International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876
Impact Factor: RJIF 5.44
www.newengineeringjournal.in
Volume 4; Issue 1; January 2018; Page No. 48-56

Online social networks: Analytical review of challenges and possible recommendations

Muhammad Adnan, Jawad Ali, Shahid Ali
Abdul Wali Khan University, Pakistan

Abstract
Online Social Networks are the backbone for online communication. Social Networking Sites provide virtual community for online users to share their thoughts, activities, interests, pictures etc. These sites are fastest, easiest and cheapest way for communication that's why Social Networking Sites become more popular in the world wide. Each user of Online Social Network has their own profile, which contain user personal information (name, contact number, address, date of birth, hobbies, interest etc). Some commonly used Social Networking Sites are Face Book, Twitter, My Space, Google Plus and LinkedIn. Among all of these, face book has peak value users. Default privacy setting of Face Book is public where each and every user is able to access each other information without awareness. Face book provide privacy up to some limit but these privacy are hard to implement for a common user. Existing privacy policies of Online Social Networks are unable to protect user personal information. In proposed work we have discuss major problems related to Online Social Networks privacy and different types of attacks on Online Social Networks/users, finally we proposed some recommendation, which improve privacy of Online Social Networks and reduces attacking risks.

Keywords: online social network, social networking sites, privacy, personal information, security

1. Introduction

Online Social Networks are one of the most well-known communication medium [22]. OSN are social graph where individuals/groups represent nodes and links between them show relationship [1-2, 11, 17-19, 29-35]. Online Social Networks are simplest and easiest way for connecting users to each other's [4, 9, 13]. These networks have hundreds of millions of users which access these networks on daily basis [16, 25]. OSN are popular throughout globe [2, 25]. There are more than 300 SNS [5], but most well-liked between them is face book, which is secondly topmost visited website after Google [4], and was launched in year 2004 [11]. Face book have 1.23 billion active users on monthly basis as of December 2013 [16]. Face book provide graphical user interface for using his feature, through GUI it's easily accessible for general users [1, 22]. Surfing of internet has become increased due to availabilities of OSN [1]. Figure 1 shows number of users in millions on each OSN [6, 9, 26, 27, 28].

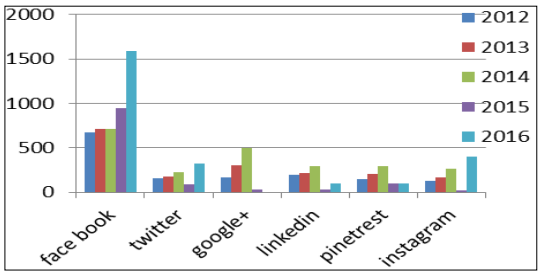

Fig 1: Users on different social network

Online Social Networks provide a lot of facilities to his users for motivating them [1, 3, 4, 7, 8, 23]. A survey conducted in 2012 show that 79% users use OSN for business purposes and 82% users use for personal reasons [12]. Every OSN user has own profile through which they connect to SNS [18, 22, 23, 24], generally profile contain personal information of users [4, 5, 7, 10, 13, 22, 23]. Profile also contain friends list [22, 23, 24], which include family members, friends, identified and strangers, anything user want to share are accessible to his friends list but sharing private information lead to risks [1, 5, 6, 36-40]. These networks tie all friends in same category, that is harm full, additionally face book and twitter provide grouping concept but that do not mimic real life friend ship [20]. Mostly users login to his OSN account through mobile phones [6] A survey conducted in year 2013 show that face book had approximately 556 million active mobile users on routine basis [1], and 945 million access face book through mobile phones on monthly basis as of December 2013 [16]. A lot of users unaware from revealing his personal information, [3, 6, 11, 14] alternately younger's are not give any concentrate on revealing his personal information because they are unaware from revelation results [5]. Figure 2 shows age wise users of OSN [6].

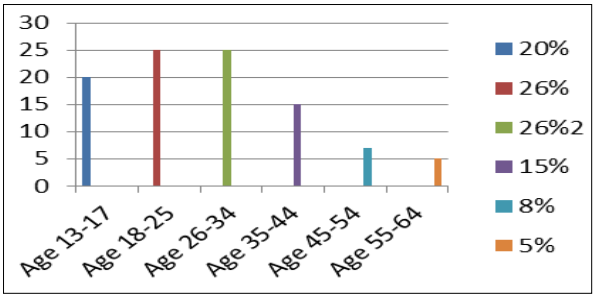

Fig 2: Age wise Users on Different OSN in Millions

In our proposed work we have categorized different attacks on OSN and suggested some recommendations which reduce information revelation threats.

