Rachana Ashetabr, Parikshit N. Mahalle and Gitanjali R. Shinde

5 Users' privacy at online social networks in Indian context: comprehensive multiaged group survey and discussion

Abstract: Nowadays, social media has become an important part of life. People across the world use social media for random purposes. They post their accomplishments, achievements, vacation photos and others on the social media. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Online privacy is one of the crucial points to safeguard our personal information. However, protecting privacy in online social networks (OSNs) is challenging as OSNs follow the strategy "Take it or Leave it." Users need to provide information asked by the service providers in order to use the OSNs that may lead to compromise the users' data privacy.

To provide privacy-aware OSNs it is important to know user's awareness about privacy. To achieve this, survey is conducted and from analysis of survey the user's awareness and requirements of privacy-aware mechanism is presented in this chapter. Survey analysis shows that users of OSNs required to have trusted third party to manage their preferences and attributes to protect their privacy. Furthermore, user required new privacy law in Indian context and they need to hide their identity on OSNs.

Keywords: Online social network security, user data privacy, user identity privacy

5.1 Introduction

In today's era of online social networks (OSNs), everything we can find online starting from entertainment to business. But this availability also gives rise to one of the important aspects, that is, privacy [1–3].

Social network services and its popularity are widely spreading, where all age users are being attracted to it across the world. Reasons for using social network may vary like relationships, interests, friendship, knowledge or other social reasons. Popular examples of social networking sites (SNSs) used worldwide include Facebook, Twitter and LinkedIn [4]. This openness raises risks of vulnerabilities, data breaches and compliance violation. Also lack of regulation and standardization brings more opportunity for hackers to live and spread attacks in OSNs. It is the newest platform for security attacks.

Now with social networks, everyone is aware of the value of information being placed online as "data is money." People with profit motives or political agendas

are few of the main causes for the attacks on data confidentiality. Service providers (SPs) may misuse users' data for advertisements and may sell these data to third party without their consent, for example, Facebook data is misused by Cambridge Analytica for US president elections [5].

Currently, the effectiveness of security policies considering data leakage is an important concern to society. Social security sites do provide security mechanism but not seem to provide a way to stop privacy compromising.

There is a need of security mechanism for protecting use's' sensitive data shared on ONSs and there should be a method to bargain for users' data sharing instead of "Take it or Leave it" strategy. Successively, we can say that there is a need to develop a mechanism for protecting user's sensitive data shared on OSNs.

5.2 Motivation

Nowadays, social media has become an important part of life. People across the world use social media for random purposes. They post their accomplishments, achievements, vacation photos and others on the social media. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Furthermore, to use location-aware services, users share their location with their SPs so that they can lead to compromise their privacy. These incidents can potentially put themselves and everyone around them in potential danger.

A serious incident happened because of the post. There was a woman who used social media very extensively. She used to post every now and then on social platform.

The incident happened on one uneventful afternoon. She was at home with her husband when armed burglars broke into their home. They stole huge amount of cash along with some personal gadgets.

After the robbery when police started their investigation, a fact came into light that the woman in question had posted photos of herself with huge amount of cash on social media. This woman is the wife of CEO of the construction firm, having turnover in crores. She is shopaholic and net-freak. She frequently uploads her activities and photos of her family on Facebook and other OSNs. Robbers understood about her financial and family background with analysis of her pattern of uploads. After post robbers took advantage of the situation and planned the heist. She and her husband were planning for some vacation, so for that purpose she had taken that money out of the bank.

In this scenario, the woman is not aware about people viewing her personal data like marital status, kids' age, school, photos and many more.

From the above and many more other scenarios shown in Figure 5.1, we can say that there is a need to make people aware about the importance of privacy and how to achieve it as a fact that OSNs cannot say everything is ok and full proof by

Figure 5.1: Consequences of privacy leakage in OSNs.

Note: <https://www.zdnet.com/article/infographic-80-of-robbers-check-twitter-facebook-google-street-view/>

<https://theweek.com/speedreads/455792/familys-home-burglarized-after-post-vacation-photos-facebook>

<https://www.myrtlebeachonline.com/news/local/crime/article223765610.html>

<https://www.springfieldnewssun.com/news/local/criminals-use-social-media-choosing-their-victims/7zjvddM93fSEuVte1Be9XI/>

just securing server systems and application on servers [which are hosted by social network sites (SNSs)], underneath awareness about privacy is also important (which is not in OSN's control).

