Comparative Study of Various Social Network Attacks: Comprehensive Survey

Zainab Khalid[1], Muhammad Sheraz Arshad Malik[2], Muhammad Usman[3], Mahwish Abid[4], Ijaz Ali Shoukat[5]

Department of Computer Science, Riphah International University, Faisalabad Campus, Pakistan [1,3,4,5]
Department of Information Technology, Government College University Faisalabad, Pakistan[2]

Summary
In today's world, Social Network is very famous for connecting people with each other to communicate and share personal information. Users openly expose their personal information such as personal details, current location, home address, and media data such as photos, videos, email, and contact numbers. These exposed users information can be captured by hackers which can harm the user. Social Network face some security issues which exploits user's privacy and security. In this paper, we presents the overview of Social network attacks with their solutions to provide security protection to users. There are some social network attacks which hasn't been compared on basis of various parameters. We also presents a comparison of various social network attacks which has been done by using various parameters.

Keywords:
Social network, Confidentiality, Integrity, Privacy, Security, Hackers, Attackers, Social Networking sites, Social Media, Social Network attacks.

1. Introduction

In today's world, the social network is a way of communication between people through various social networking websites such as Google [1], Google+, Orkut [2], Facebook [3], Twitter [4], WhatsApp [5], Instagram [6], Yahoo [7], Gmail [8]. In Social networking websites the users post various types of data and information that can be easily accessible by the people in the global world [9]. Internet is the easiest way to linked and stay connected with people [10]. In the USA, 80% of people spent their more time on social network [11] [12]. The more usage of network allows the people to interconnect with each other. The people can also search out for new friends to enlarge their social circle. Data sharing task, the users can share their daily activities. To interact with other people in Social Network the users must need an Email address to create their personal profile. Once the user is activated via email id, they provided with the communication interface to interact with people.

Users make communities, groups and societies in Social networks of people where they can share their opinions, interests and various types of information. The huge usage of these services harms the users maliciously. The two-communication media are becoming more desirable for the billions of users which are Facebook and Twitter. These two communication media's associates' users created profiles to connect people with their family and friends [13]. Users give their personal data and information which can be saved in online network. Attackers can easily obtain personal information by means of social network attacks. The modern application which is commonly used by every person is Facebook, where the users make their Facebook profile and post their personal information and add their friends in the profile. The user can also accept unknown friend request, which means the users unintentionally disclose their personal information with strangers who can misuse the user information and harm the users in various ways [14].

In the earlier times, users suffer many cases related to social media cybersecurity. The famous American airline which is named as Delta Airline, becomes victim of hijacking of social media accounts, attackers spoil their reputation by posting annoying media contents [15]. In last year the private data and the payment information of customers of Delta Air Lines have been uncovered by cracking a data [16]. Also, the Delta Airline Facebook page got hacked by and compromised by unknown hackers [17] [18]. Users mostly expose their original identities on social networking sites. Users upload the images of the friends, upload image with friends, tag current location in an image which can increase a security and privacy risks [19]. The users who have awareness and knowledge about the privacy issues can set their security settings others can become victim of attackers. The attackers can also obtain information even if the account is secure [20].

The importance of performing survey research related to social network attacks is to gain knowledge about the possible attacks which can harm user's privacy, the users should be careful before uploading data in social networking websites. A huge number of users relate to each other via social networking websites and they are increasing every year. In Figure 2 Statistic reveals the number of global users in social media from 2010 to 2016 with estimation up until 2021. It is predicted that the users will be round about

Manuscript received December 5, 2018
Manuscript revised December 20, 2018

2.77 billion globally, up and about since 2.46 billion trendies 2017 [21].

2. Social Network Attacks

There are various social network attacks, which makes the users published data at risks. In my literature review, there are few attacks which have been chosen for review and survey to have a look on various social network attacks. For this, firstly there are several attacks which has been grouped in social networks. The groups are classified into five different categories namely Network Structural Attacks, Privacy Attacks, Social Media Attacks, Social Networking Sites Attacks and Modern Attacks. The subsection shows the categories of various attacks as shown in Figure 3.

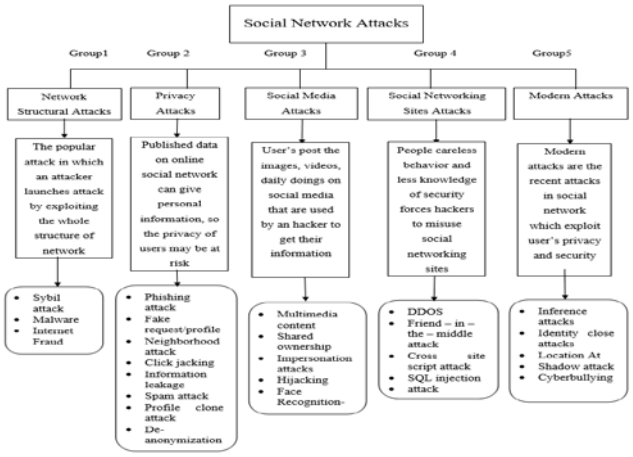

Fig. 1 Classification of Social Network Attacks

2.1 Network Structural Attacks

These types of attacks are responsible in such a way that an attacker can launches the attacks by exploiting the whole structure of network system of users. It describes the functional structure in between the largest network of any organization.

