Cyber Security Concerns in Social Networking Service

Abdul Hamid[1], Monsur Alam[1], Hafsina Sheherin[1], and Al-Sakib Khan Pathan[2]

[1]Department of Computer Science and Engineering, Southeast University, Banani, Dhaka, Bangladesh
[2]Department of Computer Science and Engineering, Independent University, Bangladesh

***Abstract*:** Today's world is unimaginable without online social networks. Nowadays, millions of people connect with their friends and families by sharing their personal information with the help of different forms of social media. Sometimes, individuals face different types of issues while maintaining the multimedia contents like, audios, videos, photos because it is difficult to maintain the security and privacy of these multimedia contents uploaded on a daily basis. In fact, sometimes personal or sensitive information could get viral if that leaks out even unintentionally. Any leaked out content can be shared and made a topic of popular talk all over the world within few seconds with the help of the social networking sites. In the setting of Internet of Things (IoT) that would connect millions of devices, such contents could be shared from anywhere anytime. Considering such a setting, in this work, we investigate the key security and privacy concerns faced by individuals who use different social networking sites differently for different reasons. We also discuss the current state-of-the-art defense mechanisms that can bring somewhat long-term solutions to tackling these threats.

***Keywords*:** Cyber, Internet, Network, Security, Social, Threat.

1. Introduction

Social Networking Service (SNS) offers the online platform for creating friendship with various types of people who may share a common interest, background, or may be interested in creating a real relationship. The opportunity to make new friends and expand the friend circles was never easier before than what is seen today. Now, friendship can transcend national boundaries, all via online communications. Someone sitting at his desk or even lying on the bed can chat, video chat, share files and various types of information just by some clicking and tapping on the electronic handheld devices. The entire setting of IoT (Internet of Things) would facilitate the expansion of SNS even at a greater scale.

SNS offers its users the key feature of data sharing where the users are free to share their photos, videos, blogs, writings, files, etc. with each other. Among various SNS platforms, Facebook and Twitter have the most of the users today, as these got relatively more popularity in terms of ease of communication among the users. Throughout the recent years, billions of people all over the globe are using these platforms daily along with some other popular media applications like, WhatsApp, Viber, Imo, Skype, and so on.

To become the users of these services, people need to create their own profiles to stay connected with their dear ones. The users get the chance to verify their information and update anything whenever they feel changing is needed. They can browse other users' profiles as well whenever they want to and interact with each other according to their personal preferences. In fact, the geographical and economic borders can be minimized with the help of SNS. SNS fulfills the necessity of searching the fields like, entertainment, job, education, and so on. Even though, SNSs have quickly become popular and widely used around the globe, some mentionable threats remain in such platforms and they become frequent targets of the online attackers. It is a fact that often the attackers use the users' sensitive and personal information to reach certain goals and spread certain attacks like, social bots, spam, malware, identity theft, etc. They use such platform to do some phishing attacks [1] as well.

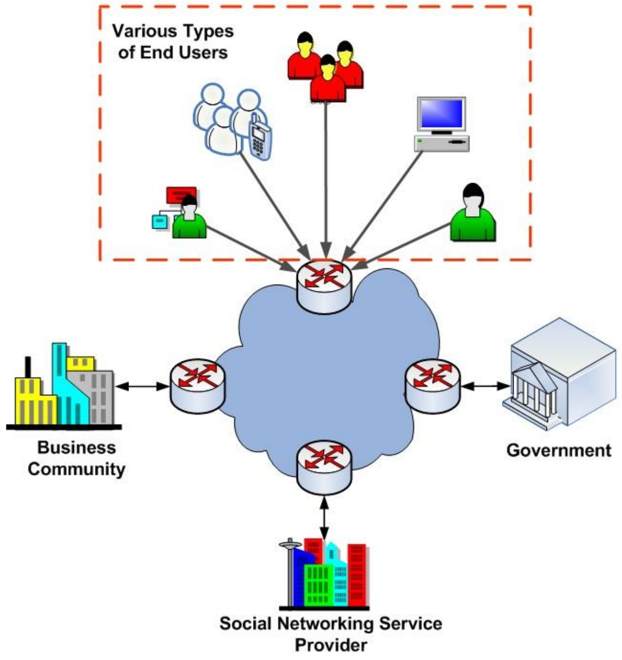

Figure 1. Various types of users using SNS.

Nowadays, often the attackers' main goal is to break into significant data storage like, national security system, official sites, bank account information, and so on, which would allow them to commit serious cyber crimes. SNSs could sometimes give the attackers the exploitable doors [2] to launch those cyber attacks. Raggo [3] analyzed various attacks in SNS that include impersonation attacks, malware distribution, account or ID hijacking, etc., and it shows that a well-planned attack can seriously jeopardize or destroy the targeted enterprise networks and create discord among the users. Various types of users of SNS are shown in the Figure 1.

Most of the SNSs are mainly used for producing and sharing multimedia data. If we check the most popular ones like Twitter or Facebook, the users use text to a great extent but images and videos or overall amount of multimedia data is also huge. ZDM (Zephoria Digital Marketing) [4] reported that in every 1 minute, 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded on Facebook. Statistical data by Ever Increasing Circles Ltd [5] shows the approximate and increased rate of videos shared and viewed on Facebook daily. If we see only the average number of views, then we get approximately 8 billion videos that are being viewed everyday only on Facebook, let alone YouTube and other media, which shows that it doubled up according to the record of 2015. That trend is still continuing and will continue in the coming years. Hence, security risk is higher than ever before because of the increasing number of uploaded multimedia data.

SNS allows the users to share multimedia contents and multimedia data allows a malicious user to share malicious information. Attackers are always in search for weak users so that they can use their personal information like, user's location or identity to reach their targeted motives. Though many SNSs (like for instance, Twitter) do not allow their users to reveal some sensitive information publicly to keep the users safe, some naïve decisions of the users could disclose their sensitive information on daily basis. That could fall in the hands of these wicked attackers who could somewhat analyze the sequenced uploaded contents. In fact, a user reveals many personal issues, choices, preferences, and so on when talking about personal life.

Attackers previously used Sammy worms in Myspace (2005) to exploit their vulnerability, Mikey worm in Twitter (April, 2009) to use people's information, and Koobface worm in Facebook (May, 2009) [6] to steal users' information. Myspace could deal with this threat quickly and could make it safe for the users. When the situation arose, though the personal information of the users was safe, its general operation was greatly affected. Twitter users' information was secured though that attack replaced some of the Twitter's data with some unimportant and unusable data. And again, Facebook was greatly damaged in that attack as many significant information of the users was stolen like, users' passwords.

Increasing number of hackers all over the world on a daily basis search information through SNSs, which is a serious issue which is stated in the Internet Security Threat Report [7]. Hackers use various malware or spam emails or advertisements as their web source to make money illegally with the help of SNSs. Many important people's accounts as well as many popular organizations have dealt with various hacking issues like even Mark Zuckerberg, CEO of Facebook - his Twitter and Pinterest accounts were hacked and the hacker also used his LinkedIn password, '*dadada*' [8]. Again, hackers succeeded to hack Newsweek and Delta Air Lines Inc.'s accounts and post fake messages [9]. It can be concluded after analyzing the accomplished attack series that attackers' most preferable way of making cyber crimes nowadays is through the SNSs.

Modern problems need modern solutions. The increasing number of typical threats along with the threats caused by the cyber criminals who use multimedia contents uploaded by individuals daily require some serious solutions and that is why, many security corporations and many researchers have come up with some interesting solutions to diminish these threats which include, Steganalysis [10], digital oblivion [11], and watermarking [12] that can protect the victims of the attacks and give them a safe field for sharing multimedia contents. And again, traditional online threats can be diminished with the help of phishing detector [1], [13] and spam detector [1], [14]. Privacy settings, authentication mechanisms [15] as security solutions and social protection application [16], Monitor Minor [17] as commercial solution can be built up to work actively against the security threats in SNS.

