RESEARCH CENTRE FOR MODELING AND SIMULATION

(RCMS)

Evaluation of Security and Privacy Perceptions in Online Social Networks

Asma Bibi

NUST201463272MRCMS64214F

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY

(NUST), ISLAMABAD

2016

Evaluation of Security and Privacy Perceptions in Online Social Networks

ASMA BIBI

Research Centre for Modeling and Simulation

A thesis submitted to the National University of Sciences & Technology in partial fulfillment of the requirement for the degree of

Masters of Science

2016

STATEMENT OF ORIGINALITY

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

Date	Asma Bibi

Dedication

This effort is dedicated to all those humble beings that have assisted me in any way to become what I am today, whose sacrifices seeded my success, especially my parents who have felt my pain beyond me and showered me with never ending prayers and support. I deem them as a divine source of inspiration.

Acknowledgements

All praise to Allah Almighty for bestowing me with the courage, knowledge and health to carry out this thesis.

I am greatly indebted to my Parents and family members, without their endless support, patience and prayers the very idea of this study was impossible.

I sincerely appreciate the continuous motivation of my project supervisor Dr. Adnan Maqsood. His encouragement was the main source of strength that stimulated me to complete this thesis.

I would specially like to extend a heartfelt thanks to my thesis committee members Dr. Zamir Hussain, Dr. Ammar Mushtaq and Lect. Fawad Khan for their precious time and skillful assistance.

I am also thankful to my colleagues who helped me through the difficulties I faced during the thesis. Due to their kindness and selfless help, I accomplished my goals within due course time.

Summary

The growth in technology has transformed our socio-economic system to socio-techno-economic dimension. The usage of online social media for formal / informal interactions has added complexity to our existing communication networks and lifestyles. Consequently, the security and privacy of individuals / information is now more vulnerable. Development of appropriate security layers in online social media requires enormous time and financial resources. A systems perspective in the development of awareness programs / trainings / additional security layers is required. However, the awareness of such complex issues in Pakistani society is still under-developed.

In this study, we have focused on estimating the existing state of awareness in the society about privacy, security steps and information hiding / sharing in social media. The study is based on a traditional method of survey research design "questionnaire filling". Student population of National University of Sciences & Technology, (NUST) Islamabad, Pakistan is considered for questionnaire filling. Correlations between variables and usage / awareness levels of security settings in social networking sites are evaluated. The results demonstrated lack of knowledge about security and privacy even in the population with maximum exposure to information. However, an increasing concern about privacy issues is also observed. Most of respondents spend much time of the day on social networking sites. The results of this study can help in evaluating current user perspective and futuristic interventions required for development of awareness programs and design of security procedures / layers in social media system.

Table of Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

Social media usage has evolved drastically in Pakistan in recent years. During Middle East and North Africa (MENA) uprising, social networks were frequently used by masses. Usage of social-media post-MENA uprising is also observed in Pakistan. However, on the downside, usage by terrorist / criminal organizations for extracting personal information from these social networks is also on the rise. This study aims to assess awareness of people and elaborates methods on how to access social environment securely. This study highlights ratio of people who are concerned about privacy. Security and privacy layers in social networks are a major contributor for reduction of criminal activities. This study aims to build up a research model, in which security and privacy issues act as predecessor of trust and seek assurance that user data entered in social networking sites is secure[1]. The ultimate goal of this research includes recognizing the setbacks of safety, expectation and seclusion concerns on the compliance of providing information in public network sites. Suitable research sample was selected based on available resources, the research question and limitations of the study[2]. Tony Bates [3] explains that new web services and tools facilitate self-learning and knowledge sharing and encourage teamwork, between student and teachers by means of feedback and assessment (assignments, tests). Another study [4] aims to highlight the risk associated with cloud based social networks and forensics trials based on data access within a cloud environment. Specifically, information is gathered from student about the time they serve on social network web sites[5]. Such respondents are unaware of the fact that

the information from these public groups is gathered for applying data mining techniques on social networking servers. These data mining tools further separate the gathered information based on religious, political and sectarian extremism and then use them for other purposes as shown in Figure 1.

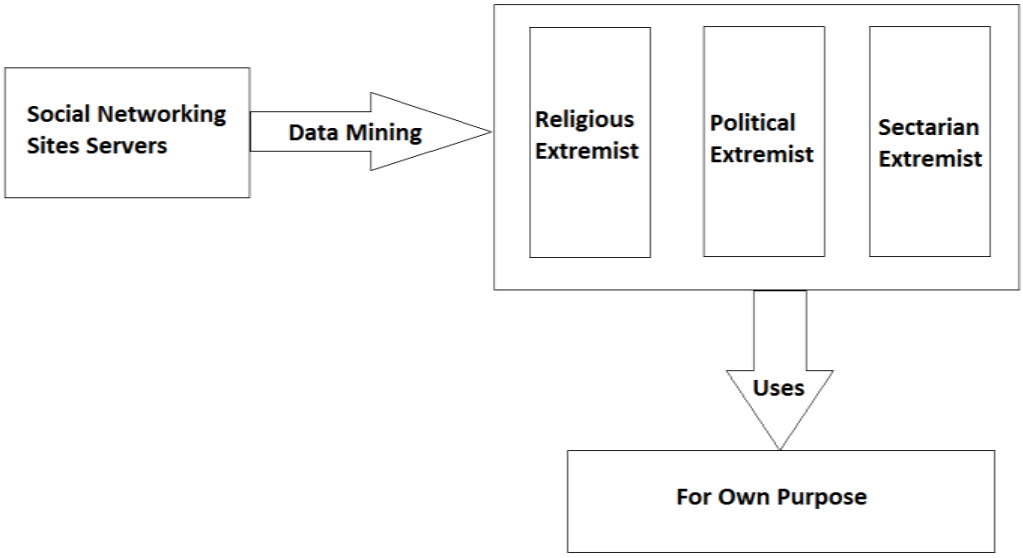

Figure 1-1: Data Mined from Social Networking sites

Majority of social networking sites servers are not hosted in Pakistan. Server owner apply various data mining techniques to the data residing on their servers. This possesses a great risk for users. Data mining tools are capable of segregating data in form of chunks. Religious, political and sectarian extremism can be three major areas of segregation among the social media data of our country.

SOCIAL NETWORKS

This research aims to provide awareness to people by presenting methods of accessing a secure social environment. Social environment include famous social sites such as Facebook, YouTube, Twitter, LinkedIn, Google+ and Instagram. Social media privacy

means that data should not be shared with third party while social media security ensures risk free environment.

SECURITY AND PRIVACY

Social networking sites usage is increasing drastically[6]. Millions of members use these social networking sites on daily basis to communicate, create, and share information with others[7]. Owing to their usage and enormous user database, social networking sites are treated as a valuable asset by the organizations[8].

INFORMATION SHARING

People who are concerned about security should be reluctant to share information in social networking sites[9]. In a recent study, a survey of 210 users of Facebook® was conducted in which it is highlighted that frequent users of Facebook® disclosed their information. They share this information with others in complex textual description and provide information related to human belief, behaviors, opinions, emotions, and relationships and so on[10].

ATTRACTIVE INTERFACES

Today social networking web sites are becoming an increasingly popular trend due to their attractive interfaces. Attacks are launched on social networks in an attractive way so that human mind gets busy in beautiful interfaces instead of paying more attention on its websites vulnerability. Attractive interfaces are an easy way of trapping users for using less secure sites. These attractive interfaces encourage users to create relationships with other users on Facebook®, LinkedIn®, and Twitter®. All web sites have their own popularities and features[11]. Attractive interface affects the social

networking web sites because of ease of use and well defined design and features rather than unattractive and difficult use of interface. To control privacy settings for each social networking site as per user consent, user should be well aware of its advanced settings. Privacy includes freedom from unwanted zones, protection of personal information and strict controls against security violations[12]. The study will cover issue of privacy focusing on individual behavior and activities[13].

OBJECTIVES OF STUDY

Enlisted below are study objectives:

1. Understanding and extracting the existing awareness state of social media users of NUST, Pakistan about privacy, security steps and information sharing in social media
2. Understanding the perception of security and privacy concerns among social media users of NUST, Pakistan and frequency/tendency of people sharing their private information on social networking sites
3. Statistical analysis of data collected through structured questionnaires
4. Proposing recommendations to improve security and privacy in online social networks

PROBLEM STATEMENT

People are participating in online social network without the knowledge of information leaks. They are concerned about security and privacy but have insufficient knowledge to accomplish it. The respondents of this study fall under four categories:

1. People who are concerned about privacy
2. People who are not concerned about privacy
3. People with sufficient knowledge for taking security steps
4. People who are unaware of outcomes of using social networking sites on their lives.

Based upon ratios of respondents, some rules are presented for achieving secure social environment. These rules empower the user in overcoming the challenges faced in social networking.

ORGANIZATION OF THE THESIS

Brief outlines of the chapters included in the thesis are presented below:

Chapter 1 --- Introduction

This chapter gives an introduction of evaluation of security and privacy in online social network. The area of research together with the formulated research methodology is also outlined. A brief description of the thesis breakdown is also included.

Chapter 2 --- Literature Review

In this chapter the thesis starts with the extensive background knowledge of the methods involved in Social Network with emphasis on security and privacy procedures**.**

Chapter 3--- Methodology

In this chapter all the approaches used in this study are described and the design is proposed.

Chapter 4 --- Results and Discussion

The results obtained by conducting a survey and then statistically analyzing the results of the questionnaire are illustrated in this chapter along with the discussions based on the recommendations for obtaining secure social networks.

Chapter 5 --- Conclusions and Future Work

Conclusions derived from the current research are presented. Recommendations for future efforts are suggested in this chapter.

CHAPTER 2

LITERATURE REVIEW

2.1 SECURITY AND PRIVACY SOLUTIONS

The privacy policy of customers using social sites can be improved by ensuring that information and content visibility is restricted to specific user or his / her contacts. It has been seen that social sites share user private data to Google® so they lose user trust. Such user information should not be open to Google® and other users should not be able to access other users pictures or related information merely by writing name of user. Privacy of users can be ensured by making sure that user information is not being shared to any other web site or any search engine[14].