i. Sybil Attack

The adversaries take benefit of creating fake accounts in peer-to-peer and distributed network system in which the enormous number of users relate to each other for communication. The Sybil attack takes place in these network systems where one online group can control many fake identities at a time [13]. The user must be careful while registering for new account, the authentication step should be stronger [22]. Online websites of social network sites, like Facebook, Twitter that enables the attackers to insert the malwares in the user's profiles by creating multiple fake accounts. If the amount of attack edges exceeds, then they will escape from Sybil detection. To overcome from this type of situation, Sybil node identification (SNI) technique has been proposed [23] [24]. Sybil attack affects Internet of things (IOT) in which attackers create multiple fake identities. Researchers identified the 7.2% billion fake users in Facebook and 20 million in Twitter per week. They proposed Sybil defense protocols such as Sybil Limit, Sybil Guard, Sybil Infer, Sybil Defender, Sybil Shield, and Symon to protect against the Sybil attack [25]. The attackers can disturb the reputation of users by exploiting the honest relationships between users and by creating a massive quantity of false personalities [26].

ii. Malware Attack

Malicious attack is a vulnerable attack which belongs to viruses such as Trojan horses and worms. Malware can transfer from one user computer to another easily. It is hard to determine about URL link whether it is vulnerable or not. It takes the user directly to the fake website. When the user clicks on the malicious URL, the attacker transfers the malware to user computer system automatically [13] [27]. The attackers make the Websites targetable and web users as a victim. The malware spread from one another and exploit the trust of users among their friends [28]. The attackers spread malicious software and worms in their email data content. The first Malware was Koobface which was not famous, and users was not familiar which run in social networking websites while browsing in internet browsers. This attack runs automatically when the user performs some tasks such as Login and activates account on Facebook by using Gmail account, join groups on Facebook, accepting friends request and add them in their profile, share anything on friend's wall [29].

iii. Internet Fraud Attack

Internet frauds happens if the user utilizes the internet services partially or entirely [30]. Mostly it is hard to detect the internet fraud because internet fraud comes in various ways such as in emails, links, communications and media [31]. The other name of Internet fraud is Cyber fraud. In the earlier time, the group meetings were arranged to maintain strong relation with each other with their victims [14]. The NASAA (North American Securities Administrators Association), Con artists exploit the social networks by arranging the special meetings to build strong connections via face to face communication. The attackers can access their victims via online profiles where they have uploaded their personal contents such as names, photos, personal media, contact numbers, home location, current location, date of births and their religion views [32]. The con artist takes benefit of users who upload their private information in their profiles.

2.2 Privacy Attacks

Users provide a large amount of personal information on their profiles, the network service providers collect and save this information and users upload their image and share their contact numbers, location, home address and post about their birth dates which can be risky for user's privacy.

iv. Phishing Attack

Attackers in the Phishing attack use fake websites to attain the user's personal information. In this attack, they create a same duplicate of an original social networking websites. They gather the user's private information and then they send the fake emails. When the social network users receive such demanding emails they give the required information to the attacker [13] [33]. A phishing scam spreads about Facebook, the users get messages from their friends to click on the following link but in actual that login page consists of different link which is http://fbaction.net. This link was rapidly jammed and for now there appears to be the new one link which is http://fbstarter.com/ [33]. User's fake friends send this link in the form of message with tittle of "See this" or "Look at this". When the user clicks the URL link, he redirected to the Facebook sign-in page.

v. Fake Request/Profile Attack

Fake profiles are also stated as Sybil's that copy the user behaviors and generate the user's personal data. The attackers send the fake friend request among the users. Though the user accept friend request then the attackers can easily get into their personal information [14]. The market of purchasing fake twitter, retweets and fake followers are doing a multimillion-dollar business today in which they used to sell fake Twitter accounts [34] [35]. If the user having no profile in social networking website, then this is a risk in the network. The risk is because the attacker take benefit of creating fake profile of the person having no account. The researchers provide a framework where the Fake Profile attack detect in a social network when victim has no exiting profile account. [36].

vi. Neighborhood Attack

If the adversary has information about the victim's neighbor and relationship between them, then the victim may be recognized again in a social network. The victim may be re-identified if the identity of the user is secured by using the techniques of anonymization [10]. If the user anonymized the data which is to be published in social network, the attackers get successful in re-identifying the user victim identity by using some background information. The paper prosed one-neighborhood adjacency matrix which is established by procedure of anonymization [37]. Social networks are used to characterize by the social graph [38].

vii. Clickjacking Attack

The attackers hide the malicious information behind the user's platform; also they hide behind the clicking button to capture the information of clicks to utilize them for their own benefits. The most prominent is Cursorjacking and Likejacking. Clickjacking working is to trick a user by clicking something without any intention. For instance, the user clicks by thinking that he is clicking on the button of play again to play the YouTube video, but in actual he clicks on the unseen malicious button. It posts the link to the users Facebook home page which can be seen by everyone and users thinks that his friend posted and shared the video link and clicks the link to see the video by trusting his friends. But in real it was posted by attacker. The more users avoid to clicks on the unknown links, the more slowly clickjacking malware spreads [39].

viii. Information Leakage

Information leakage in which the personal information may be disclosed accidentally which may include account identifiers, email addresses, the structure of file system, data base structure, application configuration and so on. The given information can break security of users [40]. Users openly share education, health, and politics. The users can also register themselves for jobs. Additionally, the information of drinking habit can also be leaked [14]. It is necessary to update their information in some cases, such as to participate in social communities, to register themselves for any job purposes which invite malicious attackers. Three ways of prevention which are to provide the private privacy settings (in which the users should hide personal data, their connections with friends, media that modified the settings of browsing scope, requirement of owner's confirmation to reveal private information [41].