An elaborated analysis on the security concerns in this area is done in this work. The organization of the paper is as follows: Section 2 discusses some notable works done previously, Section 3 describes major threats and security concerns in SNS. Classification of security threats and concerns are presented in Section 4, Section 5 talks about some available security solutions, Section 6 discusses the key takeaway points and some general guidelines for the SNS users and finally, Section 7 concludes this paper.

2. Some Notable Works

A typical social media infrastructure (including supporting network) is shown in Figure 2. After studying the security issues of SNS, many researchers have come up with different ideas and mechanisms to tackle those threats and attacks. Gao et al. [18], in their work state that SNS's security issues can be categorized into four groups and they are: (a) Malware attacks, (b) Viral marketing, (c) Network structural-based attacks, and (d) Privacy issues. Corresponding defense mechanisms were included in their in-depth discussion. Novak et al. [19] do a survey showing the privacy issues and major security problems of SNS. Through this work, the existing techniques are introduced to the users to stay secure from various entities on-net like; SNS providers, advertisers, third-party application developers, etc. It also introduces the clear overview of SNS and discusses how location hubs, users' attributes, and link prediction make interference. Users' behaviors in SNS are studied by Jin et al. [20] which give us four viewpoints: (a) traffic activity, (b) interaction and connection, (c) malicious behavior, and (d) mobile social behavior. A review showing the existing schemes needed for SNS security, users' motivations, and major challenges faced by the users has been done here in this work.

Fire et al.'s [21] work presents a comprehensive survey on SNS's different security and privacy threats and categorizes these security threats into four groups, such as: (a) threats targeting children, (b) modern threats, (c) combined threats, and (d) classic threats. They add high standard taxonomy to stay protected from these threats. Again, Kayes et al. [22] elaborate this taxonomy further adding how the social network stakeholders can prevent these traditional privacy and security attacks. SNS related attacks can be basically of two major types: attacks on SNS users and attacks on SNS infrastructure. Hence, the authors add other existing defense mechanisms to work as the mitigation strategy against these attacks and show how these mechanisms can be challenging sometimes.

Deliri et al. [23] talk about the most common attacks in SNSs that include phishing, malware, identity theft attack, Sybil, and so on. Some other counter-measures are included in their study that can be helpful in diminishing these threats. Other studies have covered the traditional security threats faced by the SNS users, but not the multimedia sharing issues.

One of the previous works that motivated us to investigate this area is Rathore et al.'s work [24]. In that work, the authors systematically studied the issues, challenges, threats and solutions in this area. While that work forms the basis of this work, we extend the understanding with more data and most recent events and issues that could not be covered by that past work. New insights are included to guide the users with modern solutions and techniques as in this field, the solutions for problems change very frequently. Also, some old information has become somewhat irrelevant today.

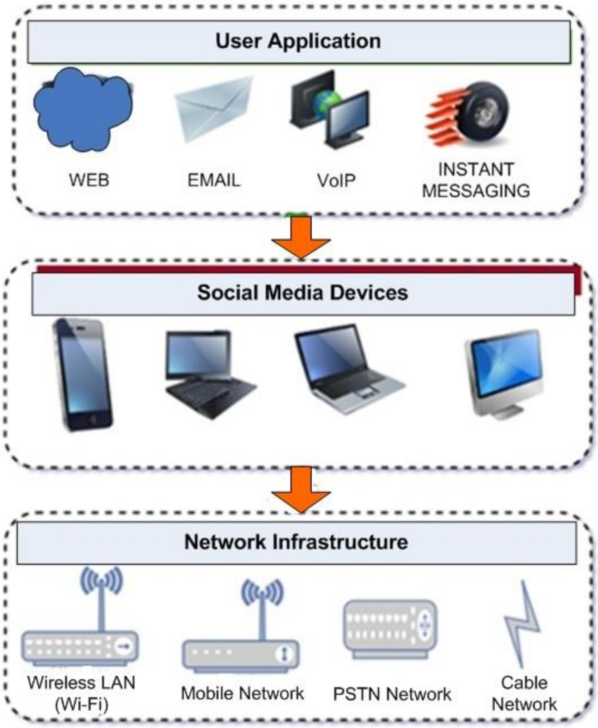

Figure 2. Network infrastructure of SNSs.

In this paper, we go through the traditional security threats as well as the threats that occur due to the sharing of the multimedia contents in SNSs. We also study the possible solutions that can mitigate these threats successfully. We discuss all the recent security solutions with high-level taxonomy. Our work concentrates on some significant attacks, the extended closer overview of the recent security threats in SNS, and also the targeted major and minor organizations. The major goal of our study is to achieve an efficient, secure and trust-worthy SNS platform. While previous works have done good job in identifying the issues, we like to extend the overall understanding to develop a feasible solution or at least to make some practical recommendations. The basic SNS perspective and concepts provide us the elaborated knowledge of the threats connected with them. Hence, this study is done to discuss the challenges and open issues of SNS that can come up with other related opportunities to overcome the problems and enhance the functional security of SNS.

3. Major Threats and Security Concerns in SNS

SNS has become the most favorite communication medium within the last decade. Every year, the quantity of SNS end-users globally is growing steadily. Statista's report [25] has shown projections for the quantity of SNS users worldwide from 2010 to 2019 with prediction until 2021 as shown in Figure 3. While the growth is encouraging as it seems the users are getting easy and cozy in using the Internet infrastructure to connect with anybody anywhere in the globe, this staggering growth also has given tremendous rise to various kinds of security vulnerabilities that have serious impact on the confidentiality, quality, and privacy of the end-users.

The Kaspersky Security Network (KSN) [26] has painted a parental leadership control using their parental control component, which could help parents safeguard their children from the hidden dangers of unbridled use of computers and the Internet. In fact, in today's era, the youngsters could easily be exposed to the unknown hazards because of the use of the Internet. Even networked printers that can be used to print images and pictures. Many of these safety hazards are related to the youngsters' physical and mental health and that is also a concern for safety and security when using social networks. To a great extent, many youngsters' lives are associated with social networks and online friends who may often be unknown on (actual) personal level.

In line with the Internet Security Threat Report [7], SNSs have become the scammers' favorite destination in the recent years. They use numerous scamming strategies to scam SNS end-users through manual sharing, fake product like jacking, supplying fake apps, and fake plugins. Manual sharing, however, has been used extensively in the most recent years. Some essential selections of SNSs, like sharing footage, commenting, tagging, and blogging, generate an oversized portion of the way of life of billions of web end-users.

3.1. Cyber Threats Related to Exposure of Personal Information

It is a reality that many users share too much personal information via SNS. Psychological traits of human beings often compel a user to post issues that he/she would not share in person in real-life. Some people regularly or on daily basis upload videos, comments, audios about personal habits, lifestyle, clothes, political views, and so on. They may use various blogs, vlogs (video blogs) that show even some of their daily routines and mundane works like even brushing teeth, washing face, etc. While there is a sense of joy in showing own life and getting some type of attention from other users, as reported in [7], various threats like fraud, spamming, phishing, on-line predators, trolls, and various forms of cybercriminal attacks could be launched against such users or individuals. It is possible today to even obtain full name, actual address, location, country of a user whether it is with his or her permission or not. As known today, even with the must-provide personal information for opening an account, a good amount of information is known about a user. Scammers can use this to start the process of obtaining more information and when this involves financial transactions, things get serious. SNS could be used to offer business opportunities and for selling fake products and in this way obtain even credit card's information.

3.2. Damage to Reputation and Character Assassination

Many SNS users use public networks to access their SNS accounts. Often, they may forget to log out from publicly accessed computers in university laboratories or in restaurants or other places. With the increase of handheld devices in IoT setting, it is also a fact that many users' devices can be stolen or lost. Logged in SNS account means any other person can then do something with that to damage the reputation of that individual. While these are restrictive cases, hacking of SNS account is also common nowadays because of using weak passwords or perhaps, someone could just pose as a friend and obtain or guess some password and do the same.