It has also been observed that majority of social sites set their privacy policy as public. Mostly users ignore the default public setting and consider it to be set as private. This may lead to compromise of data. Another way to make privacy policy better is to make privacy setting private by default so if user oversees or forget to make it private even then no information will be compromised[15]. Two thirds of internet users use one or more social networking sites. Hence social sites should improve their privacy setting and policies to increase their users[16]. User data is retrieved from social networks and restructured without user's consent. Initially profile pictures were accessible by any user on Facebook® but lately it is being made private[17]. Incidents of private information compromise reduced after companies announced a monetary award for

reporting bugs[18]. The foremost important policy of social sites must ensure customers privacy. One of the major issues is when a social user's private information is compromised[19].

Account hacking can also be prevented if social site implement maximum validation to avoid the hacking process. Furthermore, hackers should be penalized on legal grounds[20]. Since, user doesn't get unfriend notification; another study classifies fake user accounts friendship requests as a privacy attack[21]. Most of these social networks mandate users to provide firm pieces of information[22]. Such information can be retrieved by malicious users and should be made optional[23]. This thesis aims to perform a survey in which twenty five questions were asked from users belonging to different schools of National University of Sciences and Technology, Pakistan using questionnaires.

2.2 SOCIAL MEDIA SECURITY AND PRIVACY

National Cyber Security Alliance (NCSA) [24] has shown the percentages of the people who are concerned about security and privacy and check Security and Privacy settings on regular basis. Similarly Pew Research Center (PRC) [25] is showing the percentage of users that have either cruel or kind behavior towards other users on social media. Consumer Reports (CR) [26] is showing the percentages of Facebook® users that have age below 13.For example 38% of Facebook users were under 13. Similarly 69% of users are kind to each other on social media according to PRC and 15% users never checked privacy and security settings according to NCSA.

In a paper another study explains[27] the percentage of profiles revealing various type of personnel information for example profile image, birthday, home town, address, phone and interests. Another study explains[28] a survey was conducted that revealed that people between ages of 18 to 24 years have Facebook® profiles. X-axis show ages and Y-axis the percentage of people having Facebook® profiles in Figure 2.1.

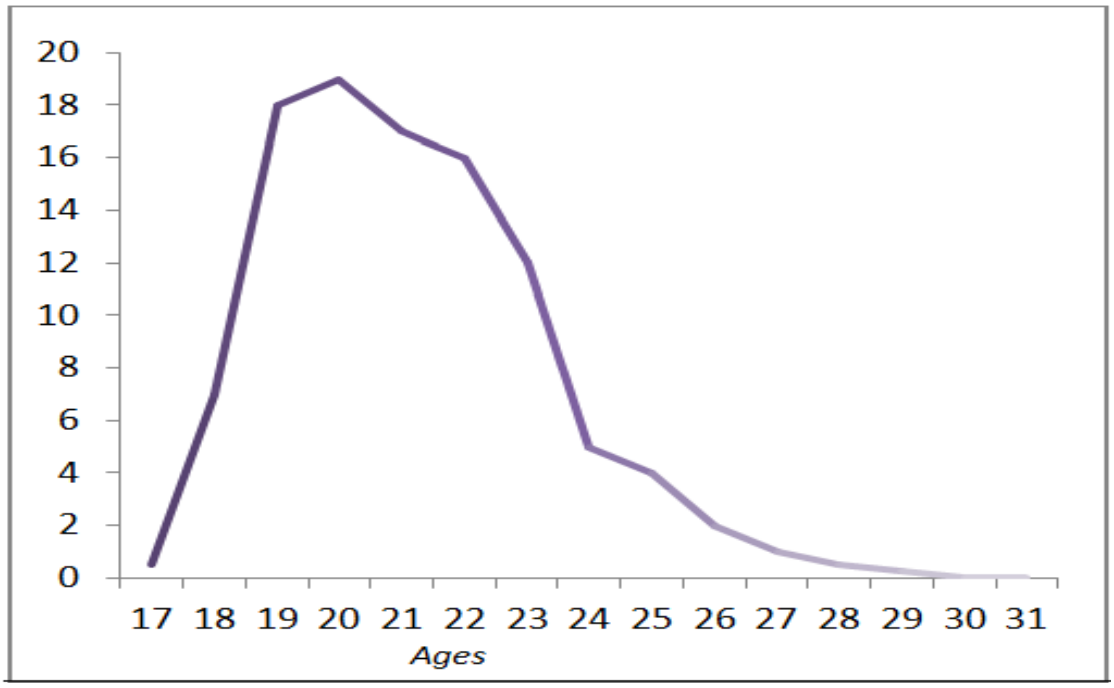

Figure 2-1: Facebook profiles ratio

Lam et al. [29] explains problem that people are participating in online social networks without the knowledge of information leaks. This study describes the impact of security, trust and privacy concerns on the willingness of sharing information in social networking sites. User's ability to give complex textual descriptions also provides information about human belief, behaviors, opinions, emotions, and relationships and so on. It will also be effective to identify factors like social norms, socioeconomics, ethnicity, and religion. It will help us to understand and describe the complex reality of given issues and the consequence of quantitative data.

Altshuler et al. [30] explained that majority of world population spend most of their time on social sites. While using internet and social networks, user is either directly or indirectly connected to many other social network users so if security of one social user is compromised then its means that the private information of many users have been compromised. Such compromises are not revealed publicly so the security and privacy of social network depends on both the online social network service provider and online social network users.

Hugl and Ulrike [31] explained that no rules on data control are prevalent on the online social network. Hence it depends upon the users how they share personal or critical data with other users. So it totally depends upon trust relationship and research has shown that the majority of online social network user privacy is compromised due to blind trust on other users. However the law has enforced the social service provider to seek user consent before using its data for advertising purposes.

Pasquale et al. [32] explained that data transience is one of the major concerns that revolve around personal information sharing. It explains that user is unaware about the data expiration time and show careless behavior while deleting shared data which cannot be deleted by other users and remain visible. In case the user forgets about the data that he or she shared and if the security of the service provider or even the user's friend that have the information visible on their social account get compromised then the whole history of the user can be captured and can be used for illegal means.

Jones et al. [33] explained that audience segregation is a good way to maintain security and privacy by creating audience segregation (group) and keeping strict security and privacy level of that group. The online network users who want to share information to

the most trust worthy people are placed in a similar group. Likewise, users who have common interest like politics and hobbies are placed in a similar group. Communities like city and country based people are placed in a different group, families are placed in a separate group and information is shared group wise. It has been observed that grouping is tough to manage. The best way to maintain privacy is to make sure that the online social network users are well aware of privacy policy before sharing the information. It is even better if the users read the privacy policy before creating a social account. It is the responsibility of the online social network service provider to provide a proper guide line to the user so that it helps the user to maintain the privacy of the data that the user shared on the social network.

Altshuler et al. [34] described that transparency is similar to awareness. The privacy and security policy should be easily understandable and applicable. Depending upon the online network service provider, better API's, easy language support and some default features like basic security and privacy policies should be set.

Wortley et al. [35] described that legal enforcement within online social network is not fully mature and is being improved day by day. Online social network users have not much awareness about the social network law. As per European's law, personal information should only be kept between trust worthy people like family members and close friends. Hence it is the responsibility of the user to inform the social network service provider about privacy and security related issues. Responsibility of improvising the security and privacy rules and their implementation and enforcement lies with the social network service provider.

Salama et al. [36] explained that a social network website usage within an organization is a big threat for an organization as these type of sites are mostly unsafe and the social network user are actually compromising the security of the entire organizational network. The personal information provided by the social network users like family pictures and date of birth is critical as this type of information can be used against the user like credit card fraud or identity theft. There were few suggestions introduced to reduce privacy and security threats. One of them was to use authentication process by creating a node also called trust node between two friends. A key is shared between both the nodes. Only owners of the key can see the messages in each other inbox. Another way to make you self-secure is to avoid using games and application on the social network as it is developed by a third party and it can use your information for advertising purpose or many others illegal activities. There were many ways introduced to measure the number of attacks on a social network such as Ant network graph attack. Attack tree method is also used to measure the goal of the attacker on the social network.

Kekwaletswe et al. [37] explained that it is the responsibility of the social network website to provide personal space management, social connection management, connectivity to other applications, social search and social traversal to the social network users. There are two other things that the social network user frequently performs. These include making new relationships and sharing information on the social websites. Both of these depend on blind trust so it is the responsibility of both the social websites and new nodes to maintain that trust and continue the chain.

Feruza et al. [38] explained different type of privacy attack on social network users one of them is identity disclosure in which a person uses another person name to gain access to medical treatment or get unauthorized drugs. Some of attackers use business names while others use person name to get access to credit card. Digital profile aggregation is a kind of threat in which user profile is being transmitted from one location to another and even analysis is being carried out on user data without the knowledge of the user. Face recognition is one of the threats in which user shares images. The shared information is placed in a huge database and analysis techniques can be used to guess the user activities. This is harmful for users as this type of information can be used for blackmailing or unwanted calling purposes. There were formulas developed to measure the privacy and security risks.

Kim et al. [39] explained that online social graph was used to connect people on social website. The same graph is used as a defense against social link forging attack. In such attacks, a person fools another person about his identity. The trust strength and interaction intensity being introduced in this graph are useful to prevent social link forging attack. Another type of attack is node link forging attack in which a person creates multiples accounts and fools others. This type of attack can be reduced if the users are forced to create account on the basis of government card number, identification numbers or other government identification processes.

Chbeir et al. [40] explained that social network is defined as the easiest and fastest way to share information and data to single or multiple users. There are multiple ways that are being used to manage user data like Algebraic notification, Matrices and Graphs. Each of them has its limitation. Majority of social networks are using Graph to

represents data in which nodes are representing the entities (like the names of persons) and edges represents the relationship between these entities (like friend or friend of friend or family member or school fellow).

Howison et al. [41] explained that there are two types of data in offline data analyzing techniques. One is behavioral data, in which past posts and information are analyzed to get idea about the nature of that particular user. The other one is derived data in which location in tags, pictures and other location data are being used to guess about users travelling activities, home town information and user current location. Mostly there are three types of user data analyzers; academic community, advertisers and governmental services. These analyzer uses the graph structure (use to connect people) to exploit the privacy by applying various techniques. Hence user privacy is not strong these days on social networks.