ix. Spam Attack

Spammers are the attackers who apply the electronic messaging system to the users to send undesirable messages such as to do advertisement of company by using social networking applications like Facebook, Instagram, and Gmail. Twitter suffered a large amount of spam messages [14]. Cybercriminals take full advantage of users exposed data and attain their information [42]. According to the security report, the most highlighting victim is Facebook [43]. Mostly spammers use the email platform because of the social relationships between the users in social networks. The attackers think that it's quite easy to convince the victim user to open the email to read the content which consists of fake data. In this way attackers can steal information of victim user easily and spread the Spam messages to the YouTube and Facebook social networking websites [13] [44].

x. Profile-Clone Attack

Attackers copy the profiles of user which exists already in social networking sites. The attackers take benefit from this cloned profile by sending fake request. The attack also commits various type of attacks for example cyber stalking, blackmailing [13]. When someone tries to clone your profile, the Facebook gives notification. When the real user notices the fake profile of them, they report it to the Facebook help center [45]. Profile cloning exists in two types such as already existing profile and cross sites profile cloning the attacker can steal the information of a user's profile from the one social networking website and then uses the profile account in some other social networking site [46].

xi. De-anonymization Attack

In the websites of social networking like Facebook, Twitter, LinkedIn and Myspace, most of the users can secure their privacy by using unique names i.e. pseudonyms. De-anonymization attack applies some techniques which are to track cookies, the paths of network and use the membership of group to disclose the real identity of user [14]. One more de-anonymization technique is used which is Personally Identifiable Information technique [47]. The de-anonymization attack is to disclose the information of group membership [48]. To take benefit from this social network, users create many accounts using personal information either same or different. They introduced a method of Entity Resolution (ER), which uses to recognize the two accounts on different social network platform by using machine learning techniques [49].

2.3 Social Media Attacks

The social media attacks are responsible to steal the privacy of users and their identities to disturb and threaten them in their social network. User's post the images, videos, daily activities on social media that can be used by a hacker to get their information.

xii. Multimedia Content Attack

Users share their personal data such as their name information, photos, videos, daily activities, home and current location. The uploading of multimedia content can increase chances of illegal usage of user data. When a user uploads the status which shows that he is not at home which indicates that home is open for an attacker. Along with this, when user share photo, it contains photo images of other people too. Face recognition technology can recognize the faces of users which may disturbs their privacy. The information of user can be easily stolen by the uploading data information, so the user must be caution about uploading data [13] [50].

xiii. Shared Ownership

If a user captures a photo and one of them upload that photo image on social media by setting his or her privacy, this step might disclose the privacy of his or her friend also the privacy of multiple users. Users can also upload a various amount of data. The need is to control the uploaded data in Web based social network (WBSN), the data which is upload by the user or by his linked user. Data management in Web Based Social network is important. Users become co-owners of other users who are owners where they are exposed to the unknown people. Risks arrives in this situation. Researchers introduced the method of co-ownership data management where the co-owner users can manage the data which is associated with them [51].

xiv. Impersonation Attack

The attackers aim is to create a fake identity for users regarding take someone's real identity which are faced by users when they are registering to create a new account. The attacker does so to get information of victim user such as financial data. The most common example of impersonation attack is CEO Fraud (Chief Executive Officer) or BEC (Business Email Compromise). The social media information data such as Name, contact number, email address, education, job, office, job duties, home address, location, etc. can be easily accessible by the attacker. It may be victims' owner, his colleague member, or his close friend. The victim can be friend on Facebook, which is very trusty because they consider that they are communicating with close friends. So, the attacker can easily figure out the person or user to impersonate [52].

xv. Hijacking Attack

The attacker takes full control of user's communication. An example of airplane, where the hijacker takes control of a flight and masquerade himself and establish connection between two entities [53]. If the attacker gets successful in cracking password of the user account, then they can hijack the account [54]. Session Hijacking Attack in which the attacker target to exploit the computer system session to get information of user's computer data [55]. In the Cookie Hijacking the attacker exploit the computer session. This cookie used to establish a temporary session which can be easily taken by a malicious attacker [56]. The attacker tries to capture the Hyper Text Transport Protocol (HTTP) headers. These headers contain the session cookies, the attacker copy the HTTP session to attain the retrieval of targeted people account to get private data and info of users [38].

xvi. Face-Recognition Attack

Almost 1.2 billion Facebook users are viewed and captured by many internet users [57]. Mostly the users Facebook account display picture settings are set to public which can be seen or saved by every user even if the user is not added in the Facebook profile which can be used for creating biometric database to recognize and identify users without their permission and knowledge [14]. In social network the researchers perform three experiments related to facial recognition. The first experiment is to recognize the face "Online to Online" system users, the second experiment is "Offline to Online". The third experiment combines the first and second experiment [58]. The attacker can gain access to user images impersonate a real user such as printed image, displayed video or images, 3D mask, sketch, reverse face image, plastic surgery, wearing jewelry makeup, fake image or video created by computer graphics [59].