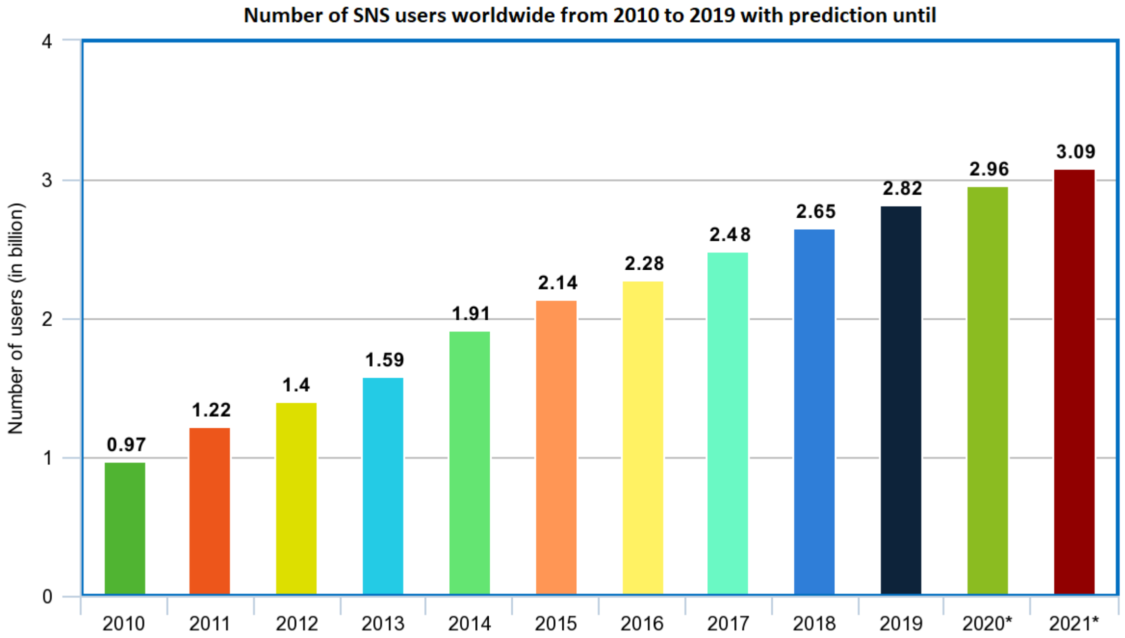

Figure 3. Number of SNS users worldwide from 2010 to 2019 with prediction until 2021.

Even if false information is spread over the SNS for a short time, there would be many people who would straight believe the fake information without verifying the authenticity. As SNS is for sharing views, videos, and photos among the friends and whoever is in a connected network, even lies could spread within quick time. Even before the actual information is known, reputation can be considerably damaged in this way. As human psychology works, even if some claim is found to be false against an individual, some doubt may remain after such fake information is shared with hundreds of users.

Indeed, character assassination is easy to do over the Internet. Character assassination could be defined as some malicious and unjustified intentional activity to harm an individual's good reputation. Such activity could be selectively applied to social groups and institutions. The reputation damage can happen for both individuals and companies that can really harm their business in short or long term. Also, some users can do public posting without much thoughts and that can affect their reputation. As an example, in Dec 2013, top Lacoste salesman was dismissed due to posting his bank check on Instagram [27]. Such whimsical posts could not only cost the reputation of an individual but also it could damage seriously the company as some sensitive information can get exposed in this way. There are other such incidents found in various blogs and newspapers (we prefer not to cite all those blogs and newspaper articles in this research article but the users may find such news on daily basis).

3.3. User Profiling

SNSs are extensively used by various companies and commercial organizations to target users with specific products and advertisements to maximize their profit and create demand for their products. Even with the publicly available information, a user profile can be created. When targeted email is sent or the user is tricked in inputting more specific information about own self, the user profile is made stronger or more accurate. Even without enough knowledge or consent, the user himself/herself often participates in this kind of trick; like simply assisting a company obtain some views about something and the initial communication starts from an SNS account.

In [28], 126 amazing statistics and facts have been presented about social media or SNS. The author note that every click, every view, and every sign-up is recorded somewhere when someone browses Internet! Some of the most interesting facts are like the amount of around US $74bn that was spent on social network advertising in 2018. 38% of organizations planned to spend more than 20% of their total advertising budgets on social media channels in 2015, up from 13% a year ago and only 20 Fortune 500 companies actually engaged with their customers on Facebook, while 83% had/have a presence on Twitter. All these efforts rely on user profiles for which SNSs are the best sources. Indeed, so much information about a user could not have been collected in any other way. This collected information possibly could influence users easily as SNS profiles contain an oversized volume of user's personal data, choices, health information and routines, friends and surroundings, concerns, political or ideological stances, and so on.

4. Classification of Threats and Security Issues

In this section, we do a classification of threats and security issues in SNS. While the previous section talked about the major categories that affect all of the issues below, here our discussion is a bit detailed. Also, we extend the concepts presented in Rathore, S. et al.'s work [24] with the most recent relevant knowledge and data. The overall classification that we have done for SNS security threats and concerns is shown in Figure 4.

4.1 Issues Related to Multimedia Content

Multimedia content sharing is an essential part of the platform of SNS. Users may post their photos, recordings, exercises, interests, etc. with some intervals. But, these multimedia contents could be exposed to various forms of threats and negative consequences. Here in this section, we talk about those issues with some addition to those discussed in [24].

4.1.1 Exposure of multimedia content

SNS frequently uncovers the written data posted by a user. When a user does any purchase via SNS, his/her identity, phone number, and postal address could be exposed. While written data may not contain audio and video components, if a user posts photos of his or her home, an unwelcome guest could discover the user's street range by analyzing those. A simple case is when someone posts a photo when traveling or on a vacation, the potential burglars can obtain the information that the home may be easy to break in. Another typical information exposure is when a user is in a group photo and that is posted by another user or random photo taker who posts that without approval of all other people captured in the photo. This can reveal information about someone's whereabouts at a particular time and place and can be spread over the Internet. There are ways of face recognition and some photos may be automatically detected for a particular user when certain information is sought about him or her. Hence, multimedia content, when with audio and video may reveal a great lot of details about a person [29].

4.1.2 Shared ownership

Many friends and known people often travel or stay together. Two friends using social network posting the same photo from two different accounts may be noticed and recorded by some third party. It is very easy nowadays to ascertain who is a friend of who, even in real life if SNS accounts and postings of similar or same multimedia contents are analyzed. Hence, there is indeed some great danger of revealing more than what an image or video shows when the content has shared ownership. This is a fact that many users simply do not use only private groups but rather many contents are rather publicly shared.

4.1.3 Manipulation

Manipulation of posted multimedia content is a great threat. A malicious user or attacker can download a video or image and modify that and repost so that others may see it differently. This can sometimes cause serious damage. Today, there are various photo modification software and technologies like for instance Adobe Photoshop, Deepfake [10], [30], and so on. Just by using these facilities, doctored images can spread discord among people and friends and things or real events could be twisted for deceitful purpose.

4.1.4 Stegobot

Steganography [31] is the technique of hiding information in multimedia carrier contents, which could be images, audio files, or video files. Though steganography is often considered for positive use, there is something called social botnets which could use the technique for negative activities taking advantage of the environment of SNS. In general, a social bot could communicate over seemingly unobservable communication channels. It could also be used to obtain sensitive information from its victims. Stegobot [32], [33] is a type of social botnet which uses steganography to hide the presence of information and communication. As unique propagation methods can be exhibited by these stegobots, existing botnet detection techniques may not be able to even detect these bots. When SNS environment is used with sharing of too many images and multimedia contents, it is even more difficult to detect propagation of the stegobots.