Ferrara et al. [42] explained that there are different data mining techniques used to extract data. By using relationship between the nodes, malicious user takes advantage of node management structure being used by the social network providers and exploits the weak links and extracts the data. Another way of data mining is to use the knowledge of node classification and node link with other nodes and get the desired data out from a social network. The third way used for data mining is to choose node and then follow its track to identify the community and people and then use the desired information. Link graph and node related threat are very sensitive these days and exploiters are using these three weak links to get the information out as these are strong techniques in terms of storing and making relationship between the individuals from social network service provider perspective. Privacy issues regarding multimedia

contents are also increasing day by day as new functions are being added in social networks. Different techniques and formulas are developed to measure and detect the privacy threat that could occur in future. Closeness or degree is term used to detect the distance between two nodes and this technique is applicable when social network service providers are using graphs to represent the data stored in the social network.

Gurses et al. [43] explained that it has been observed that different researchers and communities have agreed that privacy and security risks are increasing day by day in social networks and are becoming a big threat in a social network era. Even the social network users are aware of this issue. Computer researchers have indicated that even the government institutes are involved in tracking and using social network user data. Such bodies are involved in privacy leakage and the network service providers are also engaged in this activity as they are providing access to government institutes and other organizations to user data. However steps are taken by data protection organization to ensure that online network providers maintain the privacy on individual and institutional data up to some limit.

Mayer et al. [44] explained that service providers should block the online social networks causing privacy trouble. Another approach is to use software that will measure the privacy problem in Online Social Network. Privacy enhancement technology was also introduced to provide the online social network user with better privacy filters. Different data protection organizations also introduced policies for online network service providers in order to reduce the privacy threats for online social network users. Encryption is also used within a social network for providing user information to a specific audience. Using this feature comments or a statuses are

visible to specific peoples that are added in a decryption list. One of the common approaches is to provide user with proper guidance about privacy settings. Another suggestion that was provided by the computer science community is that user feedback should be sought while making privacy policies for an online social network service provider in order to make user friendly privacy settings.

Laufer et al. [45] explained that there are some questions that arise regarding the privacy issues like who can analyze the privacy problems etc. The excessive use and involvement of people in social network poses itself as a threat in terms of data security. One can get almost all the information about the community or country or any individual user. This has also attracted the law enforcement departments and disturbed the privacy of social network users.

Boshrooyeh et al. [46] discussed that the data uploaded on central servers are under the control of social network service providers. Maintaining privacy in a centralized server based system is a tough job. However, maintaining data integrity is also one of the major problems in the online social networks. There were more than one solution was being proposed in order to overcome the centralized server system problems. One of them was to use peer system by distributing data of different online social network users. Yet another system was not to store data permanently and to cache data till the users are communicating with each other.

Stallings et al. [47] suggests that for using digital signature, we have to verify the online social network user identity. Stress was laid on improving the search process and suggestions was also provided on how improve the privacy of other user data during the search made by other online social network users. Still there are few problems,

whose solutions are difficult to answer like data sharing and others. Even social service providers are also not willing to implement security measures like data encryption because they are selling user data for advertisement purposes. Online social network users are also publishing data for research and academia purposes which can cause problem of cross referenced with other data in order to access user private information.

The reason of popularity of online social networks [48] includes the multitude of services offered to online service users. Aiello et al. [49] explained the problem that employees of social network service provider have access to all the information of the entire users. They can sell information to third party or can use this type of information for their own purposes. Another big issue and mistake that all the social network providers are committing is the use of a specific and known technology that is graph technology to create links between different users and to store user's social relations. If any third party is able to access the graph system or guess the graph architecture being used to maintain the links, it may lead to information leak.

Aldhafferi et al. [50] discussed mobile users are also susceptible to attack. Even the online social networks are aware of privacy problems and have introduced filters in order to provide users with better privacy settings. So there are few solutions introduced to secure the privacy of the online network users one of them is to encrypt the user data and online social users can choose or place people in group who can decrypt the user information. Another solution that was being introduced is to educate people on how they can improve the privacy setting or how they can hide the

information from public user and what type of information they should place and should not place as it can be used against them.

Aimeur et al. [51] explained that if only one user account is hacked then it can cause problems for the whole chain of friends who were connected with the hacked user account. Website and others social networks providers are also using user's information and getting advantage out of it. A study shows that young generation is highly careless in term of privacy as they provide and publish data on websites and social networks without caring about the security threats. There are different communities of people that obtain and use user data, one of them is hackers. Social network users are also providing or selling user data to business in order to provide businesses with advertising opportunities. Friends can be a threat to other friend's privacy and destroy trust relationship. In the same way much other application can be a cause of personal information leakage. A survey shows that almost 90 percent of the people are using internet on the mobile phones. Majority of these people also have social networks accounts. Surveys also showed that the majority of them want customized security settings. These surveys also provide information about the importance of different type of data in form of ranking. So it is the responsibility of the online social network provider to provide better and improved privacy.

Humbert et al. [52] discussed that due to increasing popularity and use of social networks different organizations are also attracted toward the advantage that they might get from the social network of particular user. Different type of data provided by the social network user may also cause privacy disturbance such as a person can search another person based on cell phone or location or many other. So it is also the

responsibility of social network users to keep such information private so no public person should have access to such information. Study and research indicates that the targeted user was being achieved without opening or accessing his/ her profile but using a random search mechanism.

Sattikar et al. [53] explained that social networks are providing large number of beneficial services which is one of the cause of increasing number of online social network users. Author also observed that student profiles are susceptible to security threats as they place important and personal information on the social networks. Author also explained that people some time post very crucial information because they think that they have applied the maximum privacy settings and no one can get there data. However people do access their data. Some people have a blind trust on the social network service provider which is also not a good thing. One of the mistakes that a user of online network do is they make and trust online contacts without having a face to face meeting or interaction with them. One of the best solutions that can be used to protect the privacy problem is to use Artificial Intelligence that will guide the user about the severity of the data that the user are sharing with the online users and many other beneficial information.

Debatin et al. [54] explained that it is also a concerning point that users knows that the online social network are not secure even than they are uploading pictures and sharing information on the online social network accounts. One of the major causes of privacy leakage is carelessness of user about the privacy settings as they usually follow the default privacy setting which are normally set as public in majority of online social network users.

CHAPTER 3

METHODOLOGY

3.1 BACKGROUND

The main focus of the current study is to conduct a survey and analyze its results statistically. The reason for selecting statistical analysis instead of longitudinal studies is the vast reduction in resources, cost and time. Appropriate security layers are added to the upcoming systems; however, the awareness of such complex issues in Pakistani society is still under developed.

3.2 PROBLEM DESCRIPTION

Usage of social media by Pakistani youth is on the rise. There is dearth of literature on how this social media is changing lifestyles. It is imperative that perception about its potential hazards should be developed.

3.3 RESEARCH METHODOLOGY

A survey was conducted to assess student awareness level of using social media. The targeted respondents were students of NUST. Appropriate security layers are provided by the service providers however the user's awareness is still under developed. Vulnerability to various attacks on information has been evaluated based on user experience. The outcome of the study will be helpful to evaluate current user perspective and futuristic interventions required for development of awareness programs and design of security procedures / layers in social media system. The

baseline is that public of Pakistan is using social media more and more with the passage of time without considering its effects on their daily life. Opinion of general public is that social account generation and usage is free of cost but they are unaware of the effect that nothing is free and nobody is providing anything free to us rather we are paying its cost in the form of increase in malicious activities, violence and usage of our people for fulfilling others purposes. This research includes methodology starting with planning followed by objective statement, discussion and timeline. After that research design includes survey creation, determination of target population and sample size. Survey distribution and response monitoring took place in survey development which is also shown below.

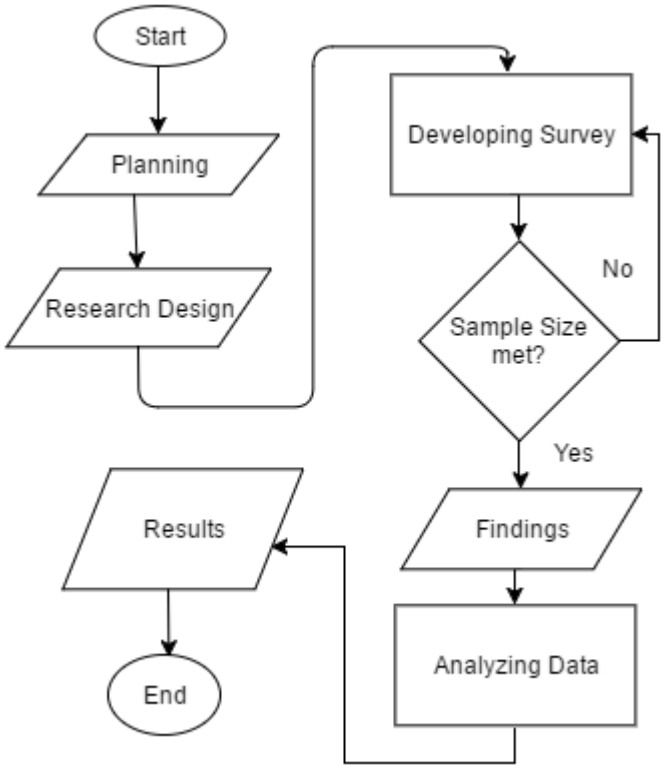

Figure 3-1: Research Methadology Flow Chart

The survey responses obtained during survey were transformed into forms in the form of flat file that are appropriate for data tabulation and analysis. Flat file is a

computerized two dimensional preparation of archives and their matching tenets. Data summarization and elucidation delivers the vibrant answer to the inquiries that originated from the survey.

3.4 RESEARCH DESIGN (SURVEY CREATION, DETERMINATION OF TARGET POPULATION)

Most traditional method of survey research design that is face to face questionnaire filling is chosen because it is the most accurate way of gathering correct information. Target population includes 122 students of NUST, Islamabad.

3.5 DEVELOPING SURVEY (SURVEY DISTRIBUTION, RESPONSE MONITORING/COLLECTION)

The survey questionnaire was distributed all over NUST and positive responses were received as majority of them were using social media. People filled the survey with interest. Responses were collected and data was manually entered in Microsoft Excel® firstly and was later used in Minitab® and IBM SPSS® for analysis. The sample size was met for data analysis. Results are included in next chapters.

