse to unknown person about personal details or information, and 12% of users using open wireless-fidelity(wi-fi) internet to submit Facebook account details, as well as only 20% of Facebook user they worried that their personal details appearance is more or not and 7% seriously noticed the way of communication using Social Network site is one of the key reason which data will be lost.

When a person registers on Facebook and he or she ever opens that account, then Facebook shows a pop-up card screen in which user fill your personal information, private details, Education details, current location, and interest area, etc. Each and mostly SNS have some rights to ask users to complete themselves profile which includes private user details including Username, address, interest, Date of Birth and so on. This information can be simply read by an unknown person. In most of the cases, user fill actual details to make facebook account profile. The current privacy setting of Facebook is not enough for the user, which means many user read and theft more data from other users.

Chi Z., Sun S. Showed how privacy is more important for any SNS. In this research paper, this report targets the security flaws for the privacy setting of Facebook. Another

unknown party can access facebook user personal and public information (information that's stored online social network) without the site's direct connection. "The authors say that the unique privacy and security design presented by basic functionalities of social media network and using social network theory users can reduce these design flaws".

Some prior studies are based on Social media privacy. and security. According to the previous study, the security and privacy both are two main concern of SNS user's can be described into those concern:
- What personal and secret data information shared with whom.
- Exchange of messages between two users without any interruption. Which means no third person is not able to see those messages.
- What and how anyone can send message unsung/ anonymously.

Privacy is the first main concern in selecting online social media. The user gives more priority to privacy system because privacy is related to user personal information.

Seigneur and Jensen told us mostly teenager and youth have responsible for social network privacy leaks(Dimitrios M., Ioannis M). In the current date, the amount of fake account of Facebook is in millions, for example, In particular, users created a profile of two different teenagers with fake name and details (one Male user and other is Female user). Friend request was sent massively to other Facebook users. Consequently, two Social networks of friends were designed and provide power to access the users' personal information. Both facebook user admits the friend request and makes a new relation on facebook. In simple words, the report leads to results that appear several threats for teenager and vital issues around the privacy of online social media users".

Tootoonchian A., Yashar G. Provide advice on this paper is predicated on Locker system, users are able to use a locker to enhance the privacy of online Social Networking systems. "First, it split social networking material from all different practicality that Online Social Network give. Second, locker provides a feature in which a digitally verified social relationship want to access social information cannot be reused by the online social network for unmotivated function. This feature reduces the deserve to others of online social content that users handed to Online social network suppliers. In Last, Locker system allows message cryptography employing a social connection key. Suppose two anonymous users with a particular common friend that check their online Connection while not open it to all others, a typical privacy issue once passing information during a suburbanized scenario".

In the report of Krishnamurthy and Wills characterized and measured different privacy facets across aside SNS using the

method of bits of share detail. They also highlight that many other websites, unauthorized third-party websites track user's movements in online Social Sites. opposite to comprehensive beliefs.

J. Kramer-Duffield gives consulting on how to improve the online SNS privacy setting for users. To ignore personal identity stolen, they suggest build profiles private for friends only, which will reduce the personal data stolen chance on online Social Networking sites

III. OBJECTIVE AND HYPOTHESIS

A. Objectives: Every survey and report has one main objective, without knowing any objective users cannot do a good survey or research. The objective of this research is that, where Facebook is failed to stop unwanted activities running on Facebook. These are some main objective that came out from this research.

These are some main key objective, and they are related to this research.
1. To examine the connection among exchanging of details or information on the Facebook platform and reportedly privacy setting.
2. To examine the wrong impact of fake account on the Facebook privacy and security system

B. Research Hypothesis:
1. **Hypothesis 1:** The H1 States, the Security, and privacy are two main predictors in picking a social networking site. Is they will change their privacy policy and security.
2. **Hypothesis 2:** H2 States, in future Facebook will improve your privacy setting against duplicate or fake account running already on Facebook platform.
3. **Hypothesis 3:** H3 states a Facebook user used custom privacy setting, are more secure against online attack on personal information.