2.4 Social Networking sites Attacks

People careless behavior and less knowledge of security forces hackers to misuse the social networking sites. They can gain and access user's information by attacking the networking sites and misuse the information and data for their own benefits.

xvii. DDOS

DDOS represents as Distributed Denial of Service in which the attacker sends a large quantity of request for the web resource while the web resource might become unreachable to users [60]. The harmful code quickly spread into the visitor's computer system. The online social networking users could be attacked by using two ways, one is directly on the Computer system or websites and other is by using some specific applications which users download on their mobile and computer system. The most general technique of attack is Distributed Denial of Service as DDOS [61]. The attacker makes one DDOS master computer by misusing the vulnerability in the user's computer system [62]. All zombie's computer system sends connection request to the most innocent system. When the computer system that is reflector accepts the connection request, it sends the information to the system of victim user. The increase in traffic can slow down the user's system performance which can turn off the website completely for users [63]

xviii. Friend-in-the-Middle Attack

The attack which can be used to steal the link of communication by taking over the temporary session cookies which exists between people and network providers [60]. By stealing the sites cookies among users and network suppliers, it becomes quite easy to impersonate the. It can gather user's personal information from various sites [64]. In the Man-in-the-middle attack, the attacker interferes itself in a communication between two users and copies the both users. The attacker inserted himself in the traffic flow between server and client user [65]. Man-in-the-middle attack in which the attacker used to impersonate the communication of both sides.. The attacker catches the public keys of both users, which is the proof of secure communication with each other. In this way the attacker can obtain the personal and confidential information of both users.

xix. Cross Site Scripting Attack (XSS)

Attackers used to insert malicious code into web applications. It doesn't attack directly into the web application. Cross site scripting attacks can be classified into two types which are stored and reflected XSS. The Client-Side code is a JavaScript code which runs on the victim users' system when a user loads a web browser. Specifically, this attack mostly hits the well-known websites such as Facebook, YouTube & Twitter [66]. Cross-Site Script is a virus and worm in social networking websites which highly depends on the three major factors which are user behaviors, the large collection structure of various groups and communities and the sizes of such communities. The attack of XSS exploits the already existing vulnerabilities in the websites applications to spread and broadcast itself [67].

xx. SQL Injection Attack

SQLi (SQL Injection) where an attacker can insert and executes SQL malicious codes that can take control of web applications database server which are also known as RDMS. Attackers can gain illegal access to users' personal data which includes customer data and other confidential information [68] In various types of web applications, the input data can be taken from the users where the SQL query statements executes to fetch the data in the database [69]. If the user needs the book which can be authored by some author, the user obviously searches the book from the name of author. The attacker breaks down the security by inserting malicious query codes in the website application database. They can delete or alter the database in order to steal user's sensitive information. These are known as SQL injection attacks [70] [71].

2.5 Modern Attacks

Modern attacks target user's information to get them to steal their privacy and security. Modern attacks are the recent attacks in social network which exploit user's friend and family trusty relationships.

xxi. Inference Attack

This type of attack happens when the user can infer the sensitive information of user indirectly from the given information [72]. Attacker can use user's social network accounts to reveals the private information of users [13]. Attackers can infer the information from the given profile information. Moreover, they can collection some more information by querying from the user's educational institute i.e. from Student Directory or Institute Alumni Directory, the attacker may be able to take out the other information such as matriculation and graduation year, courses and department [73] [74]. Another study proposed how to launch inference attack by using the release data on social networking to gain personal information. They introduce sanitization methods to prevent users from inference attack [75].

xxii. Identity Clone Attack

The type of attack that can be used to deceive users and their friends to replicate the people identity also in same network or in altered social network by making the relation of trust to attain control to their personal data. The famous NATO's senior commander whose name was Adml James Stavridis of the Washington, His identity was cloned by his colleagues using fake Facebook account by his name to gather data on defense ministry officials [76]. The profile clone attack is the subgroup of automated identity theft [77]. The modern attack which is most generally used in social network to exploit the security and privacy of user is known as Identity Clone Attack [78].

xxiii. Location Attack

The usage of mobile devices has been increasing which forces user to share their location information publicly [79]. The framework was presented to identify the user's location on the base of city level which users' tweets on Twitter account [80]. The new website introduces named as PleaseRobMe.com which may put the user into risks [81] [82]. Sharing the personal information on Twitter can be risky for users. For instance, in June 2009 the Israel Hyman tweeted in his account that he was arriving with his family for vacations where they stay for one week. He moved to Missouri and tweeted again. When they returned to them, they found their home broken and many dollars of computer equipment were stolen. Hyman said that they don't know how this happened for what reasons, but later he thinks that they were broadcasting about their location on the internet [83]. Consider an example of Apple's iPhone 3G if the user turns off the location in the global settings, then the photo taken from camera would not be tagged in location. The user must be aware of and careful of their privacy settings on mobile phones [84].

xxiv. Shadow Attack

In social network the user's login multiple account by registering themselves in same website or across multiple sites. Some users may apply same passwords for multiple account. Due to this an attacker can easily makes guesses of passwords for the user's same account. An analysis performed in which there are 70 million website passwords for four largest websites in China. There are 4.8 million people with the numerous profile accounts on different websites. The users with numerous accounts with changed keywords, can fixed a pattern for passwords which can help an attacker to guess the password which leads to passwords leakage and reveals the personal information of users [85].

xxv. Cyberbullying Attack

The aim of Cyberbullying is to share, send, and update or post some negative about anyone which can cause embarrassment for people. Cyberbullying takes place are Electronic Mail, Text Message service send via devices, Social networking websites (Facebook, Twitter, Instagram and Snapchat), Instant Messages through mobile devices and computer system [86]. Cyberbullying is also known as online bullying which is becoming common among teenagers and young youth rather than adults. The aim is to harass the people on social media and network sites online [87] [88]. In most cases the cyberbullies shows results of death and commit suicide. Let's consider a scenario of Florida Girl named Rebecca Ann Sedwick, whose age was only 12 years old, she found dead after bullies said her 'Why are you still alive?"' 'Kill yourself' [89]. The cyberbullied like to use drugs or alcoholic, skip their schools and perform poorly, feel their self-esteem lower and poorer health [90].