CHAPTER 4

RESULTS AND DISCUSSION

BACKGROUND

To meet the objectives and methodology discussed in Chapter 3, the survey responses were analyzed and the results are discussed in the following sections.

RESULTS

The results of each question (from 1 to 25) are discussed seperatly in the following section while questions are mentioned in Annex-A :

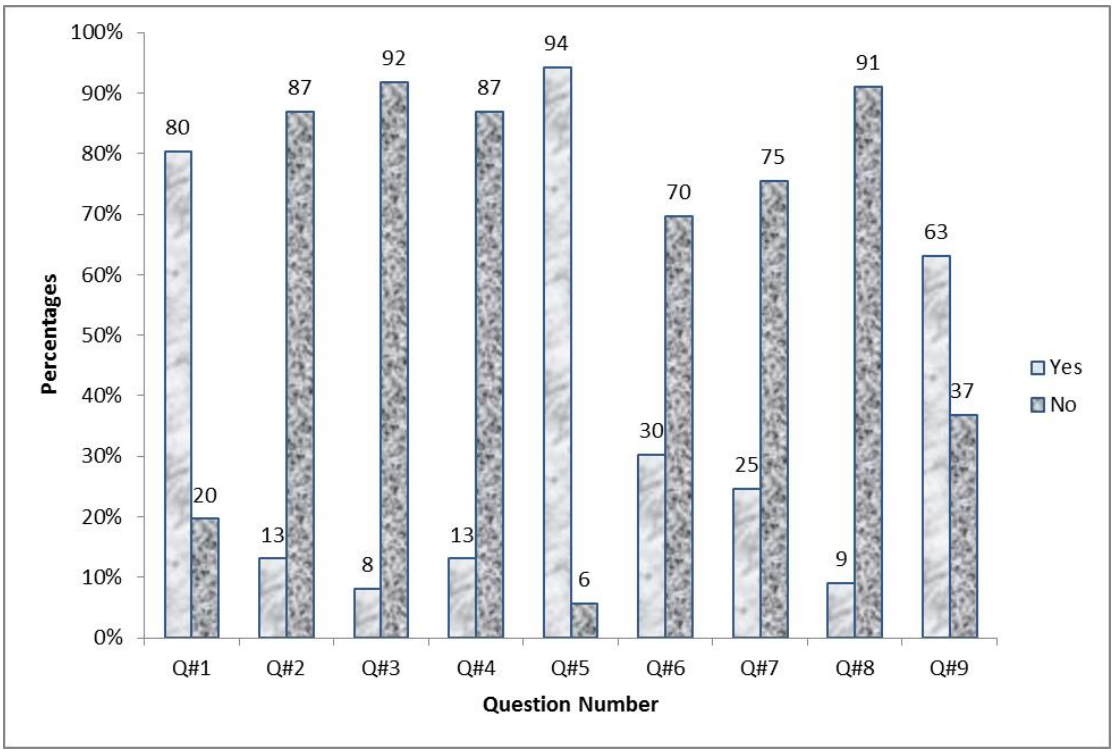

Figure 4-1: Results of question number 1 to 9

1. 80% of social media users are using their real personal information in their accounts.

2. 87% of social media users are not using credit card for their online purchasing. This shows that people are concerned about privacy while only 13% users are using credit card for online purchasing. Interestingly the percentages of responses of Q1 and Q2 are different therefore we can say that people are much concerned about privacy and security regarding their financial issues.

3. 92% of social network users do not respond to pop-ups while surfing Internet. This shows that majority of respondent are concerned about their privacy.

4. 13% respondents faced the problem that their social accounts ID's have been hacked. Therefore it is suggested that please do not open redirected webpages.

5. 94% respondents believed that people are stalking information of others and using forged identity therefore if any of your friends is having such identity then there is chance that your account is prone to attack. A possible solution can be that Ministry of Information Technology should include serious punishment in rule of law for people involved in fake identities crime. By doing so, this crime can be eliminated.

6. 30% social media users are concerned about credit card misuse and other personal information when purchasing things online. While 70% are not even concerned about it.

7. 25% respondents agreed to put their name and even address in public directories. This means that some percentage of respondents is unaware of the issues related to privacy and security. This means they are not at all concerned about privacy. While 75% don't agree but still there is chance that they are not aware of the fact that their customized information can also be easily utilized for any wrong purpose so they should also have proper awareness for privacy of information which is not public.

8. 91% respondents are not accepting friends requests of strangers but still 9% are not at all concerned and accepting even strangers also. These 91% are concerned about privacy but this not at all means that they are well aware of privacy settings.

9. 63% respondents think that privacy policies are effective in social networking sites. 37% respondents are saying no. The results of Q4 showed that 13% users have faced the problem of hacking ID's. Therefore the security and privacy policy of social network users is not completely effective

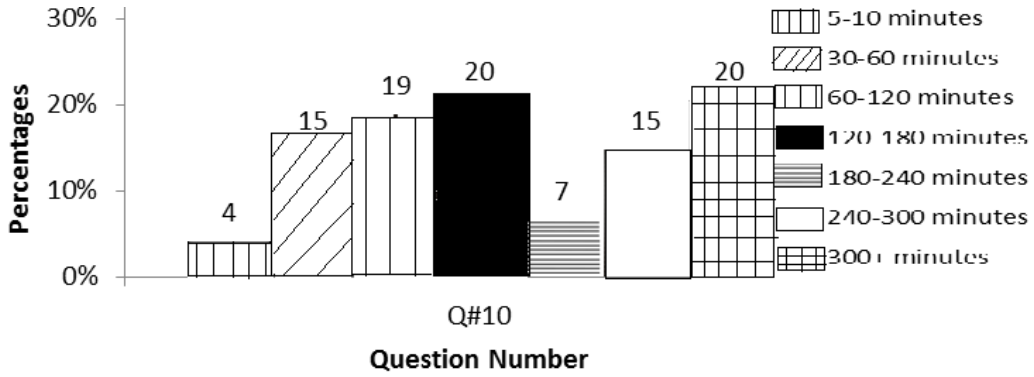

Figure 4-2: Results of question number 10

10. Highest respondents are 20% and 20% users are visting social site more than 5 hours per day while least percentage is just 4% that are visiting 5 to 10 minutes. It clearly shows the increasing interest of our public for usage of social media.

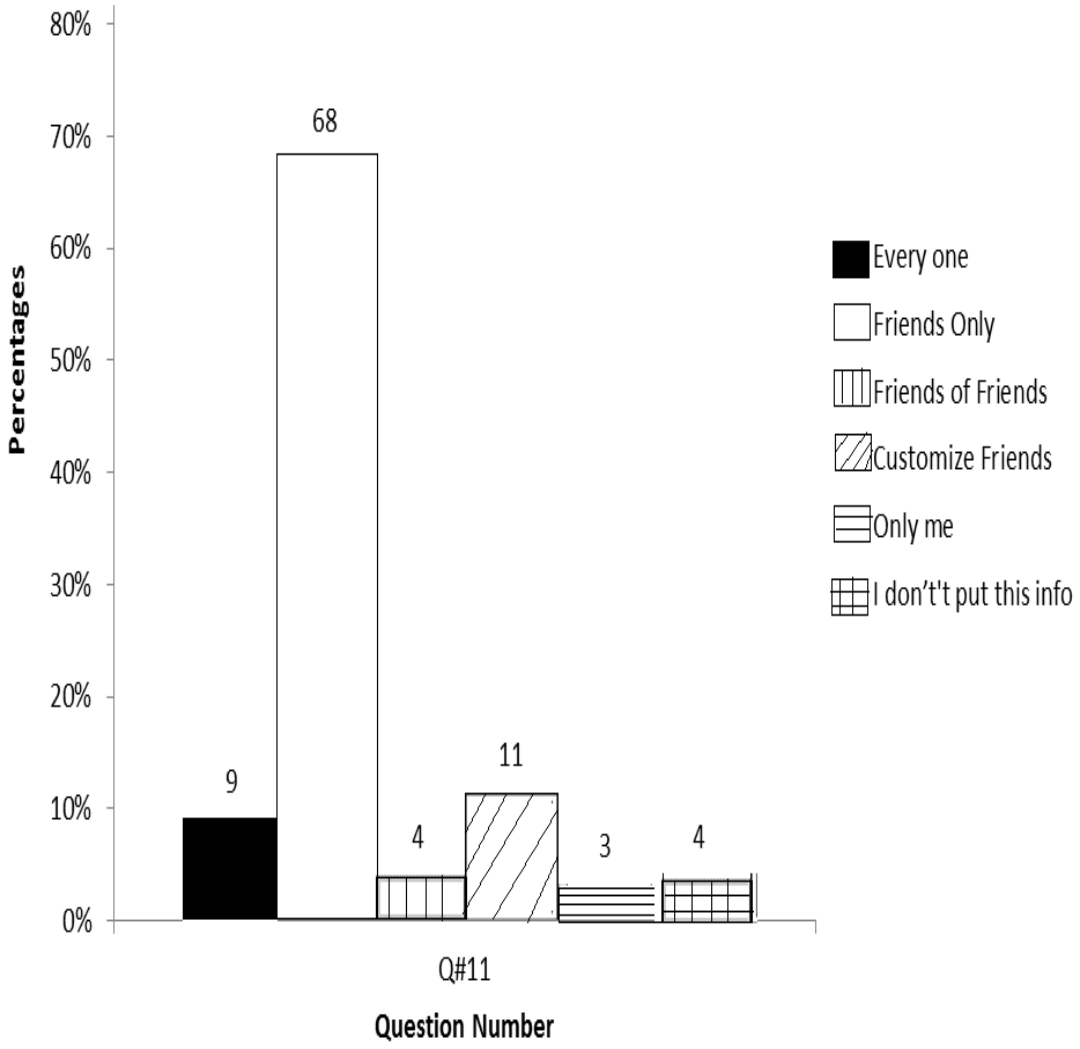

Figure 4-3: Results of question number 11

11. 68% social media users selected the privacy option as Friends only but still 9% have permanently selected their privacy option to be public. As in question number five, 94% people think that people are stalking information of others and using forged identity so if your friend is having forged identity then there isn't any option left to be saved from him / her. So if you are concerned about privacy but have insufficient knowledge to set privacy settings as customized than your personal information is at stake.