Other issues with OSNs are data stored by OSNs may be misused by the third party for advertisement or business growth or some other personal benefits/crimes. Today's third party has far more resources available to facilitate an attack and it has greater technical depth, focus plus it is well funded and is better organized.

Moreover, as end user communicates to server, end user's device security also becomes important (again this is not in SNS's hand). If user's device is with weak security mechanisms, then attack on data confidentiality is possible. Let's go one step ahead, assume user's device is safe but if user's knowledge is weak about data sharing and there comes possibility of misuse of user's data. There are fair chances that user identity attack will succeed here and start damaging user's privacy.

Also, at present there is no centralized mechanism directly available that will increase collaboration between SNSs, users and security teams to set standards or guidelines for preventing and reducing attacks on user's privacy. This is because social sites have different priorities and users have different priorities.

Consequently, from literature work we can say that there is a need to research mechanism for user identity protection and data confidentiality on OSNs to analyze behavioral modeling of most possible attacks to provide a solution set in near future.

5.3 Related work

Analysis of different privacy and security risks is presented by Fire et al. [6], due to users' unawareness about privacy and security settings they share their personal information on OSNs may put them in risk. The different types of threats presented in this chapter are, for example, clickjacking, anonymization attack, fake profiles, identity clone attacks, inference attacks, information leakage, location leakage, socware, online predators, cyberbullying. Few recommendations for protecting their privacy are suggested like removing unnecessary information shared on OSNs, adjust privacy and security settings of OSNs account, not to accept friend requests from strangers, install Internet security software, remove installed third-party applications, not to publish location, not to trust on friends on OSNs and to keep eye on children's OSN activities.

The attacks on OSNs are categorized as attacks on users and attacks on OSNs by Kayes and Lamnitchi [7]. Inference/de-anonymization attacks, attacks from other users, OSNs are categorized as attacks on users. Sybil attack, crawling attacks, social spam and distributed denial of service attack and malware attacks are considered as attacks on OSNs. The procedure of attack launch and defense techniques is presented in this work.

Comprehensive survey of personal information disclosure by members while joining OSNs especially Facebook, Instagram, Twitter and Snapchat is done by Aljohani et al. [8]. The analysis is done on the data collected in duration of 3 months, with 30 different questions and over 500 responses. The analysis concludes that in general people disclose their gender, name, age and education very frequently. Survey results show that the friend requests are accepted without knowing the person 50% of times. The privacy setting "only visible to friends" doesn't make any sense in such scenarios.

Survey of privacy risks and challenges of OSNs, cloud and big data are presented rigorously in the literature [9–19]. In these research works, different attacks on OSNs and their solutions are presented.

The effect of understanding of privacy setting and policies on the information disclosure on OSNs is presented by Fred et al. [20]. The survey is taken from 122 Facebook users. This survey shows that after reading privacy policy the information disclosure can be reduced as users are aware about the importance of privacy of their personal information.

Survey of Facebook users aged 18–29 is taken by Madejski et al. [21], to understand the awareness of users about privacy settings of Facebook. The survey results

show that 44% users take efforts to limit their personal information disclosure, About 71% users have changed their privacy settings and 47% users take actions like deleting unwanted comments to keep privacy.

In digital era, use of android apps increases in large number; however, using android apps may lead to privacy leakage as at the time of installation of apps, users unwillingly allow access to their smart phone camera, contact list, microphone and so on. Li et al. [22] presented intercomponent communication taint analysis tool to protect the privacy of android users.

Savla and Martino [23] have carried out survey about privacy. It is based on 35 OSNs that are used frequently in the United States. Survey shows that the users' privacy is at risk if the privacy policies are not implemented as per standards. Another survey carried out at countries like Saudi Arabia [24], UK [25] and India [26–27], survey shows that to protect privacy of OSNs there is a need to understand users' view about SPs and policies.

Zeadally and Winkler [28] carried out a survey to understand users' knowledge and awareness of the privacy policy. Facebook, LinkedIn, Twitter and others are selected for this survey, Findings of this survey state that people doesn't understand what they agree while registering membership on such OSNs.

From related works mentioned earlier, we can conclude that privacy surveys are done mainly in developed countries and they are in initial phases in country like India. Surveys taken in related works focus on participants who are of middle age; however, nowadays youngsters spend most of their time on OSNs, which is making necessary to research privacy issues in Indian context and it should be more focused on lower age group participants. Therefore, this research provides details of users' awareness about privacy in Indian context.