2. Problems associated with OSN

Due to high concentrate of users on SNS it attracts attackers [10, 24]. There are a lot of threats concerning with Online Social Network, Figure 3 shows percentage of threats on individual OSN [11].

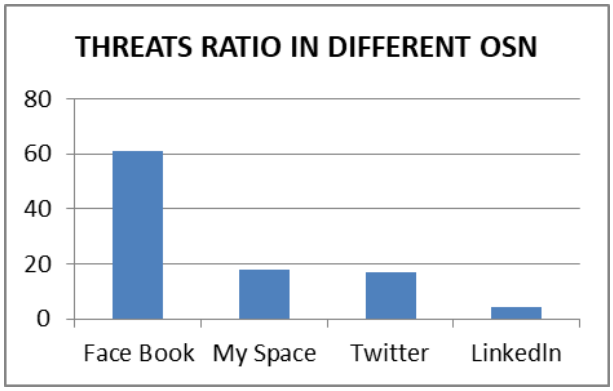

Fig 3: Threats Ratio Associated With Different OSN

In this paper we have categorized risks regarding with online social networking sites which are, privacy concerning threats and attacking scenario.

2.1 Privacy concerning threats

i) Default privacy setting of face book

Most users unaware from current security setting of face book, they think that available privacy policies are enough to protect our personal data [20-25]. Face book provide privacy policies up to some extent but default setting of face book is public which allows each and every user whether it's a friend, friend of friend or visitor can access personal data of user. Mostly users are unconscious that how to change default privacy setting and for a common user it's hard to sense that what's changes present after altering default privacy setting [3, 5, 7, 8, 9, 10, 12, 14, 20, 24].

ii) Available privacy policies of SNS

Available privacy policies of some OSN including face book is detailed than others. But few users know that how to implement them. If someone implements existing privacy policies user's data will be protected from common users but not from experts/hackers [1, 4, 7, 9, 13, 22]. In next section we will discuss that how attackers extract user data after implementing available privacy policies.

iii) 3rd party applications

Commonly users suffer social networking sites for leisure purposes. 3rd party application offer entertainment such as games and quizzes and other functionalities to attract users. 3rd party application has second degree access to user personal data. It's a big hole in security of OSN. OSN is open platform and allow 3rd party applications to access user personal data without compromising them. With third party integration it's hard to find that which application used which kind of user information. Users are unaware that his information is revealed to 3rd party application and these applications used user data for his own purposes, as many business acquired user email address to mark them in his audience for enhancing his productivity [4, 6, 9, 10, 13, 21, 24, 25].

iv) Risky friends

Some information's of users appears to his friends after implementing privacies, that information also accessible to his friends of friend who are stranger for them and they are risky for user. Some friends are also vulnerable for user's personal data for e.g. if friend "A" implements privacy to hide his relation from others and his friend "B" have keep weaker privacy setting so third party can view his relation through friend "B" [7, 13]. Moreover if one user secured his data from outsiders and allow him to his friends, his friend can share his secured data to outsider [18].

v) OSN service providers

Before creating account in OSN, user compromise with OSN service provider about his personal information, it's not sure that OSN service provider keep respect of his privacy policies [18]. Any contents that are available on OSN are accessible to OSN service provider and they are authoritative by allowing any party to access specific information [17-18]. OSN service provider used user personal data for business purposes. Illegally they give access to 3rd party application without awareness of users. Additionally if user wants to delete his account they cannot delete them completely, some personal information retained about user after deactivating account which are exposed for user [13, 14]. Furthermore Google+ and face book used centralized architecture where all users' data are stored on central domain and a single administer administrate all users information and they are not trustworthy for user to keep respectful check on users data. They used user's data for his own beneficiary purposes [7, 8, 21]. So social networks providers itself risky for users information [18].

vi) Adding strangers to friends list

Commonly user specially younger's add more friends to receive more likes and comments, they make request to strangers and also add strangers in his friend list, some users add unknown to keep aware himself from different civilizing and background, But they are unaware that how strangers misuse his personal information [1, 5, 7, 9]. On another hand, some users want to protect his information from family members not from strangers, they post abuse posting on user wall as users follow them, they click to wrong path which lead to malicious attack [3], that we will explain in next section.

vii) Trust on third party domain by OSN service providers

Many OSN uses 3rd party domain for tracking user's activities, which are unwanted for users. Also they compromised with advertisement partner on user personal data for his own advantage without user awareness [6, 10, 18, 21].

viii) Comment controversies

This is common in Face book that, most time chatting take place on photo, the drawback of this conversation is that, if NGO members upload a photo of charity which they have

conducted, the conversation start on post and some of secret concerning events reveal on the result [5].