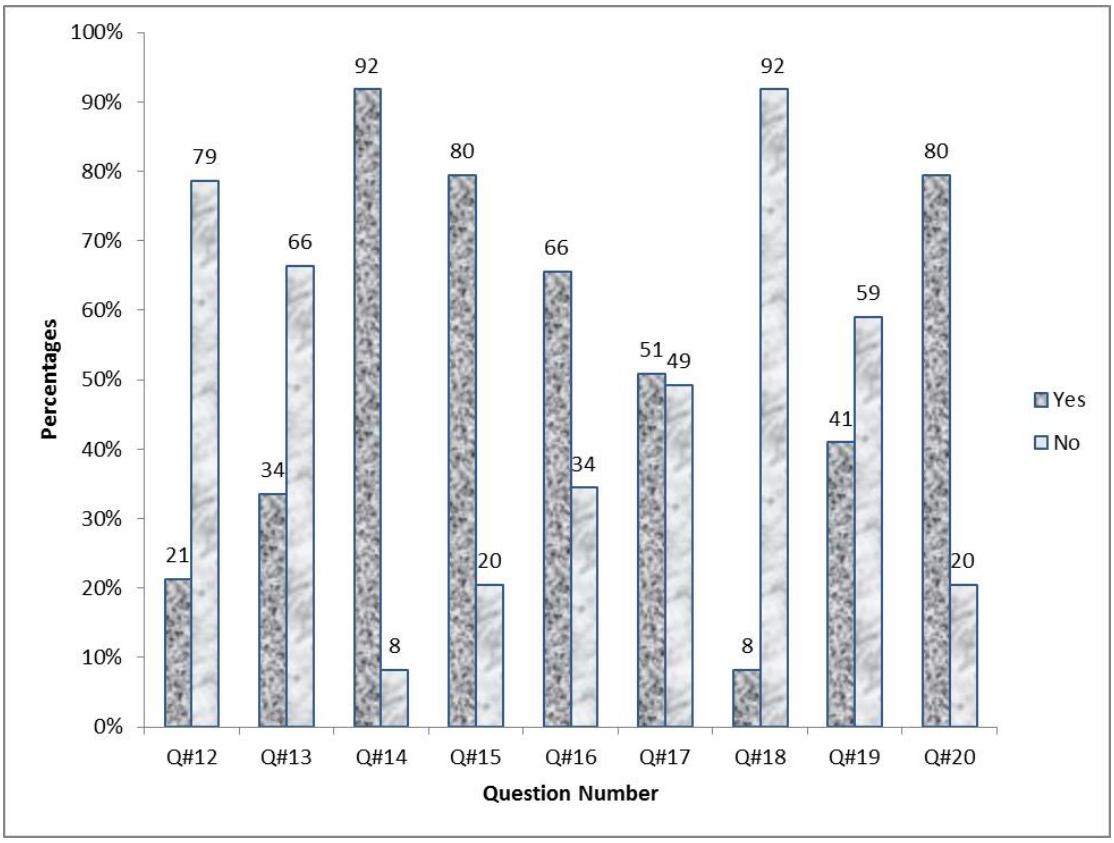

Figure 4-4: Results of question number 12 to 20

12. 21% social media user's privacy is public and their posts on Facebook® and Twitter® or other social media are visible to all internet users which shows that they are less or not concerned about their security and privacy. But 79% users are not concerned about privacy.

13. 34% social media users are sharing their thought on companies, products, services or brands through social media which means that they are not well aware of fact that their information is using directly/indirectly as reference, by the companies.

14. 92% social media users are using their real name and only 8% are not doing so. Using real name as signup name may not be preferable because it increase the chances of detecting and summing the information regarding a person.

15. 20% respondents are still not even aware of privacy setting of social media sites. And there are chances that remaining 80% are aware of Facebook® privacy setting but they are not applying them and do not show much concern about privacy. This is because may be they are not aware of the consequences they can have by doing so.

16. 66% social media users reported that they would report a security break-in of personal machine or network to system administrator who maintains their anonymity which means that they are concerned about their privacy.

17. 51% respondents alleged that they will report a security break-in of their business machine or network to system administrator who does not maintain their anonymity i.e. they are concerned about privacy while 49% said they will not.

18. 8% respondents are those whose credit cards were stolen and 92% were those whose credit cards were not stolen.

19. 41% respondents want to use credit card on the web without considering that their information can be hacked while 59% are against it because they are concerned about their privacy.

20. 80% respondents think that using the Internet for shopping and banking would make life easy. Interestingly good percentage of respondents feel that use of Internet for shopping and banking would make their life easy but as in previous question quite a large number is not willing to use the credit card on the web. This may be because of the lack of awareness.

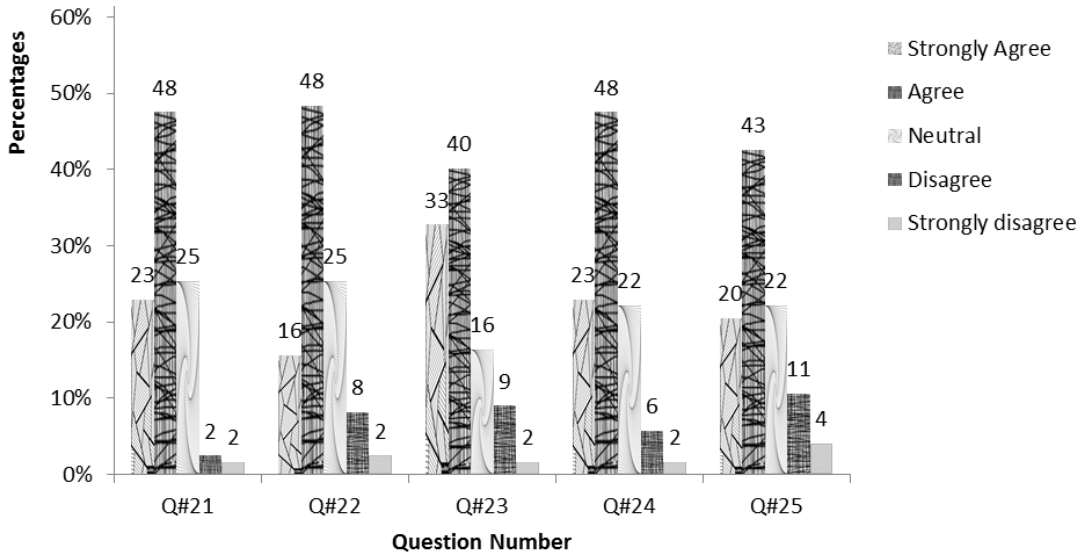

Figure 4-5: Results of question number 21 to 25

21. 48% agreed that companies gather, publicly available content that is posted on social media sites to find out what people say about different companies, brands, products and industries. By doing so, these companies gather knowledge of interests of our public.

22. 35% respondents are not agreeing about future marketing strategy of product / services in social media. This means that they are not aware of this fact. While 65% are agreeing, this clearly shows that they are not concerned about their data privacy. They know that their data will be used but they are not concerned about it.

23. 73% users think that people are concerned but 27% think that people are not even concerned about security importance because they have the opinion that social media users don't know the importance of security.

24. 71% respondents have security concerns in social media (e.g. people reading your email, finding out what websites you visit, etc.) Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identity for you or for someone else while 29% don't bother.

25. 63% social media users are concerned about privacy in purchasing using social media but there is a possibility that they have insufficient knowledge to accomplish.

STATISTICAL INTERPRETATION

Question 11, 18 and 20 are giving information about user interest i.e. related to users profiling. Remaining questions are divided into three groups or categories because we asked some question about privacy concerned and lack of awareness while third group includes security concern to check that how many people are concerned about privacy and how many have lack of awareness. Security concerns group is telling about people those are facing seriously security issues.

No	Groups	Question Numbers
1	Security concerns	5, 23, 24
2	Lack of awareness	1, 9, 14, 15
3	Concerned about privacy	2, 3, 4, 6, 7, 8, 12, 13, 16, 17, 19, 21, 22, 25

Table 4-1: Groups

Table 4-1 is showing the division of questions into three major groups as follows:-

- Security concerns group is telling about people those are facing serious security issues.
- Lack of awareness is telling about awareness level.
- Concerned privacy group is telling about people who are concerning about privacy.

Groups are created because the structured questionnaire was divided in three categories and each category was different from other in respect of data collection. Later on questions in all three categories were divided into groups because:-

1. Some questions were asked to find out the state of security concerns of social media users.
2. Similarly other questions were asked to find social media users who have lack of awareness
3. And remaining questions were asked to find social media users who was concerned about privacy

Variable	Mean
C1	0.9426
C2	2.0656
C3	2.1557

Table 4-2: Mean calculation of Security questions

C1 is variable in Minitab® for question number 5 and its options for answers were two i.e. 0 and 1 and its mean are 0.9426. C2 is the variable in Minitab for question number 23 and C3 is the variable for question number 24 and there options were strongly agree, agree, neutral, disagree and strongly disagree. Mean of question number 23 and 24 are 2.0656 and 2.1557 that are almost same which means that people answer correctly about security concerns as these questions are related.

Group 1: Security Concerns

Population is normal and standard deviation is unknown so t test is used as sample size is also normal.

Question No	Q05	Q23	Q24
Q05	1		
Q23	-0.054 [0.552]	1	
Q24	-0.272 * **[0.002]**	0.447 * **[0.000]**	1
Cell Contents: Pearson's Correlation Coefficient [P-Value]			

Table 4-3: Pearson's Correlation Coefficient of group 1

* indicates those correlations which are not zero, at 5% level of significance.

- A negative correlation coefficient means that an increase in X is associated with a decrease in Y.
- A correlation coefficient of zero, or very close to zero, shows no meaningful relationship between variables.
- Non zero correlation have p<=0.05 which also means that there is relationship

t test of Q23 and Q5:

Question No	n	Mean
Q 23	122	2.0656
Q 05	122	0.9426
Difference	---	1.1230
t-Value = 11.91 P-Value = 0.000		

Table 4-4: t test of Q23 and Q5

Based on P value, it can be concluded that μQ#23≠μQ#5, at 5% level of significance because P<=0.05 and difference is significant so

- "reject the null"
- There is relationship between A and B.
- not likely to be a result of chance (same as saying A ≠ B)

t test of Q24 and Q5:

Question No	n	Mean
Q 24	122	2.1557
Q 05	122	0.9426
Difference	---	1.2131
t-Value = 13.54 P-Value = 0.000		

Table 4-5: t test of Q24 and Q5

Based on P value, it can be concluded that μQ#24≠μQ#5, at 5% level of significance.

t test of Q23 and Q24:

Question No	N	Mean
Q 23	122	2.0656
Q 24	122	2.1557
Difference	---	-0.0902
t-Value = 0.99 P-Value = 0.323		

Table 4-6: t test of Q23 and Q24

Based on P value, it can be concluded that μQ#23=μQ#24, at 5% level of significance.