5.4 Issues and challenges

In this section we will discuss issues and challenges to provide privacy-aware secure access to OSNs. An architecture to provide secure and privacy-aware OSNs could face different challenges as today's technoworld is heterogeneous and scalable. Security and privacy algorithms need to support these heterogeneity and scalability. From the above discussion of literature and gap analysis, OSN system requirements, few challenges are mentioned below:

- Heterogeneity: Devices that are involved in OSNs are different in computational capabilities, information format, connectivity and many more. Performance of the security and privacy algorithms may vary with such heterogeneity.
- Scalability: As aforementioned, number of people using OSNs has increased tremendously and will continue to increase in the future. The privacy algorithms must perform best with such scalable environment.

- Awareness: Users need to accept policies with terms and conditions about sharing their personal data before accessing services of OSNs. SP asks these information for their business betterment; however, users may not be aware of “why, how and where their personal data being used.” Due to personal data sharing with the SP could possibly result in the infringement of privacy rights. People using OSNs are not aware of the fact that their personal data is used by the third party and moreover they not aware about consequences of privacy leakage. Hence, users should be made aware about privacy policies and their right to protect personal data.
- Standardization: Standards are not being used for protecting users’ privacy on OSNs, and lack of standardization is a major issue faced by OSNs.
- Policy interpretation: Reading and understanding of privacy policies is difficult for users of OSNs. There is a need to have understandable way to provide insight of privacy policies.
- Attribute negotiation: SP asks personal attribute for usage of OSNs. Users need to share all attributes asked by SPs. However, for protecting privacy, there should be facility of attribute negotiation. Thus, selection of basis of attribute negotiation is very challenging as users and SPs viewpoint about sharing information are contradictory to each other.

5.5 Proposed work

Quantitative analysis can be the best way to understand users’ awareness about privacy. We have conducted survey of Indian people of different age groups, different educational backgrounds and different work cultures. This survey was intended to learn about users’ activities, practices on OSNs, knowledge about privacy policies, laws related to privacy and what is missing in current privacy mechanisms.

In the survey, we have formatted questionnaire in such a way that participants’ responses will provide their suggestions and opinions about the type of privacy mechanism they wish to have with OSNs. A total of “47” questions are prepared, and these questions are formed in such a way that any layman can understand. We tried to make survey as simple as possible and users are selected randomly for survey as per principles of the survey [29]. Survey is done online using Google form, and this form is sent to the participants via email. Method of online collection of responses is used in survey instead of the off-line method to save time of the survey. Few assumptions are made while survey like participants are excited to give survey, they were honest and gave responses voluntarily.

The questions are formed in such a way to understand users’ viewpoint about what is privacy?, How user’s information get compromised?, Why SPs steal users’ information?, What benefits SPs are getting by stealing users’ information?, What actions should be taken by the user to protect their personal information? and

Where user should seek for help if information compromised?. It is depicted in Figure 5.2. These questions are categorized in six sections. The first section, that is, introduction, we formalized this section to know details of participants like age, status as whether working or student, from where they access OSNs and which type of online facility they use. The second section of questionnaire is targeted to know participants awareness about online privacy like, which information is recorded by the SPs, what happens further with these information, what is SPs aim to collect these data and so on. Third and fourth section questions are related to know participants awareness about privacy laws and agencies, and what individuals will do if their privacy compromised. In section five, questions are formed to understand participants' expectations from SPs about the privacy of their data. related to SPs. In this digital era, people are using Internet to use health facilities with the help of the Internet of things, section six questions are focused to know about users' understanding about the privacy of their health parameters that they share through Internet.

Figure 5.2: Overview of questionnaire.

5.6 Results and discussion

As aforementioned, for unbiased analysis survey is taken for users with different educational background, different working culture and different age groups, which is depicted in Figure 5.3. A total of 671 responses have been received; among which 55.3 (371)% were males and 44.7% (300) were female users who participated. Among 671 participants 42.3% (283) participants consider themselves as very new to computer field, that is, having less knowledge of computer field, 45% (301) participants see themselves as having satisfactory knowledge about computers and only 12.7% (85) claim them as experts in the computer field. This analysis shows that very few people know about risks that may happen while handling Internet as only 12.7% participants are expert in computer and Internet field.