ix) User anonymity
Many users use real name for profile name, hacker's used profile name for index searching on the basis of which they can access all personal information of user. Additionally profile owner may be the chance of losing job; if employer visits his profile they can easily understand the nature of candidate [6 18, 24, 25]. Some users use fake name for anonymity risk prevention but attackers used de-anonymization attack to extract user real identity. In this attack attackers used different techniques such as tracking cookies, network topology and user group membership [1, 10, 16].

x) Information leakage
Leakage of personal information is pivotal issue in Online Social Network. Hackers can easily put on personality of someone else and take membership in a specific group and they can easily extract personal/sensitive information of that group which is only accessible to members. Leakage of personal information is also negative impact on user's personality, as leakage of drinking and other abuse habitat [1, 14, 16, 18, 21].

xi) SNS aggregators
Application like snag, profile linker allowed SNS to integrate user's data on single web application but risk associated with such application is weak authentication methods which may lead to identity theft and XSS attack [14].

xii) Eavesdropping
Many internet users access internet through mobile devices [4, 6, 18, 25]. On most public places WIFI available for accessing internet. But accessing WIFI at some places leads to information revelation threats, as many public places used vulnerable wireless access point. Many SNS provide insecure communication layer which capturing user's transmitted data through Sniping tools [4, 25].

xiii) Extreme-scale analytics
The system is created by Raytheon called Riot. Through Riot it is probable to snapshot every moment of a person life, his friend's and visited places and they charted them on a map. Through Riots our location can easily accessible to access photographs and videos that we post on SNS. It is because of weak privacy provided by SNS, which is not only infected for SNS but also vulnerable for our daily life [3].

2.2 Attacking scenario

2.2.1 Attacks on profile image
Many users share his real images on SNS every day, where hackers used them for abuse purposes, without user awareness. Profile image is pivotal source for profile cloning. Attackers extract profile image of victim and used them for duplicate profile. General attacks used by attackers for profile image extraction [6].

- Image dragging
- Click on right button and save as image
- By snipping tool
- Save image after print preview
- Using shortcut keys Ctrl+A, Ctrl+S
- Temporary internet folder
- Getting image by using print screen button

Hackers extract profile image for the purpose of duplicate profile, finding user current location by using CBIR/Face recognition techniques and also to find his victim account on any other SNS. Additionally there is no security involved with profile image [4, 9, 14, 16].

i) Image dragging
As user posted his real images on OSN, OSN is open platform and accessible through internet where user image are easily accessible to hackers. Hackers just drag the image into the desired location where they want to store them [6].

ii) Click on right button and save as image
This option is commonly allowed in all SNS. Attacker just right click on desired image a pup up menu appear with some option, here attackers can select save as option and then browse his computer memory for keeping image [4, 6].

iii) By snipping tool
This tool used in advance operating system, which used for copying any detectable object. We can select any area of available content and save them in our computer memory. Hacker can easily copy his victim profile picture and saves them [6].

iv) Save image after print preview
In this method hacker just click on Ctrl+P shortcut key, this is used for printing web page. As printing dialogue box open hacker just select save option and browse his computer memory for saving image [6].

v) Using shortcut keys Ctrl+A, Ctrl+S
Hackers click Ctrl+A shortcut key on desired web page, which select all page contents after selecting all page contents they click Ctrl+S and browse his computer memory and save all contents. Contents consist of current webpage text and graphic [6].

vi) Temporary internet folder
This folder is present in all computers system. As user load web page all his multimedia contents automatically stored in this folder. For next time if user load same page again its loaded from this folder and if page contain some additional contents that contents will loaded from server side. This folder keeps all multimedia contents on permanent base although user deletes them manually. Hackers get his victim profile image from this folder [6].

vii) Getting image by using print screen button
Normally keyboard contains a button named print screen. This is used to capture visible contents of page. Visible contents of page are temporarily stored on RAM memory and then can be pasted in paint program. Hacker used them for getting his victim image [6].

2.2.2 Attacks targeted adults

SNS are popular now days in whole world, the usage of SNS is popular among whole population especially younger's give high attention to SNS than others [3]. On another hand mostly younger's is not care of his information they are not scared from his information revelation because they are not aware from their results [5]. Attacks related to adults are.

- Online predators
- Risky Behavior
- Cyber-Stalking

i) Online predators/sexual harassment

Online predators make a friendship with innocent boy/girl for the purpose of rapping or kidnapping. They collect personal information about his victim and found them geographically. On time they make physically attack on them [1, 13, 16].

ii) Risky behavior

While in chat room mostly younger's chatted with strangers, mostly younger's provide his private/abuse photos to strangers, which may lead to behavioral threat [1, 16].

iii) Cyber-stalking

These are harassment technique; this attack differs from identity theft. In this attack attackers may or may not copy personality of someone else, attacker represents himself of a different nature, sex, age and also changes his other details. Then attackers collect all details of victim. And make physical attack on them [1, 4, 8, 14, 16].