Group 2: Lack of awareness

Question No	Q01	Q09	Q14	Q15
Q01	1			
Q09	0.220 * **[0.015]**	1		
Q14	0.228 * **[0.012]**	0.143 [0.116]	1	
Q15	0.106 [0.244]	0.117 [0.200]	-0.004 [0.968]	1
Cell Contents: Pearson's Correlation Coefficient [P-Value]				

Table 4-7: Correlation Coefficient of Group 2

* indicates those correlations which are not zero, at 5% level of significance.

- A negative correlation coefficient means that an increase in X is associated with a decrease in Y.
- A correlation coefficient of zero, or very close to zero, shows no meaningful relationship between variables.
- Non zero correlation have p<=0.05 which also means that there is relationship
- To check there exists correlation between the responses of Q1 and Q9, the Pearson's Correlation Coefficient has been calculated and found to be 0.220 having P value of 0.015 which shows that data is not related, though common sense saying they should be related. But as there P value is 0.015 which means that correlation is zero or insignificant and there is a weak evidence. Also r is 0.220 which means that weak positive and having insignificant relation.

  Ho: $\mu 1 \neq \mu 9$

  H1: $\mu 1 = \mu 9$

Hence respondent who use real information does not have sound knowledge of privacy.

t test of Q1 and Q9:

Question No	**N**	**Mean**
Q1	122	0.8033
Q9	122	0.6311

Difference	---	0.1721
t-Value = 3.42	**P-Value = 0.001**	

Table 4-8: t test of Q1 and Q9

Based on P value, it can be concluded that μQ#1≠μQ#9, at 5% level of significance.

t test of Q1 and Q14:

Question No	**N**	**Mean**
Q1	122	0.8033
Q14	122	0.9180
Difference	---	-0.1148
t-Value = -2.95	**P-Value = 0.004**	

Table 4-9: t test of Q1 and Q14

Based on P value, it can be concluded that μQ#1≠μQ#14, at 5% level of significance.

t test of Q1 and Q15:

Question No	**N**	**Mean**
Q1	122	0.8033
Q15	122	0.7951
Difference	---	0.0082
t-Value = 0.17	**P-Value = 0.867**	

Table 4-10: t test of Q1 and Q15

Based on P value, it can be concluded that μQ#1=μQ#15, at 5% level of significance.

Pearson's Correlation Coefficient of Q1 and Q15:

- The null hypothesis of Q1 and Q15 is that data is not related, though common sense saying they should be related. But as there P value is 0.244 which means that correlation is zero or insignificant and there is a weak evidence. Also r is 0.0106 which means that weak positive and having insignificant relation.

- Ho: $\mu 1 \neq \mu 15$
- H1: $\mu 1 = \mu 15$
- So people who are using real information in there account are not related to those who are thinking that they are familiar with Facebook privacy settings. The corresponding P value is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence t value also not lies in rejection region

t test of Q14 and Q9:

Question No	**N**	**Mean**
Q14	122	0.9180
Q9	122	0.6311
Difference	---	0.2869
t-Value = 6.07 P-Value = 0.000		

Table 4-11: t test of Q14 and Q9

Based on P value, it can be concluded that μQ#14≠μQ#9, at 5% level of significance.

t test of Q14 and Q15:

Question No	N	Mean
Q14	122	0.9180
Q15	122	0.7951
Difference	---	0.1230
t-Value = 2.77	**P-Value = 0.007**	

Table 4-12: t test of Q14 and Q15

Based on P value, it can be concluded that μQ#14≠μQ#15, at 5% level of significance.

Pearson's Correlation Coefficient of Q14 and Q15:

- Null hypothesis of Q14 and Q15 is that data is accompanied. The value of correlation is -0.004 with p value 0.968>alpha (0.05). As correlation value is negative which means that these two questions have indirect relationship.

  Ho: μ14=μ15
  H1: μ14≠μ15
- The corresponding P value is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. People who are using real name for sign up are related to those who are thinking that they are familiar with Facebook privacy settings.
- The corresponding P value is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence t value also not lies in rejection region.

Group 3: Privacy Concerns

Table of group 3 including responses of privacy concerns question is given on next page.

	Q02	Q03	Q04	Q06	Q07	Q08	Q12	Q13	Q16	Q17	Q19	Q21	Q22
Q03	-0.028 [0.736]												
Q04	0.209 * **[0.021]**	0.238 * **[0.008]**											
Q06	0.061 [0.507]	-0.002 [0.981]	0.219 * **[0.015]**										
Q07	0.173 [0.057]	0.176 [0.052]	0.06 [0.511]	-0.045 [0.619]									
Q08	0.132 [0.147]	0.323 * **[0.000]**	0.132 [0.147]	0.041 [0.651]	0.352 * **[0.000]**								
Q12	0.154 [0.091]	0.209 * **[0.021]**	0.272 * **[0.002]**	-0.082 [0.369]	0.400 * **[0.000]**	0.255 * **[0.005]**							
Q13	0.186 * **[0.04]**	0.104 [0.256]	0.135 [0.139]	-0.016 [0.858]	0.279 * **[0.002]**	0.2 * **[0.027]**	0.308 * **[0.001]**						
Q16	-0.025 [0.783]	-0.035 [0.70]	0.077 [0.399]	0.065 [0.475]	0.053 [0.561]	-0.013 [0.888]	0.082 [0.368]	0.114 [0.212]					
Q17	0.042 [0.644]	0.115 [0.209]	0.091 [0.32]	-0.064 [0.482]	0.105 [0.25]	0.081 [0.377]	0.192 * **[0.034]**	0.11 [0.229]	0.15 [0.099]				
Q19	0.17 [0.061]	-0.127 [0.162]	0.17 [0.061]	-0.078 [0.39]	0.221 * **[0.015]**	0.203 * **[0.025]**	0.136 [0.135]	0.148 [0.104]	0.183 * **[0.044]**	0.020 [0.830]			
Q21	-0.085 [0.35]	0.063 [0.493]	-0.171 [0.059]	-0.117 [0.199]	-0.106 [0.247]	0.022 [0.811]	-0.099 [0.276]	-0.186 * **[0.041]**	-0.18 * **[0.047]**	0.128 [0.158]	-0.102 [0.266]		
Q22	-0.036 [0.691]	-0.142 [0.12]	-0.116 [0.205]	0.03 [0.74]	-0.167 [0.066]	-0.084 [0.358]	-0.255 * **[0.005]**	-0.203 * **[0.025]**	-0.167 [0.067]	-0.086 [0.345]	-0.196 * **[0.031**	0.390 * **[0.000]**	
Q25	0.032 [0.73]	0.156 [0.086]	-0.061 [0.503]	-0.12 [0.188]	-0.01 [0.909]	0.003 [0.971]	-0.099 [0.28]	-0.223 * **[0.014]**	-0.333 * **[0.000]**	-0.123 [0.105]	-0.105 [0.248]	0.386 * **[0.000]**	**0.226 * [0.012]**

Cell Contents: Pearson's Correlation Coefficient
[P-Value]

Table 4-13: Correlation of questions relating to privacy concerns

- * indicates those correlations which are not zero, at 5% level of significance.

One-way ANOVA: Q21, Q22 and Q25

Source	**F**	**P**
Factor	**2.70**	**0.149**

Table 4-14: One Way Anova of question 21, 22 and 25

Analysis of variance is used because it is use to find statistical significant difference between means of more than two independent questions. P value is greater than 5%, we have weak evidence against H0 so we do not reject Null hypothesis. Hence we concluded that the relation exists.

Ho: $\mu 21=\mu 22=\mu 25$

H1: $\mu 21\neq\mu 22\neq \mu 25$

So companies gathering, publicly available content that is posted on social media sites such as Twitter, blog and forum posts to find out what people say about different companies, brands, products and industries is related to companies using post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.) and people who are often concerned about security in purchasing over social media.

	Percentages of each option of answers				
Question#21	23	48	25	2	2
Question#22	16	48	25	8	2
Question#23	33	40	16	9	2
Question#24	23	48	22	6	2
Question#25	20	43	22	11	4

Table 4-15: Percentages

Above are percentages of question 21 to 25 in which Q21, Q22 and Q25 includes in Group 3 while Q23 and Q24 are of Group 1. Here Pearson's Correlation Coefficient is calculated.

Pearson's Correlation Coefficient of Group 1 and Group 3

Pearson's Correlation Coefficient of Q21 and Q22 = -0.696

P-Value = 0.192

P value for Q21 and Q22 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{21}=\mu_{22}$

H_1: $\mu_{21}\neq\mu_{22}$

So companies gathering, publicly available content that is posted on social media sites such as Twitter, blog and forum posts to find out what people say about different companies, brands, products and industries is related to companies using post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.)

Pearson's Correlation Coefficient of Q21 and Q23 = -0.877

P-Value = 0.051

P value for Q21 and Q23 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{21}=\mu_{23}$

H_1: $\mu_{21}\neq\mu_{23}$

So companies gathering, publicly available content that is posted on social media sites -- such as Twitter, blog and forum posts -- to find out what people say about different companies, brands, products and industries is related to people who are concerned about security importance.

Pearson's Correlation Coefficient of Q21 and Q24 = 0.012

P-Value = 0.985

P value for Q21 and Q24 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{21}=\mu_{24}$

H_1: $\mu_{21}\neq\mu_{24}$

So companies gathering, publicly available content that is posted on social media sites -- such as Twitter, blog and forum posts -- to find out what people say about different companies, brands, products and industries is related to people who have security concerns in social media.