In the survey, few questions are formed to know details like from where participants access Internet, what is the purpose of accessing Internet and how much work they get it done using Internet. The survey analysis shows that the common

Figure 5.3: General information about survey.

answer was that participants (i.e., 87.8%, Q5) access Internet at home, office, college and school, and only 12.2% participants access Internet from cybercafé and other places. The survey shows that 58.3% people use Internet for online shopping and 72.9% people use it for OSNs and search engines. Only 32.6% [Q.6] participants use Internet for other works than online shopping and OSNs. This analysis shows the increasing popularity of OSNs.

5.6.1 Which information may leak while using Internet/OSNs?

We tried to understand participants' response on question-related information leakage, that is, Q9. As per your knowledge, response to the question "Which information is recorded by server while you are online?" is shown in Figure 5.4. It is observed that majority of participants, that is, 65%, 62%, 52.5% think that email id,

Figure 5.4: Analysis of types of information leakage.

location and machine address may be stored by SPs, respectively. However, in reality more information stored and fetched by SPs and response shows that participants may not be aware about this.

5.6.2 Why privacy get compromised?

In question 11, we tried to know participants' views about information leakage by SPs, question formed as "Q.11 What would you think about the primary usage of collecting personal information by service providers?" 52.3% participants thought that SPs steal users' data for analysis purpose that could be further used for recommendation systems, few people thought that SPs store users' data for detection of fraud, case studies and for implementation of new laws, depicted in pie chart, that is, Figure 5.5. These responses show that people are not aware of the fact why data is stored and used by SPs.

Figure 5.5: Analysis of users' responses: reasons of privacy compromise.

5.6.3 How privacy gets compromised?

Privacy may be compromised due to fact that most of the people are not aware that they are providing personal information online, without knowing what can be done with their data. This may lead to harm their privacy and, furthermore, people are not even aware about consequences of privacy leakage.

In sequel to this, few questions of survey are formed to know users' views about privacy leakage, which is depicted in Table 5.1. Most of the people share their data online without thinking protection of their personal information. Analysis of survey shows that 72% people frequently share their data<Q15/> and furthermore 23.8% people even don't know the consequences of privacy leakage [16].

Table 5.1: Analysis of users' responses: awareness about data sharing.

Question	Response
Q15. In general, have you frequently shared your personal information with organizations that they ask for it?	72% people shared their personal information online.
Q16. Are you aware of consequences if your privacy is compromised?	23.8% people are not aware about the consequences of privacy leakage.
Q18. Have you ever asked an organization that requested personal information from you “why they want it” and “what they will do with it”?	Most of people, that is, 52.1% people never asked any question while sharing their personal information.
Q34. How regularly do you read the privacy policies of websites/service providers you visit/doing registration?	Only 15.1% people read privacy policies regularly while registering online.
Q35. Do you think that the privacy policy is very lengthy, unable to understand and descriptive?	Among those who read privacy policies, 77.1% people think it is very lengthy and not in understandable format.

5.6.4 Whom to ask if privacy gets compromised?

Privacy of personal data is an important issue in this digital era as we frequently share data on OSNs, assuming that third parties, SPs, are trusted. However, this is not the reality that privacy may compromise if these are not trusted; hence, users should be aware what steps they should take if privacy gets compromised. In the survey, few questions are formed to know users' awareness about actions that they should take if privacy gets compromised, which is depicted in Table 5.2. The analysis shows that 61.6% people are even not aware about privacy law in India [Q.12] and 59.3% people never take any action to protect their data [Q.24].

5.6.5 How and why to protect privacy

Nowadays, people use OSNs and Internet frequently. Survey analysis shows that 40% people do their 80% work like banking, shopping and so on using online services. People think life will be easier using online services as in Q.7, and 96.3% people say that online service made their life easier; however, this is one side of the coin. Other side is that, to use these facilities they need to share their personal data and accept terms and condition that may lead to compromise their personal data. SPs are using “Take it or Leave it” approach, which needed to be changed. There should be some mechanism by way that an users can use online facilities without losing their data privacy [Q.25, Q.31]. There should be new privacy laws to protect

Table 5.2: Analysis of users' responses: awareness about privacy law.