IV. METHODOLOGY

This survey used "Survey Monkey" for user feedback collection. In this survey Facebook used for data gathering process, take some screen-shot from Facebook, and collect information from an online journal. In This survey there are six questions (five multiple choices and one is a short question), these all questions are related to user privacy and fake or duplicate account, and this survey was distributed for gathering user feedback. The Survey was set up through the voting software Survey Monkey. This survey was distributed to Facebook users and collect information from there. The survey enclosed open-ended queries, wherever responding participants may specific their opinions relating to Facebook privacy and security. This survey was held on a small scale. In this survey, 100 Facebook users participate and provide feedback. In this survey 50 students, 20 teenagers, and 30 adults have aged over 30-35 years.

The study allowed the investigator to see however social networking is employed in student's lives by distinguishing Three hypotheses: **Hypothesis 1** state that, mostly user wants better privacy and security in social networking site like facebook. Privacy is the main factor in choosing Facebook more likely to change their settings on at least a monthly basis. Privacy means the condition of existing alone, or the right to take one's personal affairs and relationship cryptic. **Hypothesis 2** state that, The number of duplicates and fake account in million and currently they usage extra space on Facebook. By using the duplicate account any anonymous or unknown user can affect your personal information (Name, Home address, Interest, Educational Information, etc.). **Hypothesis 3** state that most of the Facebook users they used default privacy setting but they have no knowledge about an online attack like virus or malware attacks, ID theft attack. In the custom privacy setting, users are not 100% sure they are secure against online attacks but custom privacy setting provides better security than default privacy setting. The survey question is given below.

A. Questionnaire:
1. The default Facebook privacy setting is enough for the user.
   Perfect | Good | Enough | Less Enough.
2. Is Facebook is a trustable social networking site.
   Yes | No | Need Some Improvement | Other.
3. Fake account affects your personal information Stored on facebook online**.**
   Yes | No | I don't know | Other (specify).
4. How much surety of your personal information is safe on Facebook.
   10-30% | 31-60% | 61-90% | Other (specify).
5. Fake news is a threat or not for Facebook privacy concern.
   Yes | No | I don't know | Other (specify).
6. What's your opinion about to stop fake news and fake account.
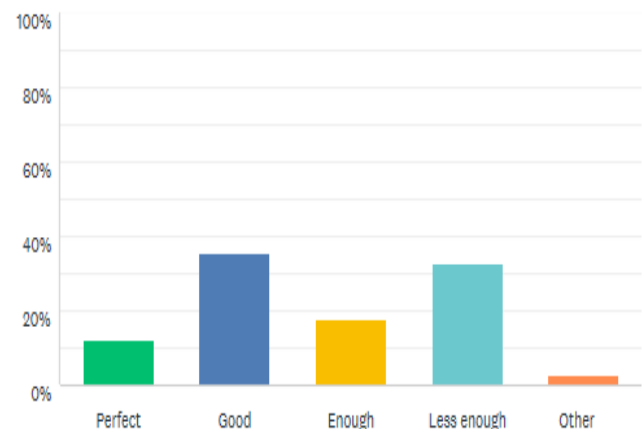
V. RESULT

Figure 1. Users feedback on the default privacy setting.