4.1.5 Metadata

Metadata simply means data about data, i.e., a form of data that contains and conveys meaning of some data. In SNSs, mixed media substance moves as information on the ground that this substance could contain vast amount of different profitable data; as an example, IDs and locations. Even though these are elementary data, these could be used for making geo-area labels. When the users are accurately modeled in various geographic regions, it could be used by both positive and negative entities. For instance, for setting up cell towers for mobile phone network, it could be useful while for some rogue marketing strategies, some company can use the same metadata. Even this is possible to map people of different spiritual or political inclinations, health conditions, and so on. As an example, Flickr photos could be used for finding the location of the web source and similar mechanism can be applied for Twitter posts or Wikipedia edited pages [34].

4.1.6 Shared links for multimedia contents

SNSs often do not support all types of sight and sound configurations and users cannot post all types of mixed media. For instance, a user may simply share a picture on Facebook as a JPEG or PNG file but it may not support GIFs (broadly speaking), as they are enlivened. In such a case, a user may provide other components via sharing links where the other users can access the audio and visual substances in some different unsupported configuration or format. Here comes the part of potential rogue user's role to misuse the other associated contents and even sometimes replacing the connected materials with fake things. Often, the original user may not even be aware of the changed items for his/her shared associated links unless someone lets him/her know and by that time, some real damage of credibility can be done [13].

4.1.7 Static links

Many users sometimes post or share static links to resources for downloading or using of other users. While the threat of content modification and changing the link remains, sometimes the user may forget to delete or remove a link that is supposed to be shared for a fixed period of time. Such longer period of shared static link could be exploited by other rogue entities to gain from that illegally or without authorization of the original owner of the online content. Even some other people can use the same static link on own profiles or own blogs and get more subscribers or followers. Hence, the original user may be deprived of the genuine level credit he should get.

4.1.8 Outsourcing and transparency of data centers

Some of the SNS providers use external repositories to store their multimedia contents; like for instance, a cloud-based server could be used. This opens the door of modification of the actual content. Even though financially it may be a good choice, often the control is not directly in the hands of the SNS provider company. Larger SNS companies like LinkedIn or Facebook have their own repository facility but smaller firms may not be able to afford such own repository or server and need to do outsourcing and that may affect the transparency of information or the content's control may be lost on some occasions.

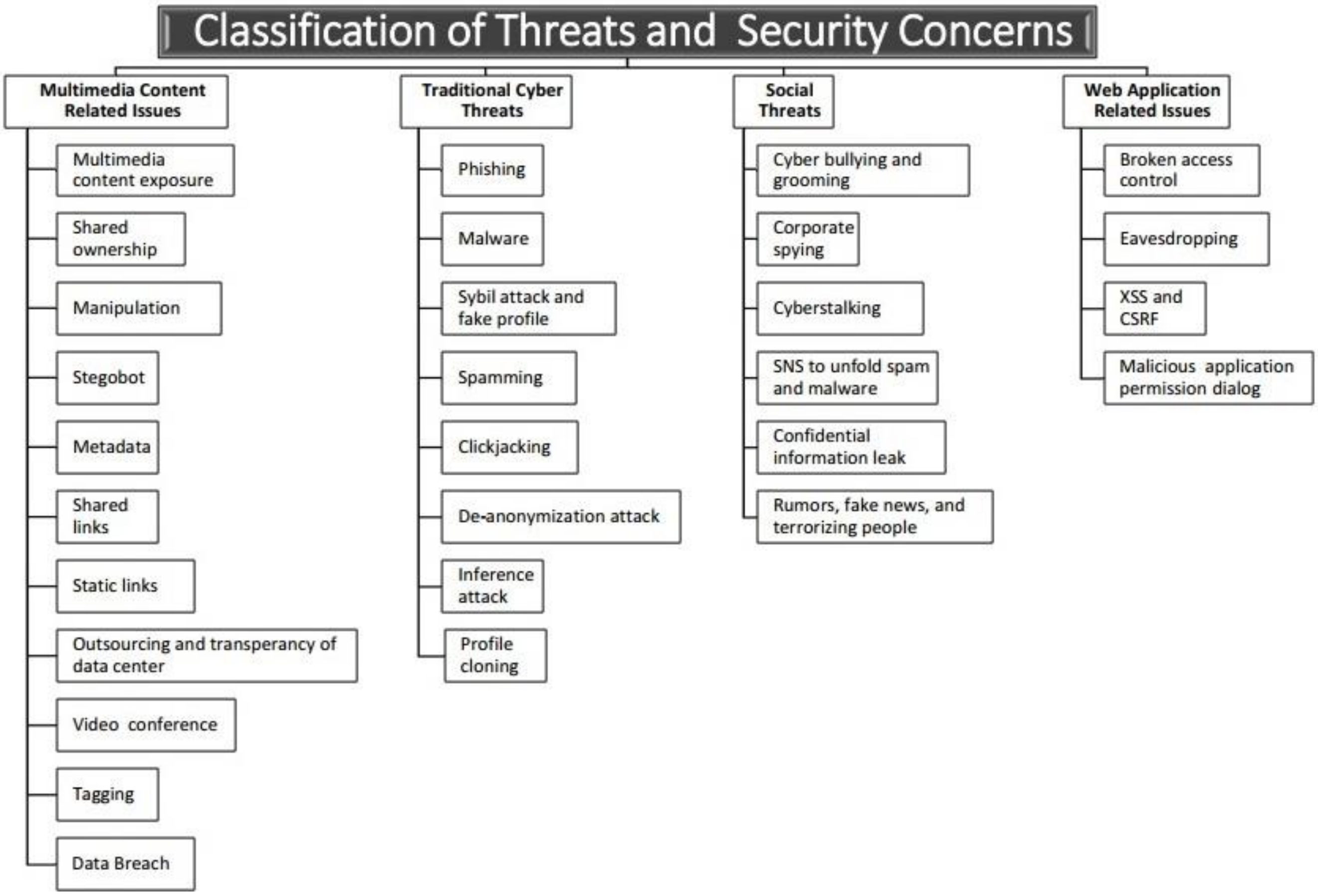
Classification of Threats and Security Concerns
Multimedia Content Related Issues
Multimedia content exposure
Shared ownership
Manipulation
Stegobot
Metadata
Shared links
Static links
Outsourcing and transparency of data center
Video conference
Tagging
Data Breach
Traditional Cyber Threats
Phishing
Malware
Sybil attack and fake profile
Spamming
Clickjacking
De-anonymization attack
Inference attack
Profile cloning
Social Threats
Cyber bullying and grooming
Corporate spying
Cyberstalking
SNS to unfold spam and malware
Confidential information leak
Rumors, fake news, and terrorizing people
Web Application Related Issues
Broken access control
Eavesdropping
XSS and CSRF
Malicious application permission dialog

Figure 4. Classification of SNS security threats and concerns.

4.1.9 Video conference

Nowadays, it is a very common phenomenon that some users do live video-streaming via SNS. Many users may also do video conferencing and communications via this platform. In such a case, when some video communication is going on, a third party may capture videos illegally and record for later use or may use some segment to distort the context and defame the user. By exploiting potential vulnerabilities, video conference can also be diverted to the malicious pretending user on the other side. Sometimes, two online friends may like to see each other over the Internet but they have not seen each other in real life. Here, some rogue person can pose as the real person on the other side (blocking the real person) and then cause harm later to the actual relationship between the original pair [35].

4.1.10 Tagging

Often SNSs offer a labeling highlight within shared media data to expand communications among the users and to enable advanced search skills. A user would label recordings and footage that the person in question discovers affordable and interface them with some extra knowledge. Nevertheless, this labeling highlight may incur some security dangers for the end users. As an example, there are various SNS users who would favor to not transfer any photo of them on any SNS website. In spite of that, someone among the friends or fellows may share one or two or more photos with labeling and acknowledging them [36]. The principal issue is that such labeling could connect even someone who does not have a space or account with any SNS and does not have any need to impart any of his/her own knowledge to SNS [37]. Likewise, a sender could label on huge amount of solitary posts - as an example, a picture or video, thus revealing much about someone else to a larger cluster of watchers with very little effort [38], [39].