2.2.3 Identity theft

In online social network every user has their own profile which consists of user personal information and every user has their own identity through which others identified him. Hacker used an attack in which they copy identity of someone and represents himself as they are the real one; this attack is known as identity theft attack. Furthermore hackers misuse the identity of his victim which dismisses the reputation of victim [8, 9, 10, 24]. Figure 4 show percentage of identity theft in each OSN individually, Survey 2011 [8].

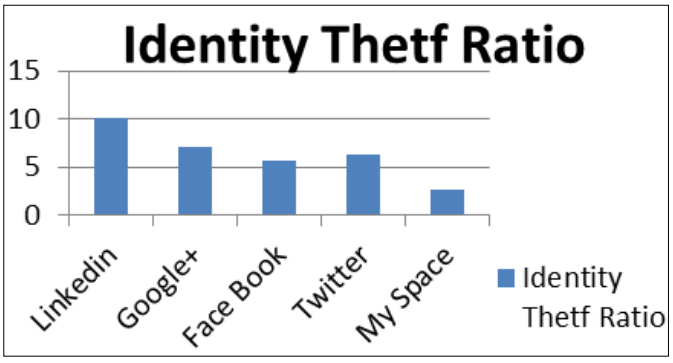

Fig 4: Identity Theft Ratio on Different OSN

A. Profile cloning

Hacker used name, profile picture and other personal information of victim and create copy of his profile which is known as profile cloning [2 10]. There is no security associated with profile cloning, hackers easily extract his victim personal information and make clone of his profile which they used for neglect purposes [9, 15]. Hackers take advantage from default setting of face book, which allow every user to access user profile data [3, 5, 8, 9, 10, 14, 16, 20]. Clone profile is used in two places which are categorized as.

- Cross site profile cloning
- Existing profile cloning

i) Cross site profile cloning

In cross site profile cloning, attackers used clone profile of his victim on another SNS, where user has not registered before. Hackers also send friend request to victim friends who are registered on that OSN for the purpose to access his profile data [2, 9, 10, 14, 21].

ii) Current profile cloning

As this is common in OSN that mostly users have multiple accounts, on these basis request made by attackers are easily accept by his victim friends. In current profile cloning, attackers used his victim identity in existing Social Network. Attacker send friend request to victim friends as they accept them, attacker got access to his friends profile [2, 9, 10, 21].

B. Phishing attack

In OSN first phishing attack was done in 2007 [9]. This attack is done to steal users confidential information**,** attackers provide fake interface for accessing user personal, sensitive, Credit card, banking and financial information [1, 3, 9, 10, 15, 16, 21]. According to current survey 84.5% of phishing attacks target OSN [1]. Mostly in OSN attackers recommend to victim, that authenticates your profile otherwise your account will be expired and provide him false interface as user enter his sensitive information they are accessed by attacker. This attack is success for most time due to unawareness of users [6].

i) Key logging

In this attack, attacker send an infected file which consist key logger, as victim execute the file then, a bit of data that victim typing will be uploaded on hacker server without awareness of user. Attacker also gets all passwords which victim used for any account on his system [15].

ii) Session hijacking

In session hijacking attack, attackers first capture the communication of victim with SNS. Then attacker captures the HTTP header, HTTP header contain session cookies which many websites used for validation purpose. Now attacker can copy HTTP session and use it for extracting victim profile [10, 15].

iii) Social engineering attack

In this attack, attacker sends a fake email to victim, which is very attractive for victim and asking victim to enter his password as victim enter password his password reveal to attacker [15].

iv) Trojans attack

In this attack, attacker sends an infected server to victim as

victim execute the infected server Trojan open a back door on victim PC, now attacker can extract whatever he wants from victim PC.

2.2.4 Malware attack

Malware is harmful code which disturbs the operation of computer system and for gaining access to user credential information so that attackers can easily access user private information [1]. In this attack, attackers provide malware injected code as user click on that URL, false information are posted on his wall. Another way, as user follow malware injected code URL, they got access to fake website where a false interface asked user to enter his sensitive information and also client side code installed on victim system which steal information stored on the system [3, 6, 10, 16, 21].

Malware are injected to the following ways.