3. Solutions

In this section, we provide the corresponding attacks solution. The solutions provide the users with security, privacy and trustworthy conversation in the social network. Table 1 provides the representation of Attacks & Solutions whereas table 3 provides Solutions against each attack.

Table 1: Representation of Attacks & Solutions

Symbols	Attacks	Symbols	Solutions
T1	Sybil	S1	Watermarking
T2	Malware	S2:	Steganalysis
T3	Internet Fraud	S3:	Digital Oblivion
T4	Phishing	S4:	Storage Encryption
T5	Fake Request	S5	Fake Profile Detection
T6	Neighborhood	S6	Authentication Mechanisms
T7	Clickjacking	S7	Security & Privacy Settings
T8	Information Leakage	S8	Socware Detection
T9	Spam	S9	Internal Protection Mechanisms
T10	Profile Clone	S10	Preventing location leakage
T11	De-anonymization	S11	Report Users
T12	Multimedia Content	S12	Internet Security Solutions
T13	Shared Ownership	S13	Sybil Defense
T14	Impersonation	S14	AVG Privacy Fix
T15	Hijacking	S15	Spammer Detection
T16	Face Recognition	S16	Defensio
T17	DDOS	S17	Co-ownership
T18	FITM	S18	Malware Detection
T19	(XSS)	S19	Fb Phishing Protector
T20	Infiltration	S20	Social Guard Privacy Scan
T21	SQL Injection	S21	McAfee Social Protection
T22	Socio-technical	S22	NoScript Security Suite
T23	Inference	S23	My Permissions
T24	Couplet	S24	ZoneAlarm Privacy Scan
T25	Identity Clone	S25	Privacy Scanner for Facebook
T26	Location	S26	Minor Monitor
T27	Shadow	S27	Web Security Software
T28	Cyberbullying	S28	Social Protection Application
		S29	Net Nanny
		S30	Profile Clone Detection
		S31	Phishing Detection
		S32	Metadata removal
		S33	Nortan Safe Web

4. Comparison

In table 2, “Environment of attack” represents the Nature of each attack. “User Privacy threat” involves the rights of personal privacy of user to prevent their data from attackers. “Usage %” represents the consumption of each attack in percentage values. “Impact Level” based on the user’s amount of private loss such as loss of personal data and reputation loss. “Server Security Efficiency” and “User Security Efficiency” defines the security of Server and User efficiency when any attack occurs. “Data Integrity threat” describes whether the attacks changes or modifies the user data or not. “Data Confidentiality threat” states that the user information has been protected or not from being accessed by unauthorized users. The type of attacks and their impact factors on users has been described.

Table 2: Comparison of Social Network attacks

Attacks	Environment of attack	User Privacy threat	Usage%	Impact Level	Server Security Efficiency	User Security Efficiency	Data Integrity	Data Secrecy threat	Impact Factor
Sybil	Computerized	☑	56%	High	Strong	Poor	☑	☑	defeat users, reputation loss
Malware	Computerized	☑	50%	Medium	Medium	Medium	☑	☑	Info disclosure, account loss
Internet Fraud	Physical	☑	51%	Medium	Poor	Poor	☑	☑	Data disclosure, Info leak
Phishing	Computerized	☑	57%	Average	Poor	Strong	☑	☑	Account loss, cyberstalking
Fake Request	Computerized	×	41%	Medium to High	Medium	Strong	×	☑	Cyber harassment, reputation loss
Neighborhood	Physical	☑	42%	High	Strong	Limited	×	☑	Relationship disclose, Safety loss
Clickjacking	Computerized	☑	39%	Medium	Medium	Low	☑	☑	Click stolen, lack user experience
Information Leakage	Physical	☑	79%	High	Limited	Poor	×	☑	Blackmailing, information disclose
Spam	Computerized	×	48%	Low	Strong	Medium	☑	×	Reputation loss, Account loss
Profile Clone	Physical	×	51%	Medium	Poor	Poor	☑	☑	Cyberbullying, Cyberstalking
De-anonymization	Physical	☑	42%	Low to High	Medium	Strong	×	☑	Identity Disclosure, profiling
Multimedia Content	Physical	☑	83%	High	Poor	Strong	×	☑	Location leakage, profiling
Shared Ownership	Physical	☑	53%	Medium	Poor	Strong	☑	☑	Content ownership loss
Impersonation Attack	Computerized	☑	37%	High	Poor	Poor	×	☑	Identity disclose, data ownership
Hijacking	Computerized	☑	33%	High	Poor	Poor	×	☑	Blackmailing, Identity disclosure
Face Recognition	Computerized	☑	44%	Average to High	Medium	Medium	☑	☑	Multimedia data disclosure
DDOS	Computerized	×	49%	High	Limited	Medium	☑	☑	User disturbance, corrupt user info
FITM	Computerized	☑	32%	Low	Poor	Low	☑	☑	Safety loss, data disclosure
XSS	Computerized	×	35%	Medium	Medium	Poor	☑	☑	Lack of trust, info loss
Infiltration	Physical	☑	44%	Medium to High	Strong	Medium	☑	☑	Affect company profiling
SQL Injection	Physical	☑	43%	High	Poor	Limited	×	☑	Data integrity, repo loss
Socio-technical	Physical	☑	40%	Medium	Limited	Poor	×	☑	Blackmailing, Info leakage
Inference	Physical	☑	57%	Medium	Medium	Strong	☑	☑	Relationship disclosure
Couplet	Physical	×	31%	Low	Medium	Medium	×	×	Identity and reputation disclose