There are 100 users, they have different working background who participated in this study. **35.20%** user said the default setting is good and **32.35%** of Facebook user said the default privacy is less enough and **18%** of user agreed with enough privacy setting.
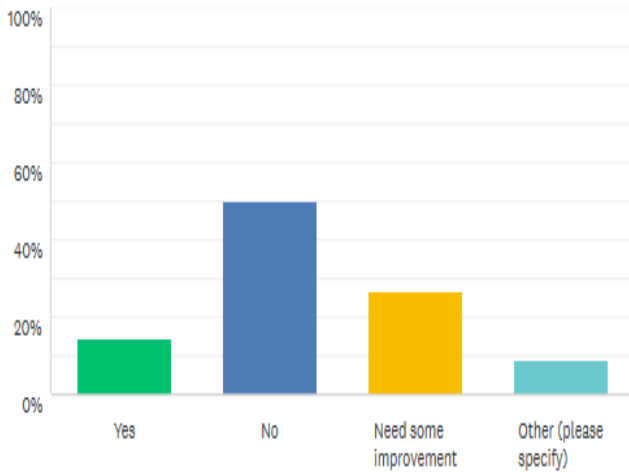

Figure 2. Feedback of users on Facebook trust.

On the base of Facebook is a trustable social networking site or not. **50%** of users said Facebook is not a trusted site and **27%** users said Facebook "Need some-Improvement". The **15%** user said Facebook is a trusted social networking site and 8% user have no issue with Facebook, Is Facebook trusted site or not. **14.71%** of user have trust on Facebook.
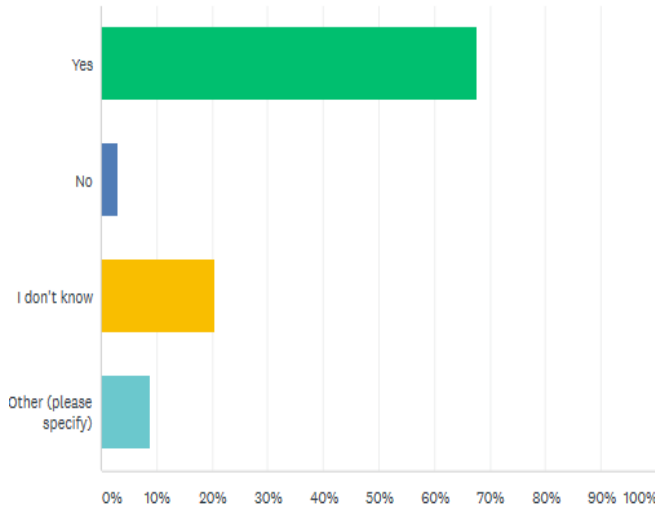

Figure 3. User feedback on fake account activities.

67% of users agreed with, the fake accounts affect personal information stored on Facebook. Surprisingly many users have no knowledge about the fake account and fake news resource. The feedback of **20%** of users said "they don't know" is a fake account affect personal information stored on Facebook. **3%** of user said fake account doesn't affect their personal details.
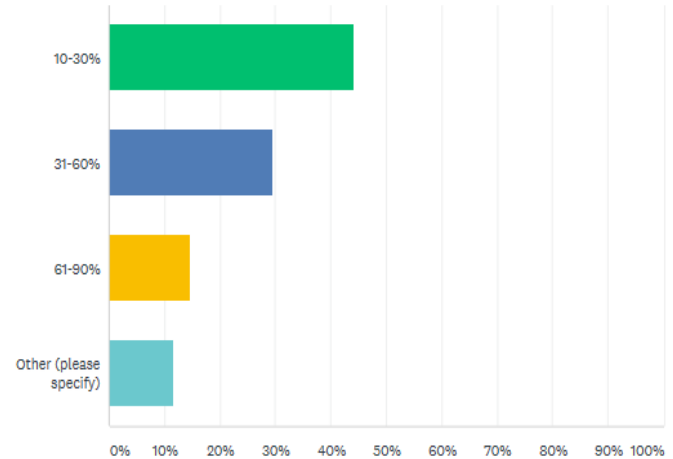

Figure 4. users feedback on personal information is safe on Facebook.