Pearson's Correlation Coefficient of Q21 and Q25 = -0.267

P-Value = 0.664

P value for Q21 and Q25 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{21}=\mu_{25}$

H_1: $\mu_{21}\neq\mu_{25}$

So companies gathering, publicly available content that is posted on social media sites such as Twitter, blog and forum posts to find out what people say about different companies, brands, products and industries is related to people who are concerned about security in purchasing over social media. Pearson's Correlation Coefficient of Q22 and Q23 = 0.879

P-Value = 0.049*

P value for Q22 and Q23 is less than 0.05 therefore it can be concluded that user's opinion before and after is not same. It is indicated by *sign. Hence relation not exists between these two questions.

H_0: $\mu_{22} \neq \mu_{23}$

H_1: $\mu_{22} = \mu_{23}$

So companies using post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.) is related to people concerned about security importance.

Pearson's Correlation Coefficient of Q22 and Q24 = -0.657

P-Value = 0.228

P value for Q22 and Q24 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{22} = \mu_{24}$

H_1: $\mu_{22} \neq \mu_{24}$

So companies using post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.) is related to people who have security concerns in social media.

Pearson's Correlation Coefficient of Q22 and Q25 = -0.361

P-Value = 0.550

P value for Q22 and Q25 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{22}=\mu_{25}$

H_1: $\mu_{22}\neq\mu_{25}$

So companies using post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.) is related to people who are concerned about security in purchasing over social media.

Pearson's Correlation Coefficient of Q23 and Q24 = -0.477

P-Value = 0.416*

P value for Q23 and Q24 is less than 0.05 therefore it can be concluded that user's opinion before and after is not same. It is indicated by *sign. We have strong evidence against H0 and concluded that difference is significant so we are rejecting Null hypothesis. Hence relation not exists between these two questions.

H_0: $\mu_{23}\neq\mu_{24}$

H_1: $\mu_{23}=\mu_{24}$

So people concerning about security importance are related to people who have security concerns in social media.

Pearson's Correlation Coefficient of Q23 and Q25 = 0.000

P-Value = 1.000

P value for Q23 and Q25 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions.

H_0: $\mu_{23}=\mu_{25}$

H_1: $\mu_{23}\neq\mu_{25}$

So people concerning about security importance are related to people who are concerned about security in purchasing over social media.

Pearson's Correlation Coefficient of Q24 and Q25 = 0.621

P-Value = 0.264

P value for Q24 and Q25 is greater than 0.05 therefore it can be concluded that user's opinion before and after is same. Hence strong relation exists between these two questions

Histogram of ages is the graph generated to view ages of respondents who filled our survey.

H_0: $\mu_{24}=\mu_{25}$

H_1: $\mu_{24}\neq\mu_{25}$

So people having security concerns in social media are related to people who concerning about security in purchasing over social media.

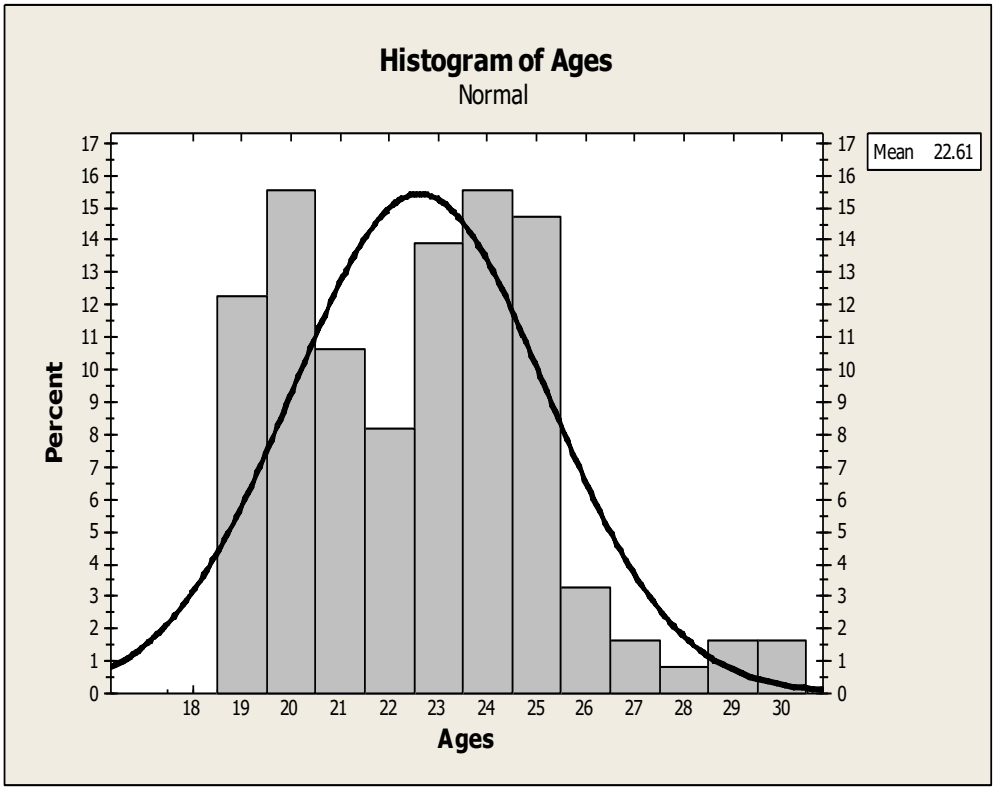

Figure 4-6: Population ages

Graph clearly shows that our population includes majority respondent of 22 year old. Graph is showing percentages on Y-axis while ages on X-axis and distribution is normal.

LAWS

Following are the laws which can ensure you secure and safe online social network usage:-

1: Always be watchful when you are clicking any link sent by even your friend in message or shared openly. For example during my research a case is found in which a user was using her Facebook® account and was also logged in on twitter. She was sent a link on Facebook, she carelessly opened the link and that site asked to again login by entering id password, the user entered by just thinking that may be the session expired so she entered and her id was being hacked so easily.

2: You should be clear that what you are posting. Otherwise your privacy can be easily breached by using posted information. For example in many case include when remember password option was clicked and posted information was used to answer the security question. And security question was right in most teenage cases.

3: Never allow social networking sites to scan your address book.

4: Assume that everything you put on social networking sites is permanent i-e if u delete it later on, even then it exists and anyone can get your photos videos or text anytime.

5: Avoid installing third party application on your social site as it mostly uses your personal information.

6: Don’t use social networking sites at work.

7: User should also show careful attitude while providing their private information online. Be careful when you are providing information such as name, address, place of birth, date of birth, workplace and contact number.

8: It is responsibility of user to keep himself up to date about the changes or improvement in privacy settings made by the social sites as well as all the social site should unite and arrange a meeting and discus how to keep privacy policy much better.

9: Most of these social networks need users to provide firm pieces of information. This allows other users to seek by some type of criteria, majority of social network keeps this information to be mandatory for a user if he or she want to use social sites.

CHAPTER 5

CONCLUSIONS & FUTURE WORK

BACKGROUND

Security and privacy is becoming very much important in social networking sites as people are sharing their personal information. So the survey is giving the ratio of people who are concerning about privacy, who have sufficient knowledge for taking security steps and people who are unaware of outcomes of using social networking sites on their lives.

CONCLUSIONS

In recent times, it has been observed that people frequently share their private information so social networking sites on a vast scale in contrast to other platforms. In this survey, a survey questionnaire is designed that comprise of dependent and independent questions. Dependent questions validate that a person is providing similar answers in those questions and indicate if he / she is filling the survey seriously or not. Afterwards, relation between these questions is also proved by using statistical technique in the result and discussion chapter. Several tests were applied to verify the hypothesis whether it is Null or alternate. Results of the question also show several interesting facts like People are interested in having security in online social network and they are concerned about privacy but they do not know about their information

leak. Consequently, majority of people use social networking sites for prolonged period but have lack of knowledge about security and privacy.

Obj#1: Understanding and extracting the existing awareness state of social media users of NUST, Pakistan about privacy, security steps and information sharing in social media

Con#1

Study is focusing on extracting the existing awareness state of social media users of NUST, Pakistan about privacy, security steps and information hiding / sharing in social media.

Obj#2: Understanding the perception of security and privacy concerns among social media users of NUST, Pakistan and frequency/tendency of people sharing their private information on social networking sites

Con#2

People frequently share their private information on social networking sites in a vast scale in contrast to other platforms.

Obj#3: Statistical analysis of data collected through structured questionnaires

Con#3

Statistical analyses of data collected through structured questionnaires are:-

1. Respondents are concerned about privacy but they do not know about their information leak.

2. Majority of respondent use social networking sites for prolonged period but have lack of knowledge about security and privacy.

3. Respondent are also concerned about security laps in several social sites.

Obj#4: Proposing recommendations to improve security and privacy in online social networks

Con#4

Recommendations proposed to improve security and privacy in online social networks.

Though social networks are getting better at protecting users against these threats – but there's a long way to go **so you don't stop using social media, instead just make sure you use it safely!**

FUTURE WORK

- This study may be useful for creating awareness in masses for complex issues especially related to privacy which is usually ignored in our society.
- For generalization of results further exploration is required by increasing the sample size along with various section of the society i.e. doctors, engineers and skilled workers etc.

LIMITATION OF STUDY

- The current study uses data of 122 respondents (students of NUST), 60 from software engineering, computer science and Information Technology while 62 from Business and Civil

Annex-A

1. Do you use your credit card for online purchasing? Yes/No
2. Do you use your credit card for online purchasing? Yes/No
3. Do you answer pop-ups while surfing Internet? Yes/No
4. Have your social account ID ever been hacked by redirecting to a fake webpage? Yes/No
5. Do you think “Stalking and impersonation (including forged identity) are common on the Internet” Yes/No
6. Have you ever been concerned about abuse of your credit card and other personal information when/if you purchase things online? Yes/No
7. Would you put your name and address in a directory for public access on the Web (e.g. the online equivalent of a phone company's "White Pages")? Yes/No
8. Do you accept strangers who try to friend you in social networking sites? Yes/No
9. Do you think privacy policies are effective in social networking sites? Yes/No
10. How long do you spend on social networking sites during a typical day?

    (i)5-10 min (ii)30 min- 1hour (iii)1 hour- 2 hour (iv)2hour-3hour (v)3hour-4hour (vi)4hour-5hour (vii)5+ hour
11. Which privacy option did you choose for 'your status, photos and posts?