- Fake profile/Sybil
- 3rd party application
- False advertisement
- Shortened URL
- Cross site scripting, viruses and Worms
- Click jacking
- Watering hole

i) Fake profile

With fake profile, an attacker mimics personality of someone else and represents himself a celebrity person. In this way attacker can easily spread malware on different ways, as user click on view profile of attacker which put on personality of some celebrity, malware injected to his system [24].

ii) 3rd party application

Third party application is attractive application; attackers also spread malware by using third party application. Malware are injected through third party application when user is trying to install them [10, 13].

iii) False advertisement

The malware also injected through advertisement. False advertisement consist malicious code as user follow them malware injected in his system [15]. The antivirus company, Trend Micro originated that, some face book applications compromised with advertisement companies [10].

iv) Shortened URL

Every web page has unique URL, some URL have much long for reducing them shortened URL methods is used. By following shortened URL its lead to original address. Attacker used shortened URL for spreading malware. As social circle based on trust, if a user share shortened malware injected URL his friend will follow them and result they will be entrapped in malware attack. Symantec Cooperation Survey conducted on malicious shortened URLs in OSN show that, 65% URLs of Online Social Networks are shortened URLs and from them 88% URLs follow by social networks users [10].

v) Cross site scripting attack

Cross site scripting (XSS) is a virus worm which is browser side script and spread out among chain of users that's why OSN is best choice for (XSS) attack. The attacking scenario of (XSS) attack, attacker select a source node for spreading malware, as source node log in to SNS, malware will take control of browser. Then attacker act as an account owner, they can send messages to other SNS users, add application to user account, steal contact list of victim, access cookies, access sensitive information, access session token etc. The process will be continuing and malware will be injected in the form a chain [16].

vi) Click jacking

In Social Networking Sites click jacking is known like jacking. In this scenario, attacker spread malware code by hiding them into a button or an item as user press on that button/item malware injected into his system for example embedding malware into fake advertisement "LIKE" button, also this attack lead to access personal information of users. For example fake video player same as YouTube interface are present to user as user click on them they lead to a fake interface where user personal information are required for proceeding up, as user enter his personal information attackers access them [9-10]. Popular malware examples are

- Koobface
- Twitter worm

a) Koobface

Koobface is a worm that spread through messages in face book and my space in the form of a video link, as user trying for playing video a message asking user to update his flash player. As users install update plug in his computer will be infected and attacker can steal his information as well as use his system for attacking on another computer [10].

b) Twitter worm

Twitter worm spread through twitter. Common types of twitter worm are [10].

- **Profile spy worm:** This worm spread through downloading "profile spy" which is a third party application that is a fake application which permits users to find out who has viewed their profile. For downloading such application users must fill some information, that information is accessed to attacker. Malware code then injected into followers after infecting victim account [10].
- **Goo.gl worm:** Malware spread through this worm in the form of shortened Google URL. As users click on URL users lead to a fake antivirus website and a message displayed that your computer has been infected and suggest to users for installing fake antivirus software. After installing fake antivirus users system got infected [10].

vii) Watering whole

This attack was firstly done on face book in 2013. This attack is not used for extracting user information but it's used to infect the system of developer. In 2003 attacker hacked a mobile developer forum as developer visited to his system their system got infected. After face book this attack was also done on other companies not only on SNS [9].

2.2.5 Spam issues

Spam attacks are done to overload the communication channel, its unwanted messages that send attacker on

communication path [1]. But traditional spam attack are not reach to the victim, as many users are aware from these attacks and if spam reach to victim system due to awareness of users they delete them. New spam attacks are in the form of.

- Wall posts
- News feed
- Message spam

The SNS spam commonly consist advertisement and hyperlink that come from fake websites, as users will follow them they will entrapped in spam attack further its lead to phishing and malware attacks [10].
Other spam attacking strategies are.

A. Email based spam attack

In this attacking scenario, attackers get email address of victim and forward spam mails to victim. OSN also provide option to protect email address from others but attackers extract email address through first and last name. OSN also provide the facility to search someone through email address, attackers generate randomly email address for finding his victim [6, 10]. There are two types of email spam which are.

- Broadcast spam
- Context-Aware spam

i) Broadcast spam

In this spamming attack, attacker generates spam emails to all email addresses which are in their list. But email is not specified to one email, so victim easily recognized them and deletes the [10, 21].

ii) Context-aware spam

In this attack, attacker collects context information or relationship of victim to other users, through these information attacker send spam emails [6, 9, 10, 21].

2.2.6 Physical threats

Providing personal information is lead to physical, psychological and property base threats. As users of SNS provide his real name, contact number and home address which may leads several physical threats [1-6], [7, 10, 11, 18]. These threats are Risky Behavior, online predators, and cyber stalking which have been discussed. Attackers track his victim by extracting the Time line history provide by face book, Time line consist all previous details like places visited and attending events. Time line encourage users to upload his images/video by time manner, attackers inspect the time line of a user and understand the nature and habitat of user, that is easy way for attackers to collect old detail about victim. Another feature Geo tag which allow users to tag location with image, which expose the location of user [10]. Additionally sharing day to day activities may also lead physical threats, especially for female like to post that I am going for shopping at 12:00 O clock, lead to kidnapping [6, 30-36].