5. Conclusion

Social network has become essential part of our daily life. The usage of social network can also be risky for users. In this paper, various social network attacks has been discussed which can affect user security and privacy which has been classified in groups. Along with these attacks, their solutions are also provided to protect against such attacks. The data has been collected by using survey methodology which has been formulated by using questionnaire. The main aim is to collect respondent's observations against the social network attacks. Hypothesis has been developed to identify the objectives of research and to see the relationship between problem statement and literature review. Test has been applied by using SPSS on these attacks to get the results against the developed hypothesis. The tests includes Reliability test using Cronbach alpha, Chi-square test of independence, t-test, person's correlation. The paper proposed a comprehensive review on the social network attacks with their appropriate solutions and provides the comparison between these attacks on the basis of certain parameters.

6. Future Research Directions

To improve more security and privacy of users, the need is to find more recent attacks which are applying currently in social network, also improve the existing solutions to create more effective security solutions against each type of attacks. By combing all these new algorithms and techniques, it can provide with better and compatible solutions against social network attacks. Users must avoid to post their sensitive and personal information on social media directly and try to make less accounts on social network to protect themselves from attacks. Moreover the future direction includes that users must study the reasons of these attacks, and protects them accordingly.

References

[1] L. Page and S. Brin, "Google," 1997. [Online]. Available: https://www.google.com.pk/. [Accessed 2018].

[2] "Orkut," Google, 2008. [Online]. Available: http://www.orkut.com/index.html. [Accessed 2018].

[3] E. Z. Mark, "Facebook," 2004. [Online]. Available: https://www.facebook.com/. [Accessed 2018].

[4] J. Dorsey, N. Glass, B. Stone and E. Williams, "Twitter," 2006. [Online]. Available: https://twitter.com. [Accessed 2018].

[5] J. Koum, "WhatsApp," 2009. [Online]. Available: www.whatsapp.com. [Accessed 2018].

[6] K. Y. Systrom and M. M. Kreiger, "Instagram," 2010. [Online]. Available: www.Instagram.com. [Accessed 2018].

[7] [7] J. Yang and D. Filo, "Yahoo," 1994. [Online]. Available: https://www.yahoo.com/. [Accessed 2018].

[8] P. Buchheit, "Gmail," 2001. [Online]. Available: www.gmail.com. [Accessed 2018].

[9] A. Viejo, G. Rufian and J. . C. Roca, "Preserving the User's Privacy in Social Networking Sites," Springer, p. 62–73, 2013.

[10] P. Joshi and . J. Kuo , "Security and Privacy in Online Social Network," IEEE, 2011.