    (i) Every one (ii)Friends Only (iii)Friends of Friends (iv)Customize Friends

    (v)Only Me (vi)I don’t put this info
12. Are your posts on Facebook and Twitter or other social media visible to all internet users? Yes/No
13. Do you share your thoughts on companies, products, services or brands through social media? Yes/No
14. Did you use your real name as sign-up name? Yes/No
15. Do you think you are familiar with Facebook privacy settings? Yes/No
16. Would you report a security break-in of your personal machine or network to system administrator who maintains your anonymity? Yes/No
17. Would you report a security break-in of your business machine or network to system administrator who does not maintain your anonymity? Yes/No
18. Have you ever had your credit card number stolen (either online or

offline)? Yes/No

19. Are you willing to use your credit card on the web? Yes/No

20. Do you think using the Internet for shopping and banking would make life easy? Yes/No

21. Some companies gather, publicly available content that is posted on social media sites -- such as Twitter, blog and forum posts -- to find out what people say about different companies, brands, products and industries.

(i) Strongly agree (ii) Agree (iii) Neutral (iv) Disagree (v) Strongly disagree

22. Companies use your post in social media about their products/services to inform its future marketing strategy (advertising campaign, product improvement, sales strategy, etc.)

(i) Strongly agree (ii) Agree (iii) Neutral (iv) Disagree (v) Strongly disagree

23. People are concern about security importance.

(i) Strongly agree (ii) Agree (iii) Neutral (iv) Disagree (v) Strongly disagree

24. People have security concerns in social media (e.g. people reading your email, finding out what websites you visit, etc.) Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identity for you or for someone else.

(i) Strongly agree (ii) Agree (iii) Neutral (iv) Disagree (v) Strongly disagree

25. People are often concerned about security in purchasing over social media.

(i) Strongly agree (ii) Agree (iii) Neutral (iv) Disagree (v) Strongly disagree

References

[1] *Irani, Danesh, et al. "Reverse social engineering attacks in online social networks." Detection of intrusions and malware, and vulnerability assessment. Springer Berlin Heidelberg, 2011. 55-74.*

[2] *Beach, Aaron, et al. "Whozthat? evolving an ecosystem for context-aware mobile social networks." Network, IEEE 22.4 (2008): 50-55*

[3] *Lee, Mark JW, ed. Web 2.0-Based E-Learning: Applying Social Informatics for Tertiary Teaching: Applying Social Informatics for Tertiary Teaching. IGI Global, 2010.*

[4] *Pearson, Siani. "Privacy, security and trust in cloud computing." Privacy and Security for Cloud Computing. Springer London, 2013. 3-42*

[5] *Drapeau, Mark, and I. I. Wells. Social software and national security: An initial net assessment. NATIONAL DEFENSE UNIV WASHINGTON DC CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY, 2009.*

[6] *Nair, Sunil, et al. "Evidence management for compliance of critical systems with safety standards: A survey on the state of practice." Information and Software Technology 60 (2015): 1-15.*

[7] *Maggiani, Rich. "Social media and its effect on communication." SOLARI Making the Complicated*

[8] *Saransomrurtai, Chayanin. Converting a social network into a brand network: How brand profile on Facebook is used as an online marketing communication tool. Diss. Auckland University of Technology, 2011.*

[9] *Gianvecchio, Steven, et al. "Battle of botcraft: fighting bots in online games with human observational proofs." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.*

[10] *Tuunainen, Virpi Kristiina, Olli Pitkänen, and Marjaana Hovi. "Users' Awareness of Privacy on Online Social Networking sites-Case Facebook." Bled 2009 Proceedings (2009):42.*

[11] *Raynes-Goldie, Kate. "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook." First Monday 15.1 (2010) Simple (2009).*

[12] *Thierer, Adam. "Pursuit of Privacy in a World Where Information Control Is Failing, The." Harv. JL & Pub. Pol'y 36 (2013): 409.*

[13] Strahilevitz, Lior Jacob. "A social networks theory of privacy." *The University of Chicago Law Review* (2005): 919-988.

[14] *Kim, Won, Ok-Ran Jeong, and Sang-Won Lee. "On social Web sites." Information systems 35.2 (2010): 215-236.*

[15]*Minocha, Shailey. "Role of social software tools in education: a literature review." Education+ Training 51.5/6 (2009): 353-369.*

[16]*Braunschweiger, Paul, and Kenneth W. Goodman. "The CITI program: An international online resource for education in human subjects protection and the responsible conduct of research." Academic Medicine 82.9 (2007): 861-864.*

[17] *Kessler, Laura T. "'A Sordid Case': Stump v. Sparkman, Judicial Immunity, and the Other Side of Reproductive Rights." Maryland Law Review, Forthcoming(2014).*

[18] *Norris, Ingrid N. Mitigating the effects of doxing. Diss. Utica College, 2012.*

[19] *Cain, Jeff. "Social media in health care: the case for organizational policy and employee education." American Journal of Health-System Pharmacy 68.11 (2011): 1036-1040.*

[20] *Krishnamurthy, Balachander, and Craig E. Wills. "Privacy leakage in mobile online social networks." Proceedings of the 3rd Wonference on Online social networks. USENIX Association, 2010.*

[21] *Alam, Iftikhar, et al. "Conducting surveys and data collection: From traditional to mobile and SMS-based surveys." Pakistan Journal of Statistics and Operation Research 10.2 (2014): 169-187.*

[22] *Pearson, Siani. "Taking account of privacy when designing cloud computing services." Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society, 2009.*

[23] *Albrechtslund, Anders. "Online social networking as participatory surveillance."First Monday 13.3 (2008).*

[24] *Boss, Scott R., et al. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security." European Journal of Information Systems 18.2 (2009): 151-164.*

[25] *Jansen, Bernard J. Use of the internet in higher-income households. Pew Research Center, 2010.*

[26] *Seligman, Martin EP. "The effectiveness of psychotherapy: the Consumer Reports study." American Psychologist 50.12 (1995): 965.*

[27] *Goettke, Richard, and Joseph Christiana. "Privacy and online social networking websites." Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology (2007).*

[28] *Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.*

[29] Lam, Ieng-Fat, Kuan-Ta Chen, and Ling-Jyh Chen. "Involuntary information leakage in social network services." *International Workshop on Security*. Springer Berlin Heidelberg, 2008.

[30] Altshuler, Yaniv, et al., eds. *Security and privacy in social networks*. Springer Science & Business Media, 2012.

[31] Hugl, Ulrike. "Reviewing person's value of privacy of online social networking." *Internet Research* 21.4 (2011): 384-407.

[32] Pasquale, Frank, and Tara Adams Ragone. "Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing." *Stan. Tech. L. Rev.* 17 (2013): 595.

[33] Jones, Simon, and Eamonn O'Neill. "Feasibility of structural network clustering for group-based privacy control in social networks." *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010.

[34] *Altshuler, Yaniv, et al. Stealing reality: when criminals become data scientists (or vice versa). Springer New York, 2013.*

[35] Wortley, Richard, and Stephen Smallbone. *Internet child pornography: Causes, investigation, and prevention*. ABC-CLIO, 2012.

[36] *Salama, Mostafa, et al. "Computational Social Networks: Security and Privacy." Computational Social Networks. Springer London, 2012. 3-21.*

[37] Kekwaletswe, Raymond M. *Knowledge transformation in a mobile learning environment: an interpretive inquiry of ubiquitous context and social presence awareness*. Diss. University of Cape Town, 2007.

[38] Sattarova Feruza, Y., and Tao-hoon Kim. "IT security review: Privacy, protection, access control, assurance and system security." *International journal of multimedia and ubiquitous engineering* 2.2 (2007): 17-32.

[39] Kim, Won, et al. "The dark side of the Internet: Attacks, costs and responses." *Information systems* 36.3 (2011): 675-705.

[40] *Chbeir, Richard, and Bechara Al Bouna. Security and privacy preserving in social networks. Springer, 2013.*

[41] Howison, James, Andrea Wiggins, and Kevin Crowston. "Validity issues in the use of social network analysis with digital trace data." *Journal of the Association for Information Systems* 12.12 (2011): 767.

[42] Ferrara, Emilio, et al. "Web data extraction, applications and techniques: a survey." *Knowledge-based systems* 70 (2014): 301-323.

[43] *Gurses, Seda, and Carlos Diaz. "Two tales of privacy in online social networks." Security & Privacy, IEEE 11.3 (2013): 29-37.*

[44] Mayer, Jonathan R., and John C. Mitchell. "Third-party web tracking: Policy and technology." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

[45] Laufer, Robert S., and Maxine Wolfe. "Privacy as a concept and a social issue: A multidimensional developmental theory." *Journal of social Issues*33.3 (1977): 22-42.

[46] *Taheri-Boshrooyeh, Sanaz, Alptekin Kupcu, and Oznur Ozkasap. "Security and Privacy of Distributed Online Social Networks." Distributed Computing Systems Workshops (ICDCSW), 2015 IEEE 35th International Conference on. IEEE, 2015.*

[47] Stallings, William. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[48] *Verma, Akriti, Deepak Kshirsagar, and Sana Khan. "Privacy and security: Online social networking." International Journal of Advanced Computer Research 3.8 (2013): 310-315.*

[49] Aiello, Luca Maria, and Giancarlo Ruffo. "LotusNet: Tunable privacy for distributed online social network services." *Computer Communications* 35.1 (2012): 75-88.

[50] *Aldhafferi, Nahier, Charles Watson, and A. S. Sajeev. "Personal information privacy settings of online social networks and their suitability for mobile internet devices." arXiv preprint arXiv:1305.2770 (2013).*

[51] Aimeur, Esma, Sebastien Gambs, and Ai Ho. "Towards a privacy-enhanced social networking site." *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 2010.

[52] *Humbert, Mathias, et al. "Nowhere to hide: Navigating around privacy in online social networks." Computer Security–ESORICS 2013. Springer Berlin Heidelberg, 2013. 682-699.*

[53] *Sattikar, A. A., and Dr RV Kulkarni. "A Review of Security and Privacy Issues in Social Networking." International Journal of Computer Science and Information Technologies 2.6 (2011): 2784-2787.*

[54] Debatin, Bernhard, et al. "Facebook and online privacy: Attitudes, behaviors, and unintended consequences." *Journal of Computer-Mediated Communication* 15.1 (2009): 83-108.