3. Recommendations

1. **Bound your personal information:** SNS are accessible through internet and internet always public. Do not provide real information such as home address, contact number, date of birth and daily events. Such information cause physical attack and online predator.
2. **Change privacy setting:** As default privacy setting of face book provides access to every user to extract user's personal information's. Default setting of face book welcomes to each attack. Face book provides privacy up to some limit. So be aware from default setting of OSN particularly face book.
3. **Skip suspicious application/links:** Many SNS provide platform for third party application which is in the form of entertainment or functionality. Skip those applications/links which asked about your personal information for proceeding up. These applications / links lead to malware, phishing, profile cloning and spam issues.
4. **Do not trust on strangers:** Some information must revealed to your friends list, so do not add persons which are suspicious to you and also do not add everyone to your friend lists after verifying them surely because attacker can fake represent himself.
5. **Follow right path:** If you found some links, applications or users which are harmful for your personal data, so inform your social circle about them.
6. **Update your password:** It is a key path for protecting our accounts. Do not use same password for all your accounts because one time attackers got them they can easily access to all of your accounts, so use different password for different accounts and used complex password. Update your passwords after a specific time that will be hard for attacker to guess them.
7. **Verifying information:** SNS provide platform for sharing thoughts, interest and activities also many users used them for gaining knowledge and updates but information provided by SNS are not surely to be correct, so do not believe on information provided by SNS without verifying them.
8. **Be conscious of wifi at public area:** Mostly user's access SNS through mobile phone and use single access sign in for all accounts, the concern cons over here, if hacker accesses his password they can access his all accounts financial, banking and credit card detail easily. So, don't trust on WIFI at public area such as hotels, restaurant, hospitals etc because some SNS used insecure data layer which capture the log in detail such as user name/password and also the rest of user communication through snipping tools.
9. **Awareness at institutional basis:** Teen agers have high ratio of using SNS. They do not aware from privacy of SNS that how to implement them, additionally they do not know the risks of information revelation. So, by arranging "Precaution tips of SNS" at institutional basis can limit attacks on younger's by providing them full guidance.
10. **Utilize two-factor validation:** Add second factor authentication with user name and password as in the form of Capcha code, voice ID, face recognition, iris recognition, finger scanning etc.
11. **Mark "automatic updates" your operating system:** Keeping update your operating system is key step for keep yourself safer. Turn on "Automatic Update" on your

operating system if you have not done so. Latest version of operating system will be more careful about security.

12. **Keep update your anti-virus:** Install updatable version of antivirus as, attacker try to use new viruses to attack, so old versions of antivirus are unable to block new viruses.
13. **Revolving of posts:** Mostly posts of SNS revolved on OSN, if any user posts something on his wall everyone can share his post without to compromise him. But some post have no need to stay more on SNS and user share them again and again that cause some problems for example, once upon a time a little boy named Asad lived in swat was disappear from his family, the message about him was posted on face book. After some days someone found him and returned him to his family, but the post still revolved on SNS. After that many times, when someone found him by going school, shop, etc he took him to his house. So be careful while sharing that types of content.
14. **Keep your software up to date:** Be aware of your software specifically your browser up to date as attackers known the vulnerabilities of existing version. Enable mark "Automatic Update" option, if available.
15. **Be careful while comments:** Commonly conversation takes place over posts which may lead to several threats. Manipulation of ideology on post result, as people said Face book is the way for falling kingdom and twitter can cause to change GOVT faster. Additionally some of secret revealed about secret events through comments.
16. **Enhancing the current legislation:** Current legislation is not enough to defense new fraud and attacks so modify legislation according to advance fraud and attacks that will hard for attackers to broke them.
17. **Build an online status:** Be careful while posting something because it represents your personality and behavior that are the keys for your future trends. As researchers concluded that, 70% of recruiters lose their jobs after employer visiting him online. Represent yourself thoughtful and creative mind.
18. **Logout your account:** If you did not want surfing SNS more so logout from your account, as your account is logged in and you are not visiting SNS attackers can hijack your session and also can infiltrating your account. Delete your cookies while logging out form your account.
19. **Do not post about journey:** Do not post something about your journey plan i.e. date, time, place and to whom you visit. These kinds of information lead to home robbery and others physical threats.
20. **Do Not Follow Shortened URLS:** Mostly attackers used shortened URLs for malware spreading which disturb our personal computer and also can extract our personal information. So do not follow any shortened URLs although it provides by your friends don't trust on anyone just verify.
21. **Do not trust on OSN:** Mostly users are willing to OSN privacy, they think that these networks have free of risks. A survey conducted in 2015 which consists 200 OSN users as samples concluded that, most users feel safe while sharing contents [20]. So it's very crucial for OSN users to be aware himself from OSN privacy risks.
22. **Be careful while posting:** Anything that post user remain forever so be careful while posting something, if someone post sensitive/private picture/data accidently and they directly delete the posted content, the post will be removed from his wall but SNS operators and external web archive automatically accept the copy of post, which is harmful for users.