[11] B. Mei, Y. Xiao, . R. Li, H. Li, . X. Cheng and Y. Sun, "Image and Attribute Based Convolutional Neural Network Inference Attacks in Social Networks," IEEE, 2018.
[12] "THE RISE OF SOCIAL MEDIA ADVERTISING PROMINENCE," 2016. [Online]. Available: http://www.adcheck.co.za/the-rise-of-social-media-advertising-prominence/. [Accessed 7 11 2018].
[13] S. Rathore , P. K. Sharma , V. Loia , Y. S. Jeong and J. H. Park, "Social network security: issues, challanges, threats and solutions," Elsevier, pp. 43-69, 2017.
[14] M. Fire, R. Goldschmidt and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE, vol. 11, 2013.
[15] K. and B. Young, "komando," 2015. [Online]. Available: https://www.komando.com/happening-now/449796/hacked-your-personal-data-exposed-by-delta-sears-and-more.
[16] "Money," [Online]. Available: https://money.cnn.com/2018/04/05/news/companies/sears-delta-data-breach/index.html.
[17] J. Fox, "Time," 2015. [Online]. Available: http://time.com/3703640/delta-airlines-facebook-page-got-hacked/.
[18] "businessinsider," 2015. [Online]. Available: http://www.businessinsider.com/delta-airlines-facebook-page-got-hacked--obscene-content-posted-2015-2.
[19] A. C. Squicciarin, H. Xu and X. Zhang, "CoPE:Enabling Collaborative Privacy Management in Online Social Networks," Journal of the American Society for Information Science and Technology, 2011.
[20] M. Joe and D. B. Ramakrishnan, "A Survey of Various Security Issues in Online Social Networks," International Journal of Computer Networks and Applications, vol. 1, no. 1, 2014.
[21] S. "Statista," 3 April 2017. [Online]. Available: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
[22] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," Elsevier, 2016.
[23] K. B. Kansara and N. M. Shekokar , "Security against sybil attack in social network," in International Conference On Information Communication And Embedded System(ICICES 2016), 2016.
[24] "Sybil Attack," [Online]. Available: https://www.searchenginegenie.com/101-articles/Sybil-attack.html. [Accessed 11 9 2018].
[25] D. Valarmathi , A. Meenakowshalya and A. Barathi, "Robust Sybil Attack Detection Mechanism For Social Networks," in International Conference on Advanced Computing and Communication Systems (lCACCS -2016), 2016.
[26] Z. Xu, B. Chen, X. Meng and L. Liu, "Towards Efficient Detection of Sybil Attacks in Location-based Social Networks," IEEE, 2017.
[27] M. Nauman, . N. Azam and J. Yao, "A Three-way Decision Making Approach to Malware Analysis Using Probabilistic Rough Sets," Elsevier, 2016.
[28] M. R. Faghani and H. Saidi , "Malware Propagation in Online Social Networks," 2009.
[29] H. Gu, J. Hu, T. Huang, J. Wang and Y. Chen, "Security Issues in Online Social Networks," IEEE, 2011.
[30] "Wikipedia," 2005. [Online]. Available: https://en.wikipedia.org/wiki/Internet_fraud.
[31] "Spam Laws," 2018. [Online]. Available: https://www.spamlaws.com/internet-fraud.html.
[32] "NASAA," 2011. [Online]. Available: http://www.nasaa.org/5568/informed-investor-advisory-social-networking/.
[33] "Techcrunch," 2018. [Online]. Available: https://techcrunch.com/2009/04/30/new-phishing-attack-spreading-on-facebook-this-time-from-fbstarter/.
[34] N. Perlroth, "Bits," 2017. [Online]. Available: https://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/. [Accessed April 2013].
[35] "Why you should beware fake Facebook profile," 2018. [Online]. Available: https://www.mywot.com/en/blog/why-you-should-beware-fake-facebook-profiles.
[36] M. Conti, R. Poovendran and M. Secchiero, "FakeBook: Detecting Fake Profiles in On-line Social Networks," in International Conference on Advances in Social Networks Analysis and Mining, 2012.
[37] A. K. Diwakar , N. K. Singh and D. S. Tomar , "End User Privacy Preservation in Social Networks Against Neighborhood Attack," IEEE, 2017.
[38] D. Gunatilaka, "A Survey of Privacy and Security Issues in Social Network," IEEE, 2011.
[39] M. . R. Faghani and U. T. Nguyen , "A Study of ClickJacking Worm Propagation in Online Social Networks," IEEE, 2014.
[40] "information leakage," [Online]. Available: https://affinity-it-security.com/what-is-information-leakage/.
[41] l. F. Lam, K. T. Chen and L. -J. Chen, "Involuntary Information Leakage in Social Network Services," 2018.
[42] M. Fire, G. Katz and Y. Elovici , "Strangers Intrusion Detection - Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies," vol. 1, no. 1, 2012.
[43] E. Barnett, "Technology News," 2011. [Online]. Available: https://www.telegraph.co.uk/technology/news/8267462/Spam-attacks-on-social-networks-rise-dramatically.html.
[44] "2013 State of Social Media Spam," 2013.
[45] R. Krishnan, "Facebook's latest feature Alerts You if Someone Impersonates Your Profile," 2016. [Online]. Available: https://thehackernews.com/2016/03/fake-facebook-account.html. [Accessed 2018].
[46] E. J. Ikhalia, "A New Social Media Security Model (SMSM)," International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 7, 2013.
[47] B. Krishnamurthy and C. E. Wills, "On the Leakage of Personally Identifiable Information Via Online Social Networks," 2009.
[48] G. Wondracek , T. Holz , E. Kirda and C. Kruegel , "APracticalAttacktoDe-AnonymizeSocialNetworkUsers," IEEE, 2010.
[49] O. Peled, M. Fire, L. Rokach and Y. Elovici, "Entity Matching in Online Social Networks," IEEE, 2013.
[50] M. Kandias, L. Mitrou, V. Stavrou and D. Gritzalis, "Which side are you on? A new Panopticon vs. privacy," in 2013 International Conference on Security and Cryptography (SECRYPT), 2015.
[51] L. G. Manzano, A. G. Tablas, J. Fuetness and A. Ribagorda, "CooPed: Co-owned Personal Data management," Elsevier, 2014.
[52] V. Cambazoglu, 2016. [Online]. Available: https://slideplayer.com/slide/4128699/. [Accessed 2018].