Table 1. Data breach for SNS (only selected data from the Bromium report [40] – 'm' means million).

Year	Platform	Losses	Method
2018	Facebook	50m user records	Security key hack that allowed users to stay logged in.
2018	Google+	52m user records	Glitch in Google+ platform. External app developers could access the data.
2016	Myspace	427m user records	Data discovered for sale from an earlier hack.
2016	Linkedin	117m user profiles	Unknown.
2016	Twitter	33m	Hackers used infected browsers.
2014	Snapchat	4.9m phone numbers	Simply used 'Find Friends' feature, which requires users to enter their phone number to see if other contacts are also using Snapchat

4.1.11 Data breach or data disclosure without authorization

SNSs often keep record of the user's association with certain workplace or group or committee, etc. Even if one may not like to share all information in public setting, some of that information would be often disclosed without proper authorization due to the nature of SNS. Such data disclosure can harm someone even after long number of years. The cyber world often in reality does not forget what has been recorded or what someone had posted as image or video or audio long

number of years ago. Hence, this is indeed a great concern.
McGuire in a Bromium report [40] reports the extent of data breaches via various social networking services. Here, Table 1 shows the data breaches for some top SNS platforms (only some selected SNSs and associated figures are mentioned). This is indeed at an alarming level.

4.2 Traditional Cyber Threats

SNS is a platform for almost all types of traditional security cyber threats. By using some tricks, an attacker can obtain information about a client's standardized savings range, login secret key, monetary balance subtleties, and so on. In this section, we talk about the major ones.

Figure 5. Phishing (conceptual image).

4.2.1 Phishing

Phishing [41] (conceptual image shown in Figure 5) is a type of cyber attack in which the targeted person is bombarded with the emails that look very similar to the emails coming from their banks, insurance companies, and other service providers. The hacker targets the people through emails to get their sensitive and personal information related to their financial and other account information disguising as the genuine and trustworthy individuals.

The main target of the phishing attack is to illegally obtain credit card number, ATM pin codes, passwords, user name, and the related information. Once the information has been collected, the hackers use that information to steal money or other valuable digital assets. This attack is normally used for financial theft from the bank accounts. The marketing strategies and campaigns also use similar kinds of tactics to increase the sales of the products.

There are three major modes of phishing used in the modern phishing activities as listed below:

- Telephone calls commonly referred to as voice phishing or, Vishing
- Emails referred to as general phishing
- Small text messages (SMS) referred to as Smishing

The core objective in all three modes of phishing is to steal the identity and sensitive information of the legitimate user by alluring via different modes of communications. SNS is the first formal information source for an attacker to choose a potential victim.

4.2.2 Malware

This can be a rogue program that contains Trojan seeds, infections, and worms. SNSs work upon the connections of assorted frameworks of clients. During this connection activities, malware would essentially move between various clients' frameworks by means of the network or web connections [42], [43]. Different types of SNSs have different systems and all of them do not have the most effective tool to make a decision if a computer address is pernicious or not. A malignant computer address could divert the client to counterfeit sites, and, later transmit malware to client's computer and thus take his or her personal data. Faghani et al. [44] reported that the malware can propagate through online social networks. They identify the parameters which are related to malware propagation in online social networks. Two types of social network worms were simulated: XSS and Koobface-like worms. It was found that the propagation of XSS worms depend on the visiting behavior of the members/users. By visiting strangers' profiles/pages, the worm propagation gets relatively faster while visiting known people or family members and friends slows down the process. The highly clustered feature of social networks also helps slow down the propagation. Increasing the initial infected profiles at the early stages of XSS (Cross Site Scripting) [45] worm propagation leads to an impressively faster propagation.

4.2.3 Sybil attack and fake profile

Attackers in such case create phony personalities that facilitate them to accomplish their objectives within the shared framework of SNS. A Sybil attack [46] is a noteworthy concern for SNS security since in this case a good number of fake user profiles can be used to target someone to make him believe something or to invest in some business or to pay for instance for charity works or humanitarian needs. In this way, all these Sybil profiles which are actually not what they claim to be can deceive easily many other genuine users.

4.2.4 Spamming

Spamming is usually associated with emails. However, SNS can also get spamming attacks [47]. For instance, many small businesses use Facebook or other SNS platforms to sell products and items. Spam or fake reviews could be used to raise the demand of a product. Hence, consumers could be targeted with spam information, potentially dangerous URLs (Uniform Resource Locators) and web links, and even fake email addresses that, if contacted would be attended by an attacker or a group of attackers who could do other forms of fraud.

4.2.5 Clickjacking

There are many threats that overlap each other in terms of the objective of deceiving genuine or legitimate users of SNS. Clickjacking is basically tricking a user into clicking on something different from what the user intends to click on [48]. This is pretty easy to do in this era. Users are often curious and just some attractive words may make them click on something online. There may be mainly three types: Likejacking, Cursorjacking, and Filejacking. Likejacking is a type of clickjacking in which malicious coding is associated with a Facebook "Like" button. Cursorjacking deceives users by means of a custom cursor image, where the pointer is displayed with an offset. Hence, the displayed cursor is shifted to the right or the position is changed from the actual mouse position. Filejacking allows extrusion of directory content from the target underlying Operating System (OS) to the attacker's server through clever UI (User Interface) manipulation within the browser. All these could start with some click of the computer mouse button when using SNS sites!

4.2.6 De-anonymization attack

Some users may like to have anonymous profiles on the SNS. This may be done to assess something for positive purpose, like for instance a responsible government official is trying to understand the mood and sentiment of some people who is under his care or perhaps, a company manager is trying to find out any serious issue that is shared among the other employees but that does not reach him. Such profile could be used to fight certain behavioral misconduct or such kind of true cases which may not often be reported with clear identity. The problem here is that with de-anonymization attack, the anonymous profile could be exposed. The concept of de-anonymization is basically found in data mining field which re-identifies encrypted or generalized information. If certain tricks are used to uncover the user's actual identity, that may cause trouble. A case could be a lower level employee who faced some harassment and posted some issues with anonymous identity. If the identity is revealed by de-anonymization technique [49], [50], the person may find trouble or even can get death-threat in some cases.

4.2.7 Inference attack

Social networks are such that many connected friends and other users can also be great source of information about a particular individual. Some works [51], [52] show that a user's friends list could be checked and their given information about the user could be used to obtain complete set of properties and traits of someone. Then, that information can be used to influence another one in the circle. Such case is termed inference attack. In fact, by studying recorded posts in Facebook or even LinkedIn, a client's professional inclination, covert personal knowledge about another one, etc. can be obtained. For instance, even the recommendation made by someone on Linkedin Profile can be used to communicate with the person in a certain manner to beguile and cheat him/her online.

4.2.8 Profile cloning attack

Profile cloning [53], [74] is a serious threat in SNS platform as a rogue user may copy another profile or use similar looking themes and items to dupe other genuine users. Thus, the perpetrator can abuse someone else's identity, reputation, image, and so on. Profile cloning and Sybil attack are different because in case of Sybil attack, an attacker takes another's identity but in profile cloning, a very similar profile page or cloned page or account is opened targeting the actual owner of a user profile. An aggressive profile cloning attacker can even download photos and files from other accounts and use those as his/her own. For YouTube for instance, there are often stealing of videos and re-posting without taking appropriate permission to get clicks and views. Not all these are reported and when similar looking profiles are used, the genuine users can get confused. Great level of harm could be done in this way in reality.

4.3 Social Threats

Social threats are related to the social interactions. Online platform could be used in various ways to affect the psychological and social behavior of a person. In this part, we discuss some of the most prominent ones.