Every user wants a better and secure privacy setting, a setting that protects user personal information to others. **44%** user said **10-30%** user personal data is safe on Facebook and **29%** users agreed about **31-60%** data is safe on Facebook.
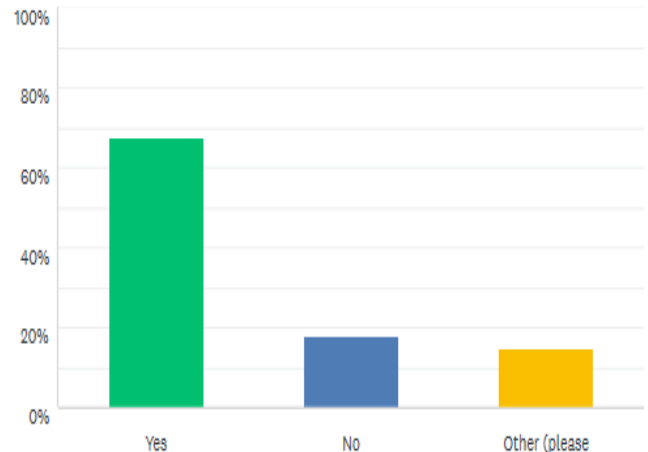

Figure 5. Users feedback on fake news as a threat.

Fake news is a concern related to the user privacy setting. Use of fake news any anonymous user can help to increase the unwanted resource on Facebook. **68%** of user said that fake news may be a threat to Facebook.

In the last, Most of the user tell facebook to need more improvement in the field of duplicate account and, link Facebook ID with one Govt ID like Aadhar card and most of the user said that Facebook takes strict action against unwanted activities on Facebook.

VI. PRIVACY FLAWS ON FACEBOOK

We know Facebook could be a huge space for analysis and plenty of varieties of analysis are already done on Facebook

privacy and security, Security flaws on facebook privacy. In line with a report of "Massachusetts Institute of Technology" establish how Facebook affects our user privacy. In this research paper, we noticed some privacy and security threats which will arise by Facebook or Facebook user.

1. **Facebook**: In 2013, according to report peoples are quitting Facebook in concern with privacy. The main reason behind this matter they feel, the current privacy is not enough when they used Facebook media. In such case when a Facebook user tries to switch from Facebook to another SNS than some information of user still saved on the Facebook platform but the information is hidden for another user.

2. **Single-Tap Sign In:** Using the username and password, we can easily access Facebook on one click. This is a privacy concern for a Facebook user, which using the default Facebook privacy setting. Using custom setting like using two-tap verification setting we can make a secure Facebook account.

3. **Third-Party Advertising:** Most of the companies use Facebook as an Advertisement publishing platform because the number of Facebook users in billion and companies show attractive aids on Facebook. Facebook show third parties ads on our platform for money collection because the third party pays some amount of money to Facebook for publishing their ads. In FTC report many internet sites they access business advertising gather in personal data from kids.

4. **Fake or Duplicate Accounts.**
5. **Fake News Source Identification.**
6. **Personal ID Theft.**

VII. CONCLUSION & FUTURE SCOPE

In this research, highlight the need for many improvements in privacy setting to Facebook need to stop online attacks and expose personal information publically. In the world of social networking sites the user more concern about how much privacy still has. As our survey report, 70% of users are students and they have no issue with the default privacy and security but they have a suggestion for Facebook needs improvement in the default privacy policy. 8% of user said that Facebook is a trusted social networking site whereas 52% don't trust. For the user, privacy safety Facebook takes a strict step toward the fake accounts. Facebook needs to change its privacy policies and improve it and make it user-friendly and at the same time, Facebook should stop access to the third party so that there is no threat to its user personal information. In total 64% of, users want to improve privacy setting for their Facebook account.

If we like to make this research even better in the future, then some need to spread this survey on a large scale in which user can include more questionnaire (should be related to user privacy and security) and after collect feedback and information from users, and on the bases of user feedback researcher can be built a better report for future. Beside from Facebook even on internet many online chatting websites and they have a need for more security and privacy improvement.