Question	Response
Q24. Do you personally take any steps/actions to limit tracking of your Internet/online activities?	38.5% people never took any action to protect their privacy.
Q14. Have you ever actively hunted out for information about your privacy rights, for example, by visiting a website searching on the Internet contacting an agency/organization or reviewing a standard publication for help?	Most of the people, that is, 59.3% didn't search any help to protect their privacy.
Q12. Are you aware of any federal institutions/ law that help Indians to deal with privacy and the protection of personal information from wrong collection use and exposing publicly?	61.6% people are not aware about privacy law that can help to protect their privacy.
Q38. Where do you ask the question if security/ privacy is breached?	Majority of the participants (55.4%) respond that they will take help from security specialist and system admin, and very few participants (30%) choose to take help from government agencies.

privacy as once people are aware about consequences of privacy leakage, people may think not to use online services on cost of privacy [Q. 22, Q.28], which is listed in Table 5.3.

5.7 Conclusion and future work

Analysis of this survey shows that users are not aware of the privacy compromise and consequences of it. Moreover, users are not aware where to seek for help if privacy gets compromised, and what actions they should take to protect privacy. In the sequel of this we wanted to know what are the expectations of users from OSN privacy systems.

These expectations may lead us to provide a novel method to provide privacy-aware OSNs, as people prefer privacy over services Q.22. In Q29, "I support the establishment of a personal trust manager (where a trusted entity/party keeps my preferences/experience to build trust between me and the service provider)" we tried to understand that whether trusted third party can be a solution to build trust between the user and SP. The analysis is depicted in Figure 5.6. It shows that 83.5% participants agree to have trusted third party to store their preferences and build trust between them and SPs.

Table 5.3: Analysis of users' views on "Privacy vs Services".

Question	Response
Q22. What do you most prefer, <i>privacy</i> or <i>utilities/services</i> .	86.5% people prefer privacy over services and online utilities.
Q25. Do you think that service provider/Internet companies should ask your consent/permission to track what you do on the Internet?	Majority of people (83.2%) think that service providers should ask consent before tracking online activities.
Q28. There should be new laws to protect user privacy on the Internet.	Almost every person (97.6%) thinks that there should be a new law to protect user privacy.
Q31. A user should have complete control over which sites that collect the user's important and critical information.	In the view of protecting users' privacy, users should have control over sites that collect their information.
41. Do you feel that the service provider should notify you when they deal (access sale share) your personal information?	87.1% people demand for such service providers, which will notify users while using their personal data.
44. Have you ever decided not to install an app because of the amount of personal information you need to provide?	80.6% people choose not to install app due to the risk of personal information sharing.

Figure 5.6: Users' response on privacy solutions: "Trusted Third Party."

In another question Q32, we wanted to know users' viewpoint on their identity, whether they want to keep their identity hide from OSNs, to protect their privacy. Question formed as "Q.32. I will be interested in being anonymous when visiting sites on the Internet." The analysis of users' responses is depicted in Figure 5.7. Among 671 users, 77.9% of them expect to have trusted third party to protect their identity while working on OSNs.

Based on the above analysis of users' responses on privacy, we can build privacy-aware mechanism to protect users' privacy on social media. The features of

Figure 5.7: Users' response on "protecting their identity."

such a mechanism will be as follows: it will have an "algorithm to protect users' identity across OSNs," and a "trusted data management algorithm to maintain data confidentiality."

References

- [1] Dey, N., Babo, R., Ashour, A. S., Bhatnagar, V., and Bouhlef, M. S. (Eds.). *Social networks science: Design, implementation, security, and challenges: From social networks analysis to social networks intelligence*, Springer International Publishing: Springer, 2018.
- [2] Marpaung, J.A.P.; Sain, M. and Lee, Hoon-Jae, "Survey on malware evasion techniques: State of the art and challenges" in *IEEE, Advanced Communication Technology (ICACT)*, 14th International Conference, 2012, pp. 744–749.
- [3] Das, N., Borra, S., Dey, N., and Borah, S. *Social Networking in Web Based Movie Recommendation System*, In *Social Networks : Design, Implementation, Security, and Challenges Science*, Cham : Springer, 2018, pp. 25–45.
- [4] Hashimoto, G.T., "A security framework to protect against social networks services threats", in *IEEE, Systems and Networks Communications (ICSN)*, Fifth International Conference, 2010, pp. 189–194.
- [5] <https://techcrunch.com/story/facebook-responds-to-data-misuse/>
- [6] Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online social networks: threats and solutions", *IEEE Communications Surveys & Tutorials*, 16(4), 2014, pp. 2019–2036.
- [7] Kayes, Imrul, and Adriana Iamnitich. "A survey on privacy and security in online social networks," *arXiv preprint arXiv:1504.03342* 2015.
- [8] Aljohani, Mashael, Nisbet, Alastair, and Blincoe, Kelly. "A survey of social media users privacy settings & information disclosure", 2016.
- [9] Ajami, Racha, et al. "Security challenges and approaches in online social networks: A survey", *IJCSNS*, 11(8), 2011, pp. 1.
- [10] Zheleva, Elena, and Getoor, Lise. "Privacy in social networks: A survey," *Social network data analytics*, Boston, MA : Springer, 2011, pp. 277–306.
- [11] Cavoukian, Ann. "Privacy in the clouds", *Identity in the Information Society* , 1.1, 2008, pp. 89–108.
- [12] Chewae, Mafaisu, et al. "How much privacy we still have on social network?," *International Journal of Scientific and Research Publications*, 5(1), 2015, pp. 2250–3153.
- [13] Rubinstein, Ira. "Big data: the end of privacy or a new beginning?." 2012.