4.3.1 Cyber bullying and grooming

This is purposeful verbal or other types of remarks or actions towards someone via online means [51]. SNS could be used to also groom someone for a particular action taking long course of time. There may be criminals who could first pose as friends and then get into personal affairs and even influence a teenage person to commit suicide! Even crooked remarks on someone's photo or appearance could hurt someone in a bad way. Especially, the adolescents can easily fall victim to cyber bullying and grooming as they could be affected with depression in that age. SNS could also be used to threaten someone's life or property and making him panicked about something.

4.3.2 Corporate spying

By analyzing SNS based information, a company can spy on another, possibly understand or predict a possible business move. Though SNS brings lots of benefits in spreading good name and attracting more customers, the same could be used for spying as it reveals a lot of information that would not be otherwise easily spread over the Internet. The work in [54] depicts advanced social engineering done by utilizing SNSs.

4.3.3 Cyberstalking

Cyberstalking [55] is one of the most serious problems in the domain of cyberspace and especially for SNS. Women are the most affected population of cyberstalking. Cyberstalking is a systematic approach of harassing done through email, phones, SMS, chats, and other forms of communication. Someone's social network account can be the opening door for this. The main components used in the communication to threaten the targeted entity include defaming, false allegations, slandering, and other forms of blackmailing. Digital cyberstalking is similar to the offline or physical stalking done in the streets, at home, or at shopping centers through different traditional modes of communication. The impact of cyberstalking on the teenage group is much pervasive and widespread. They happen to be so sensitive and less mature to handle the pressure of blackmailing targeted on them. In certain conditions, people succumb to the pressure and commit some serious life threatening acts such as suicide and other such things. The other common names of cyber stalking are Internet stalking, online stalking and e-stalking. In many countries, the cyber stalking is a punishable crime.

4.3.4 SNS to unfold spam and malware

Social networking platforms like Twitter and Facebook typically do not spread malware on their own. However, there is a growing trend of using shortened URLs (Uniform Resource Locators) which could be used by the cyber criminals to mask their malicious links. This kind of brief URL looks different than the original one and it could easily attract the user to click on it. In this way, the platform could be used to spread malware and spam codes.

4.3.5 Confidential information leak

Much of the confidential information could be leaked via SNS. An employee may tweet often about his mental status or a company job or apparently uncritical technical information how he might have had bypassed the system's restriction to use a company computer to post a tweet or so. Such kind of discloser can reveal a lot about the safety measures put in place in the company and some confidential information about the company's security system could be leaked out. Usually, there are some banks which do not allow the employees to browse SNS sites during office hours and such breach of information may be used by the attackers. That piece of information then can be used via the cyber space to influence the other online SNS users' behaviors.

4.3.6 Rumors, fake news, and terrorizing people

SNS platforms could spread rumors quite fast. Youtube, Facebook, Twitter and so on can be used by terrorist groups to post propaganda or threaten people with something. There could be fake threat givers as well. Rumors over the Facebook in the recent times have been seen to spread for some country's internal issues. Some events in some countries led to violent protests. Many random users share stories from those events, even if untrue. Again, a case like the gunman who live-streamed his attack via Facebook while moving from mosque to mosque at Christchurch, New Zealand, during Friday Prayer on 15 March 2019 created panic and terrorized lots of people [56]. This kind of incident could really create terror among the people who may watch such ongoing event via social networks.

4.4 Web Application Related Issues

Typical web based attacks can also be launched in SNS. In this part, we talk about those that are common but related to such platform.

4.4.1 Broken access control

There are many access management applications that enforce some policy for specific users and without fulfilling the conditions, the users are not given permission to access certain items in some social network account. When such access control is applied, even failed attempts may cause unauthorized data revelation, modification or destruction of all data, or doing tricks with any of the users. Common access management vulnerabilities include: (1) Allowing change of the primary key of another user's record, permitting viewing or editing someone else's account; (2) Elevation of privilege like acting as a user while not being logged in, or acting as associate admin once logged in as a user; (3) Metadata manipulation, like replaying or changing of state with a JSON (JavaScript Object Notation) Web Token (JWT) access control token or a cookie or hidden field manipulated to elevate privileges [57]. The web platform that is used for SNS could be vulnerable to various forms of broken access control attacks.

4.4.2 Eavesdropping

When the users access their SNS accounts from various locations, sometimes via publicly available networks and Wi-Fi facilities, in the airport or restaurants or such places, they may become targets of the eavesdroppers who may try to capture their communication while logging in. Afterwards, they could analyze that to find out the key or password used. Hence, eavesdropping over communication for social network systems is indeed possible [58], [59].

4.4.3 Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)

The work in [60] shows that XSS worms can be injected or planted in the form of post on SNS web applications for hijacking the online user's account. In case of an XSS attack, an attacker basically tries to lure the user either to click on the malicious link or visit an infected web page so that malicious script injected by the attacker could be executed at the browser side. SNS is in fact an easy target for such tricks as many users click on links without much thought or out of curiosity when using Facebook, Twitter, and so on.

4.4.4 Malicious application permission dialog

Many SNS sites enable integration and development of widgets. A widget is an element of a graphical user interface (GUI) which displays information or provides a specific way for a user to interact with the operating system or an application. Games, interesting interactive tools, etc. can be used in this way for interaction among friends on SNS platform. Often, such tools ask for granting specific permission or specific access to user's account information. But, this mechanism can be also used by cyber criminals who do deceptions with those widgets and gain information about the victim illegally. Sometimes, a victim can be asked to repeat and execute a malicious script manually. For example: "*find your facebook twin*" scam on Facebook [61]. User usually follows the given instructions however, in the background, hidden JavaScript executes and provides permission to attackers to use this logged in session to send messages to any or all the user's friends, asking them to repeat the cycle. This kind of fraudulent activity could be used for spreading fake information and exploit the friends' sentiment or at least could cause harm to the victim and his/her reputation. The malicious web application could open the door for this.

5. Some Security Solutions for SNS

In this section, we discuss some notable security solutions for SNS. While user behavior cannot be controlled and even training does not work for someone's private behavior, there are some technological means to tackle many of the security threats and thwart many of the security attacks in SNS environment. Figure 6 shows the names of some security and privacy solutions available for SNS environment.

5.1 Watermarking

Digital Watermarking could be used to verify the authenticity or integrity of files in SNS. This is the process of hiding digital information in a carrier signal. In this case, the hidden information should contain a relation to the carrier signal. Some files can reveal the watermark and still shows who the original owner of the file is. Zigomitros et al. [12], in their work present a concept that utilizes double watermarks to ensure client's security in SNSs. Thongkor et al. [62] present an image watermarking technique based on DWT (Discrete Wavelet Transform) coefficients modification for social networking services. Watermarking could be an approach to protect ownership of photos especially in SNS platform.

5.2 Fake Profile Detection

Fake profiles on SNSs are quite common. To detect fake profiles, there are various types of methods. Some techniques use for instance machine learning method [63], some use another forged profile or account to detect a fake profile [64], detection of emotions [65] and there could be also some collective efforts among the legitimate or real users for such detection.

5.3 Metadata Removal

As many SNS users do not even know that their uploaded images to the SNS sites contain embedded metadata (like the camera which was used to take the photo or the geographical location or from where it was uploaded, etc.), metadata removal [66], [67] is an effective technique to ensure privacy of the users. In fact, embedded metadata reveals a lot of information about the user and that could be used by other companies to set their strategy to target specific users with their products. In the work recently done in [68], the authors provide a programming example in the Python programming language which could perform the removal of all the metadata, or just the Global Positioning System (GPS) location data, from photos. Their technique suggests that it is a better strategy to create identical copies of the images/photos that are free of metadata instead of completely stripping away the metadata. Just this technique can help the users maintain their privacy to a great extent.