4 Conclusion

Online social networking sites make communication much easier than traditional methods. Online Social Networks are hybrid platform by mean of, they can used for voice calling, video calling, text messages, multimedia messages, news posting, etc. Due to its functionality it's becoming more popular and increases its users day by day. Popularity of Online Social Networks attracts attackers. Existing legislation of social networking sites are unable to protect user profile information. In our proposed work we have categorized common attacks on Online Social Networking sites and hole in privacy. At last we suggest some solution to improve privacy and security of Online Social Networking Sites. Still there is a lot of research work required to improve privacy and security of Online Social Networks.

5. References

1. Khan F, ur Rehman A, Usman M, Tan Z, Puthal D. Performance of Cognitive Radio Sensor Networks Using Hybrid Automatic Repeat ReQuest: Stop-and-Wait. Mobile Networks and Applications, 2018, 1-10. https://doi.org/10.1007/s11036-018-1020-4
2. Alam M, Trapps P, Mumtaz S, Rodriguez J. Context-aware cooperative testbed for energy analysis in beyond 4G networks. Telecommunication Systems, 2016, doi:10.1007/s11235-016-0171-5
3. Khan F, Rahman F, Khan S, Kamal SA. Performance Analysis of Transport Protocols for Multimedia Traffic over Mobile Wi-Max Network Under Nakagami Fading. In Information Technology-New Generations Springer, Cham, 2018, 101-110.
4. Alam M, Albano M, Radwan A, Rodriguez J. CANDi: context-aware node discovery for short-range cooperation. Transactions on Emerging Telecommunications Technologies. 2013; 26(5):861-875. doi:10.1002/ett.2763
5. Khan F, Nakagawa K. Comparative study of spectrum sensing techniques in cognitive radio networks. In Computer and Information Technology (WCCIT), 2013 World Congress on IEEE, 2013, 1-8.
6. Alam M, Mumtaz S, Saghezchi FB, Radwan A, Rodriguez J. Energy and Throughput Analysis of Reservation Protocols of Wi Media MAC. Journal of Green Engineering. 2013; 3(4):363-382. doi:10.13052/jge1904-4720.341
7. Khan F, Bashir F, Nakagawa K. Dual head clustering scheme in wireless sensor networks. In Emerging Technologies (ICET), International Conference on IEEE, 2012, 1-5.
8. Alam M, Yang D, Huq K, Saghezchi F, Mumtaz S, Rodriguez J. Towards 5G: Context Aware Resource Allocation for Energy Saving. Journal of Signal