REFERENCES

[1] Chewie M., Hayikader S., Hasan M H. and Ibrahim J. 2015 How Much Privacy We Still Have on Social Network?. International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015 Edition, page no:1.

[2] Adgaonkar, A. and Shaikh, H. 2015 Privacy in Online Social Networks (OSNs). International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[3] D. Boyd and E. Hargittai. 2010. Facebook privacy settings: Who cares?" Journal on the Internet, 15(8), 2010.

[4] Leitch S and Warren M. Security Issues Challenging Facebook.

[5] Hashimoto G T., Rosa P.F., Filho E.L. and Machado J M. 2010. A Security Framework to Protect Against Social Networks Services Threats. Fifth International Conference on Systems and Networks Communications.

[6] Shabir G., Hameed M.Y., Safdar G. and Gilani S.M.F.S. 2014.The Impact of Social Media on Youth: A Case Study of Bahawalpur City. Asian Journal of Social Sciences & Humanities Vol. 3(4) November 2014.

[7] Al-Darwish A.A., Al-Joudi A.S., Al-Gahtani H.B, and Al-Qahtani M.S. Social Networks Benefits, Privacy, and Identity Theft: KSA Case Study (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 12, 2014.

[8] Guy-Hermann Ngambeket Ndiandukue." Social Networks and Privacy— Threats and Protection ." Isaca Journal, Volume 5, 2012.

[9] A. Srivastava and G. Geethakumari, "Measuring Privacy Leaks in Online Social Networks," International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100, 2013.

[10] B2B International In Conjunction and KasperskyLab, "CONSUMER SECURITY RISKS SURVEY 2014: MULTI-DEVICE THREATS IN A MULTI-DEVICE WORLD," Kaspersky Lab, 2014.

[11] X. Chen and S. Shi, "A Literature Review of Privacy Research on Social Network Sites," International Conference on Multimedia Information Networking and Security, pp. 93-97, 2009.

[12] C. Wüest, "The Risks of Social Networking," Symantec Corporation, 2010.

[13] G.-H. N. Ndiandukue, "Social Networks and Privacy—Threats and Protection," ISACA, vol. 5, pp. 19-23, 2012.

[14] A. Al has, "Threats of the online social network," Seminar on internetworking, 2008.

[15] Shin, D. (2010) 'The effects of trust, security, and privacy in social networking: A security-based approach to understand the pattern of adoption', Interacting with Computers, Vol. 22, No. 5, pp. 428–438.

[16] Goettke, R. and Christiana, J. (2007) 'Privacy and online social networking websites', Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, 14 May.

[17] Camp, L. J. (1999) 'Web security and privacy: An American perspective', Information Society, Vol. 15, No. 4, pp. 249–256.

[18] Suh,B.Han,I.(2003)'Theimpactofcustomertrust and perception of security control on the acceptance of electronic commerce',

International Journal of Electronic Commerce, Vol. 7, No. 3, pp. 135–161.

[19] Kumar DV, Varma P, Pabboju SS. Security issues in social networking. Int J Comput Sci Netw Security. 2013;13(6):120–124.

Author Profile

Akhil Kumar completes Bachelor of Technology (B.Tech.) from Rajasthan Technical University, Kota in 2016 and pursuing Master of Technology from Indira Gandhi University() Meerpur, Haryana in the Year 2019. His main research work focused on issues and flaws related to the privacy and security of Facebook users. He has more than 6 months of experience in IT industry.

Sapna Jain completes our Bachelor of Technology from UP Technical University, Lucknow in 2006 and Master of Technology from Teerthanker Mahaveer University, Moradabad in the year 2013. She is currently working as Assistant Professor in Department of Computer Science, Mata Raj Kaur Institute of Engineering & Technology, Rewari since 2009. She has published and presented more than 10 research papers in reputed international journals and conferences. Her main research work focuses on Network Security, Data Mining, IoT and Computational Intelligence based education. She has more than 8 years of teaching experience along with 2-year experience in the IT industry.