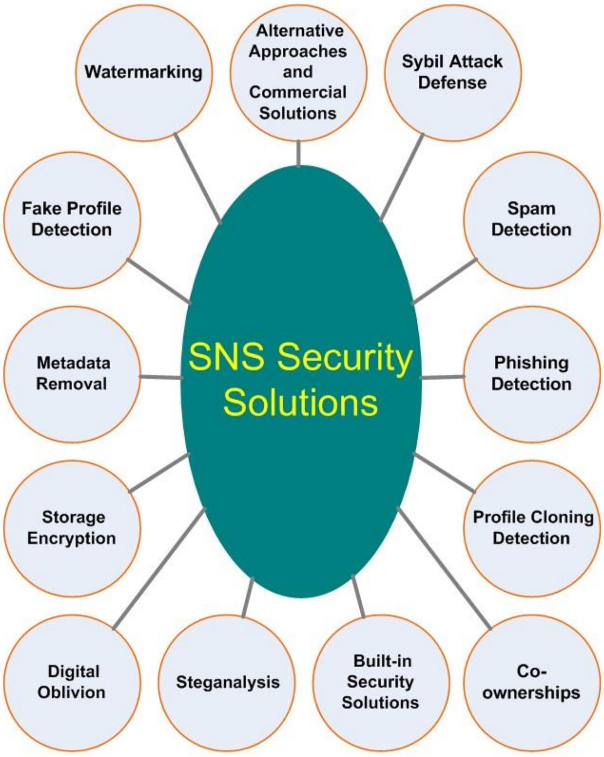

Figure 6. Security and privacy solutions for SNS.

5.4 Storage Encryption

SNSs often do not have their own data centers and they customarily store information of the user in the data centers of third parties. The problem is that the data centers can provide the information to other parties due to political or security or other critical purposes. Sometimes, this kind of sharing of information is needed as a country's policy is, like for instance even to ensure homeland security or to protect the country from external threats or so. Such disclosure to some other party without consent of the original owner of the data, especially for healthcare or medical issues, violates the privacy of the patients often. There may be great deal of sensitive knowledge regarding these SNS data. Hence, encryption of all such storage is a solution. Savla et al. [69] reviewed the privacy policies of thirty-five health-related SNSs and therefore, the outcomes indicate that there was no explicit privacy policy for nine percent of them. The reality is that such leak of personal information could be very harmful for some individuals and hence, data storage encryption is the solution in this case.

5.5 Digital Oblivion

Digital oblivion is a technique which sets a date and time after which any posted image or multimedia material or similar thing could expire in the digital or cyber space [11], [70]. It is a fact that often the teenagers post sensitive materials via SNS sites that may sometimes include personal behavior or some other comment or something that may be found through search over the Internet which could potentially harm them when they apply for a job or for their careers at any point of their life. In such case, even if the original user who posted those materials forget, digital oblivion technique would take care of the issue and would automatically delete or destroy the image or video (or any other sensitive post or material). This could be an effective technique to deal with user's forgetfulness of a past issue which perhaps he or she was involved in and during that time, acted imprudently.

5.6 Steganalysis

Steganalysis can be used to detect suspicious images that hide information within those images that could be used by rogue users in SNS platforms. Li et al. [10], in their work talk about steganographer detection problem in social media networks. They mention that the issue is quite different than the traditional stego detection problem because, steganographer detection is for detecting suspicious users while stego detection means detecting suspicious images. As SNS contains huge amount of images, stego detection techniques could be effective to solve the steganographer detection problem as well.

5.7 Built-in Security Solutions

Some built-in security solutions could better safeguard user's authenticity and privacy. SNSs often support a wide variety of essential safety alternatives, like privacy settings for users, permission mechanisms, abusive content reportage, etc. SNSs offer authentication mechanisms to verify that the user operating the account or confirming whoever is registering is the legitimate one. Over the course of time, various built-in security solutions are being used or newly implemented. For instance, multi-factor authentication [71] is an effective way to tackling fraudulent users. Multi-factor authentication means that the system of authentication consists of multi-stage authentication factors or is based on three or more factors. The major 3 factors used are known as: (a) *What you know?* Like for instance, PIN (Personal Identification Number) code. (b) *What you are?* Like, biometrics, face recognition, fingerprint. *(c) What you have?* Like, digital key, or mobile device with a software application to scan. Many SNSs, like Facebook and Twitter, or so nowadays have options of two-factor authentication mechanism.

5.8 Co-ownerships

A method of ensuring privacy of SNS materials is using co-ownership where more than one user holds the ownership of an item [72], [73]. Palomar et al. [73] present a mechanism where all co-owners have right to take part in the process of data sharing by choosing their suitable privacy preferences. Also, all of the owners must agree on the access policy. The authors use a number of parameters like gender, affiliation, postal code to define particular privacy preferences. If all conditions are satisfied, the material could be viewed by another user via SNS. Also, such content can be accessed by a user who satisfies the access policy even without disclosing his/her real identity.

5.9 Profile Cloning Detection

As profiles could be cloned in SNS, profile cloning detection methods are very important to safeguard the reputation and identity of the real user. There are a few techniques available. For instance, Bródka et al. [74] propose a method which checks the similarity of attributes from both profiles (the real one and the fake one). Another approach suggested by the authors is to verify the similarity of relationship networks. In fact, real profile would be verified and would have real friends that are connected to the user while the fake one would not get many of those legitimate friends in its surroundings or in connection. Devmane et al. [75] studied Facebook, LinkedIn and Google+ for detecting profile cloning. The authors suggest information extraction from user's profile and searching techniques for detection while for prevention of profile cloning, they suggest limited publicly available personal information, proactive profile management, accepting only known people as friends and double verification, routine checking of profile settings, visibility setting to limit access or views to contents in such SNS profiles.

5.10 Phishing detection

Phishing detection is difficult for SNS sites however, not impossible. Again, user's personal online behavior also is a main factor for phishing based attacks. Aggarwal et al. [76] propose the phishAri methodology to identify phishing on Twitter. This technique classifies tweets with URLs into two categories by pattern of the content of the tweets. Several issues like hash tags, tweet length, range of followers, sort of tweets, etc. are taken into consideration for such categorization. It detects suspicious URLs posted on Twitter. Hence, it could warn user even before he/she clicks a malicious link and gets trapped with phishing attack afterwards.

5.11 Spam detection

Wang in the work in [77] presents a Web crawler which is developed relying on API (Application Programming Interface) methods provided by Twitter. The author collected around 25K users, 500K tweets, and 49M follower/friend relationships in total from publicly available data on Twitter. The core mechanism for suspicious behavior detection is based on Bayesian classification algorithm. The results showed promising results. Similar mechanisms could be developed for other types of SNS sites/platforms as well.

5.12 Sybil Attack Defense

While fake profile (as discussed in section 5.2) is in reality a kind of Sybil identity, here in this section, we mean by Sybil attack that it is a deliberate attempt to assume someone else's identity to actively engage in deceiving that original user's friends and family profiles. Such organized campaign can be sometimes very dangerous especially in a large scale social network – for a person who has hundreds of friends even in real life. Wei et al. [78] in their work introduce SybilDefender which utilizes the topology of the network to defend against Sybil attack. Their mechanism was tested on two 3,000,000 node real-world social topologies. The results were promising in defending against Sybil attack in large scale social networks.

5.13 Alternative Approaches and Commercial Solutions

There are some alternative approaches and commercial solutions that could help secure SNS when using those via some tools and browsers. For instance, Facebook Phishing Protector is employed as a Firefox add-on to identify dubious operations, like injection of malicious browser scripts into Facebook [79]. Symantec, McAfee, Panda, Kaspersky, and AVG presently provide SNS users with net security coding system. This coding system includes firewalls, some intrusion detection system (IDS), anti-virus programs and different coding systems to safeguard users from attacks like phishing, Clickjacking and different types of malware [80]. Again, Xu et al. [81] propose a malware detection scheme for SNSs that leverages every SNS topology and malware propagation choices.