Processing Systems. 2015; 83(2):279-291. doi:10.1007/s11265-015-1061
9. Khan F, Kamal SA, Arif F. Fairness improvement in long chain multihop wireless ad hoc networks. In 2013 International Conference on Connected Vehicles and Expo (ICCVE) IEEE, 2013, 556-561.
10. Jan MA, Nanda P, He X, Liu RP. PASCCC: Priority-based application-specific congestion control clustering protocol. Computer Networks. 2014; 74:92-102.
11. Khan F. Secure communication and routing architecture in wireless sensor networks. In 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE) 2014, 647-650. IEEE.
12. Jan MA, Nanda P, He X, Liu RP. A sybil attack detection scheme for a centralized clustering-based hierarchical network. In Trustcom/BigDataSE/ISPA, IEEEIEEE, 2015; 1:318-325.
13. Jabeen Q, Khan F, Khan S, Jan MA. Performance Improvement in Multihop Wireless Mobile Adhoc Networks. the Journal Applied, Environmental, and Biological Sciences (JAEBS). 2016; 6(4S):82-92.
14. Jan MA, Nanda P, He X, Tan Z, Liu RP. A robust authentication scheme for observing resources in the internet of things environment. In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 13th International Conference on. 2014; 205-211.
15. Jan M, Nanda P, Usman M, He X. PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience. 2017; 29(17).
16. Khattak MI, Edwards RM, Shafi M, Ahmed S, Shaikh R, Khan F. Wet Environmental Conditions Affecting Narrow Band On-Body Communication Channel for WBANs. Adhoc & Sensor Wireless Networks, 2018, 40.
17. Jan MA, Nanda P, He X, Liu RP. Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on IEEE, 2013, 1400-1407.
18. Khan F. Fairness and throughput improvement in multihop wireless ad hoc networks. In Electrical and Computer Engineering (CCECE), IEEE 27th Canadian Conference on). IEEE, 2014, 1-6.
19. Jan MA, Nanda P, He X, Liu RP. A Sybil attack detection scheme for a forest wildfire monitoring application. Future Generation Computer Systems. 2018; 80:613-626.
20. Khan F, Jan SR, Tahir M, Khan S. Applications, limitations, and improvements in visible light communication systems. In2015 International Conference on Connected Vehicles and Expo (ICCVE) IEEE, 2015, 259-262.
21. Jan MA, Nanda P, He X. Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In International Conference on Wired/Wireless Internet Communication (pp. 154-167). Springer, Berlin, Heidelberg.
22. Usman M, Jan MA, He X. Cryptography-based secure data storage and sharing using HEVC and public clouds. Information Sciences. 2017; 387:90-102.
23. Usman M, Jan MA, He X, Nanda P. Data sharing in secure multimedia wireless sensor networks. In Trustcom/BigDataSE/ISPA, IEEE). IEEE, 2016, 590-597.
24. Khan F, Khan M, Iqbal Z, ur Rahman I, Alam M. Secure and Safe Surveillance System Using Sensors Networks-Internet of Things. In International Conference on Future Intelligent Vehicular Technologies (pp. 167-174). Springer, Cham, 2016.
25. Usman M, Yang N, Jan MA, He X, Xu M, Lam KM. A joint framework for QoS and QoE for video transmission over wireless multimedia sensor networks. IEEE Transactions on Mobile Computing. 2018; 17(4):746-759.
26. Khan F, ur Rahman I, Khan M, Iqbal N, Alam M. CoAP-Based Request-Response Interaction Model for the Internet of Things. In International Conference on Future Intelligent Vehicular Technologies Springer, Cham. 2016, 146-156.
27. Fida N, Khan F, Jan MA, Khan Z. Performance Analysis of Vehicular Adhoc Network Using Different Highway Traffic Scenarios in Cloud Computing. In International Conference on Future Intelligent Vehicular Technologies Springer, Cham, 2016, 157-166.
28. Jan MA, Khan F, Alam M, Usman M. A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems, 2017.
29. Usman M, He X, Lam KK, Xu M, Chen J, Bokhari SMM, Jan MA. Error Concealment for Cloud-based and Scalable Video Coding of HD Videos. IEEE Transactions on Cloud Computing, 2017.
30. Yang N, Usman M, He X, Jan M A, Zhang L. Time-Frequency Filter Bank: A Simple Approach for Audio and Music Separation. IEEE Access. 2017; 5:27114-27125.
31. Usman M, Jan MA, He X, Alam M. Performance evaluation of High Definition video streaming over Mobile Ad Hoc Networks. Signal Processing. 2018; 148:303-313.
32. Jabeen Q, Khan F, Hayat MN, Khan H, Jan SR, Ullah F. A Survey: Embedded Systems Supporting By Different Operating Systems. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN, 2016, 2395-1990.
33. Tahir M, Khan F, Babar M, Arif F, Khan F. Framework for Better Reusability in Component Based Software Engineering. In the Journal of Applied Environmental and Biological Sciences (JAEBS). 2016; 6(4S):77-81.
34. Khan S, Babar M, Khan F, Arif F, Tahir M. Collaboration Methodology for Integrating Non-Functional Requirements in Architecture. In the Journal of Applied Environmental and Biological Sciences (JAEBS). 2016; 6(4S):63-67.
35. Usman M, Jan MA, He X, Nanda P. QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems, 2018.
36. Jan MA, Tan Z, He X, Ni W. Moving Towards Highly Reliable and Effective Sensor Networks, 2018.
37. Jan MA, Jan SRU, Alam M, Akhunzada A, Rahman IU.

A Comprehensive Analysis of Congestion Control Protocols in Wireless Sensor Networks. Mobile Networks and Applications, 2018, 1-13.

38. Alam M, Ferreira J, Mumtaz S, Jan MA, Rebelo R, Fonseca JA. Smart Cameras Are Making Our Beaches Safer: A 5G-Envisioned Distributed Architecture for Safe, Connected Coastal Areas. IEEE Vehicular Technology Magazine. 2017; 12(4):50-59.
39. Jan MA, Usman M, He X, Rehman AU. SAMS: A Seamless and Authorized Multimedia Streaming frame work for WMSN-based IoMT. IEEE Internet of Things Journal, 2018, doi: 10.1109/JIOT.2018.2848284
40. Jan MA, Jan SR, Usman M, Alam M. State-of-the-Art Congestion Control Protocols in WSN: A Survey, IoT, 2018, EAI, DOI: 10.4108/eai.26-3-2018.154379