- [14] Jayalakshmi, N., and R. G. Kavitha. "A survey on privacy in social networking websites," *Adarsh Journal of Information Technology*, 5(2), 2016, pp. 30–37.
- [15] Zhang, Chi, et al. "Privacy and security for online social networks: challenges and opportunities," *IEEE network*, 24(4), 2010, pp. 13–18.
- [16] Kayes, Imrul, and Adriana Iamnitchi. "Privacy and security in online social networks: A survey," *Online Social Networks and Media*, 3, 2017, pp. 1–21.
- [17] Gao, Hongyu, et al. "Security issues in online social networks," *IEEE Internet Computing*, 15(4), 2011, pp. 56–63.
- [18] Wang, Yang, and Alfred Kobsa. "Privacy in online social networking at workplace." *Computational Science and Engineering*, 2009, CSE'09. International Conference on, 4, IEEE, 2009.
- [19] Toch, Eran, Yang Wang, and Lorrie Faith Cranor. "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, 22(1–2), 2012, pp. 203–220.
- [20] Stutzman, Fred, Robert Capra, and Jamila Thompson. "Factors mediating disclosure in social network sites," *Computers in Human Behavior*, 27(1), 2011, pp. 590–598.
- [21] Madejski, Michelle, Maritza Lupe Johnson, and Steven Michael Bellovin. "The failure of online social network privacy settings.," Department of Computer Science, Columbia University, 2011.
- [22] Li, Alexandre Bartel, Bissyandé, Tegawendé F., Klein, Jacques, Traon, Yves Le, Arzt, Steven, Rasthofer, Siegfried, Bodden, Eric, Outeau, Damien, and Patrick McDaniel. "IccTA: Detecting inter-component privacy leaks in android apps," In *Proceedings of the 37th International Conference on Software Engineering*, 1, IEEE Press, 2015, pp. 280–291.
- [23] Savla, P., and Martino, L. D. Content analysis of privacy policies for health social networks. *Proceedings – 2012, IEEE International Symposium on Policies for Distributed Systems and Networks, POLICY 2012*, 2012, pp. 94–101. <http://doi.org/10.1109/POLICY.2012.20>
- [24] Alsagri, H. S., and Alaboodi, S. S. Privacy awareness of online social networking in Saudi Arabia. 2015, *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*, 2015. <http://doi.org/10.1109/CyberSA.2015.7166111>
- [25] Khan, R., and Hasan, R. The story of naive alice: Behavioral analysis of susceptible internet Users, *Proceedings – International Computer Software and Applications Conference*, 1, 2016, pp. 390–395. <http://doi.org/10.1109/COMPSAC.2016.206>
- [26] Kumaraguru, Ponnurangam, and Niharika Sachdeva. "Privacy in India: Attitudes and awareness v 2.0." Available at SSRN 2188749 2012.
- [27] Dhawan, S., Singh, K., and Goel, S. Impact of privacy attitude, concern and awareness on use of online social networking, *Proceedings of the 5th International Conference on Confluence 2014: The Next Generation Information Technology Summit*, 2014, pp. 14–17. <http://doi.org/10.1109/CONFLUENCE.2014.6949226>
- [28] Zeadally, S., and Winkler, S. Privacy policy analysis of popular web platforms. *IEEE technology and society magazine* (June), 2016, pp. 75–85.
- [29] Susan Farrell 28 Tips for creating great qualitative surveys,. Retrieved May 29, 2017, from <https://www.nngroup.com/articles/qualitative-surveys/>, . 2016.