[53] M. Rouse, "Hijacking," [Online]. Available: https://searchsecurity.techtarget.com/definition/hijacking. [Accessed 2018].
[54] Z. Zhang and B. B. Dupta, "Social media security and trustworthiness: Overview and new direction," Elsevier, 2016.
[55] S. "Various types of network attacks," 27 Dec 2013. [Online]. Available: https://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks. [Accessed 2018].
[56] "Session Hijacking," [Online]. Available: https://en.wikipedia.org/wiki/Session_hijacking. [Accessed 2018].
[57] N. ROJAS, "Faces of Facebook," 2013. [Online]. Available: https://docubase.mit.edu/project/faces-of-facebook/. [Accessed 2018].
[58] A. Acquisti, R. Gross and F. Stutzman, "Faces of Facebook: Privacy in the age of Augmented Relaity," 2011.
[59] L. Li, . P. L. Correia and . A. Hadid, "Face recognition under spoofing attacks: countermeasures and research directions," IET(The Institution of Engineering and Technology), vol. 7, no. 1, pp. 3-14, 2017.
[60] A. Maurya and M. P. Singh, "A Survey on Social Networks: Issues and Attacks," 2015.
[61] X. Chen and K. MICHAEL, "Privacy Issues and Solutions in Social Network Sites," IEEE, 2012.
[62] M. Rouse, "distributed denial of service (DDoS) attack," 2017. [Online]. Available: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack. [Accessed 2018].
[63] J. Strickland, "Distributed Denial of Service Attacks," [Online]. Available: https://computer.howstuffworks.com/zombie-computer3.htm. [Accessed 2018].
[64] M. Huber, M. Mulazzani, . G. Kitzler, S. Goluch and E. Weippl, "Friend-in-the-middle Attacks: Exploiting Social Networking Sites for Spam," 2011.
[65] N. DuPaul, "MAN IN THE MIDDLE (MITM) ATTACK," [Online]. Available: https://www.veracode.com/security/man-middle-attack. [Accessed 2018].
[66] [66] "CROSS SITE SCRIPTING (XSS) ATTACKS," 2018. [Online]. Available: https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html. [Accessed August 2018].
[67] M. . R. Faghani and U. T. Nguyen, "A Study of XSS Worm Propagation and Detection Mechanisms in Online Social Networks," IEEE, vol. 8, no. 11, 2013.
[68] "SQL Injection (SQLi)," [Online]. Available: https://www.acunetix.com/websitesecurity/sql-injection/. [Accessed 2018].
[69] R. . M. Pandurang and D. D. Karia, "Impact Analysis of Preventing Cross Site Scripting and SQL Injection Attacks on Web Application," IEEE , 2015.
[70] T. author, "What is SQL Injection Attack ?," 2017. [Online]. Available: https://www.thesecuritybuddy.com/vulnerabilities/what-is-sql-injection-attack/. [Accessed 2018].
[71] S. Hoi, "Hacking And Protecting Websites From SQL Injection Attacks," 2017. [Online]. Available: https://www.sunnyhoi.com/hacking-protecting-websites-sql-injection-attacks/. [Accessed 2018].
[72] "Inference Attack," [Online]. Available: https://www.cybrary.it/glossary/i-the-glossary/inference-attack/. [Accessed August 2018].
[73] A. Mislove, B. Viswanath, K. P. Gummadi and . P. Druschel, "You Are Who You Know: Inferring User Profiles in Online Social Networks," in Third ACM international conference on Web search and data mining, New York, 2010.
[74] M. Fire and R. Puzis, "Organization Mining Using Online Social Networks," Springer, vol. 16, no. 2, pp. 545-578, 2016.
[75] R. Heatherly, M. Kantarcioglu and B. Thuraisingham, "Preventing Private Information Inference Attacks on Social Networks," IEEE, vol. 2, no. 8, 2013.
[76] J. Lewis, 10 March 2012. [Online]. Available: https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html. [Accessed 2018].
[77] D. Dave, N. Mishra and S. Sharma , "Detection Techniques of Clone Attack on Online Social Networks," in International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014.
[78] G. A. Kamhoua, N. Pissinou , S. S. Iyengar, . J. Beltran, C. Kamhoua and B. L. Hernandez, "Preventing Colluding Identity Clone Attacks in Online Social Networks," IEEE, 2017.
[79] L. Humphreys, "Mobile Social Networks and Social Practice: A Case Study of Dodgeball," Journal of Computer-Mediated Communication , 2009.
[80] Z. Cheng , J. Caverlee and K. Lee, "You Are Where You Tweet: A Content-Based Approach to Geo-locating Twitter Users," pp. 26-30, 2010.
[81] [Online]. Available: http://pleaserobme.com. [Accessed 2018].
[82] J. V. Grove, "Are We All Asking to Be Robbed?," 2010. [Online]. Available: https://mashable.com/2010/02/17/pleaserobme/#vcaP.tGNnqqz. [Accessed 2018].
[83] L. Humphreys, . P. Gill and B. Krishnamurthy , "How much is too much? Privacy issues on Twitter," 2015.
[84] G. Friedland and R. Sommer , "Cybercasing the Joint: On the Privacy Implications of Geo-Tagging," 2010.
[85] W. Han, Z. Li, M. Ni, G. Gu and W. Xu, "Shadow Attacks based on Password Reuses: A Quantitative Empirical Analysis," IEEE, vol. 10, no. 10, 2017.
[86] "What Is Cyberbullying?," [Online]. Available: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html. [Accessed 2018].
[87] "Cyberbullying," [Online]. Available: https://en.wikipedia.org/wiki/Cyberbullying. [Accessed August 2018].
[88] M. Dean, "The Story of Amanda Todd," 18 October 2012. [Online]. Available: https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd. [Accessed 2018].
[89] "Florida girl, 12, found dead after bullies said 'kill yourself'," 12 September 2013. [Online]. Available: http://articles.latimes.com/2013/sep/12/nation/la-na-nn-florida-cyberbullying-20130912. [Accessed August 2018].
[90] R. "Examples of Cyberbullying," 10 June 2014. [Online]. Available: https://blog.udemy.com/examples-of-cyberbullying/. [Accessed 2018].

Table 3: Social Network Attacks and Their Solutions