6. Discussions and Key Takeaway Points

Given today's staggering growth of various IoT devices and especially, smartphones in the hands of people, it is clear that the future of social networks would heavily depend on the mobile networking services. Today, we see that some smartphones have added separate button to directly hit Facebook or Twitter or such SNS sites. Many users are simply attached to the SNS sites for their daily activities. Emotions depend on the SNS posts and others' comments and "likes". Even we have seen that opinion of a particular user may be heavily influenced based on the remarks and comments of other users. Many try to get others' approval for doing something even for personal life!

In an IoT setting, such issues would be more penetrating in the coming years. We have reached a stage today when we see that SNS can heavily influence even the election results for various countries. It is reported that social media companies took a more active role in combatting election interference in the recent years. In fact, Facebook set up a war room to tackle election interference; Twitter removed over 10,000 bots posting messages encouraging people not to vote on one occasion [82].

As we may see the future, as it is almost impossible to control such social network addictions for many people, we need to take measures to allow such interaction to happen even in a large IoT setting ensuring that the privacy and security of the users and their devices are maintained.

As the technologies related to biometric authentication are advancing, it is expected that in the near future, a massive amount of smartphones and handheld devices connected to the IoT would have at least a two-factor authentication system. As for the SNS platforms, they may be more dynamic. People may do video chatting and video conferences frequently when the support system based on IoT offers faster speed and greater volume of data transmission with low latency. SNS sites or platforms could be used for live streaming of real events, for instance football matches from the stadium directly. When virtual reality (VR) technologies would be linked with that, some streaming can be used for 3D viewing via SNS for other users to get some feelings that they are present in the stadium that is geographically at a distant location or even in another country on the face of the earth.

Various technologies and their advancements thus could make SNS more effective for the general people and those who use those. On the other hand, such IoT-based massive use could provide more data about a user to the chance-seeking companies. Hence, SNS must do more to set proper privacy policy, take care of the user's sensitive information, and there must be appropriate filtering mechanism when sharing data with other parties that may not be directly related with the user. As the dynamism in SNS setting is expected to increase in IoT-based infrastructure, proper regulations must be employed to address all the concerns discussed above.

Whatever the future yields, for any user using SNS, there are some general recommendations:

- User should use strong password.
- Password should be changed on a regular basis.
- Unnecessary data should not be provided by SNS profiles.
- On the friends list, unknown online personalities, whatever attractive one is, should not be added.
- Even if someone is added without enough knowledge about the person having an SNS account, the

activities of the person should be monitored for some time.

- Remarks of trusted online friends, even if not known in person must be given importance when it is about warning about other rogue accounts or profiles.
- When mentioning email address on SNS sites, the user should spell out an address instead of writing the exact one like for instance, xyz@site.com as “xyz at site dot com”.
- Typical anti-virus software, firewalls and other security tools should be kept active/enabled while using SNS.
- The user should never click on suspicious URLs posted on unverified or unknown profiles.
- Even URLs posted on known profiles should be at least skimmed through before clicking. Taking mouse cursor over the URL shows the actual link on some browser’s bottom part. That could indeed help.

7. Conclusions

Billions of Internet users have now chosen SNSs as a vital way to communicate with each other. The free sharing facility for their own photos, views, achievements, etc. have kept many captivated daily to use such platform to engage with their friends and families. The users can now connect with each other beyond the boundaries without thinking of the extra expenditure. In fact, just the Internet line’s monthly fee is enough. Life is now easier, but with that the risk is also higher as very sensitive and very personal information could easily get leaked via social networks. In this paper, we summed up all the most recent security concerns in SNS and considered what could happen when IoT makes the SNS platform easily accessible for anywhere with greater penetration and access to every day’s events. While some existing works analyzed some of these issues, we have considered the future and suggested some common guidelines that would be relevant when using SNSs also in future irrespective of the technology used for the interconnection of online users. We some real facts and figures, we showed that as SNS was vulnerable in the past years, in future also, similar security concerns would exist. The best protection hence could be user’s awareness and knowing the basic guidelines while using such systems.

References

[1] K. Thakur, J. Shan, and A.-S.K. Pathan, “Innovations of Phishing Defense: The Mechanism, Measurement and Defense Strategies,” International Journal of Communication Networks and Information Security, Vol. 10, No. 1, pp. 19-27, April 2018.

[2] A.-S.K. Pathan, The State of the Art in Intrusion Prevention and Detection, ISBN 9781482203516, CRC Press, Taylor & Francis Group, USA, January 2014.

[3] M. Raggo, “Anatomy of a Social Media Attack,” available at: https://www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680 (last accessed: 16 December 2019).

[4] “The Top 20 Valuable Facebook Statistics,” Zephoria Digital Marketing, available at: https://zephoria.com/top-15-valuable-facebook-statistics/ (last accessed: 16 December 2019).

[5] “2019 Top 5 Facebook Video Statistics Infographics,” available at: https://www.everincreasingcircles.com/2019-top-5-facebook-video-statistics-infographics/ (last accessed: 16 December 2019).

[6] W. Luo, J. Liu, J. Liu, and C. Fan, “An Analysis of Security in Social Networks,” 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC’09), 12-14 Dec. 2009, Chengdu, China.

[7] “Internet Security Threat Report 2016,” Symantec, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (last accessed: 16 December 2019)

[8] L. Keating, “Hacking Of Mark Zuckerberg's Social Media Accounts Teaches Us A Big Lesson: Always Choose A Good Password,” available at: https://www.techtimes.com/articles/163422/20160607/hacking-mark-zuckerbergs-social-media-accounts-teaches-big-lesson-always.htm (last accessed: 16 December 2019)

[9] A. Barinka, “Bad Day for Newsweek, Delta Amid Social-Media Hackings,” available at: https://www.bloomberg.com/news/articles/2015-02-10/newsweek-s-twitter-account-briefly-hacked-by-cybercaliphate- (last accessed: 16 December 2019)

[10] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, and C. Gu, “Steganalysis Over Large-Scale Social Networks With High-Order Joint Features and Clustering Ensembles,” IEEE Transactions on Information Forensics and Security, Volume: 11 , Issue: 2 , pp. 344-357, Feb. 2016.

[11] K. Stokes and N. Carlsson, “A peer-to-peer agent community for digital oblivion in online social networks,” Proceedings of the Eleventh Annual International Conference on Privacy, Security and Trust (PST), 10-12 July 2013, Tarragona, Spain.

[12] A. Zigomitros, A. Papageorgiou, and C. Patsakis, “Social network content management through watermarking,” Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications, 25-27 June 2012, Liverpool, UK.

[13] S. Lee and J. Kim, “WarningBird: A Near Real-Time Detection System for Suspicious URLs in Twitter Stream,” IEEE Transactions on Dependable and Secure Computing, Volume: 10, Issue: 3, pp. 183-195, May-June 2013.

[14] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A.H. Wang, “Twitter spammer detection using data stream clustering, Information Sciences,” Volume 260, pp. 64-73, 01 March 2014.

[15] M.M. Joe and B. Ramakrishnan, “Novel authentication procedures for preventing unauthorized access in social networks,” Peer-to-Peer Networking and Applications, Volume 10, pp. 833-843, 2017.

[16] “McAfee Social Protection Facebook Photos App Launches For Android,” available at: https://www.adweek.com/digital/mcafee-social-protection-android/ (last accessed: 16 December 2019)

[17] “Monitor Minor, Ultimate Monitoring Software for Family,” available at: https://www.monitorminor.com/ (last accessed: 16 December 2019)

[18] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, “Security issues in online social networks,” IEEE Internet Computing, Volume: 15, Issue: 4, July-Aug. 2011, pp. 56-63.

[19] E. Novak and Q. Li, “A Survey of Security and Privacy in Online Social Networks,” available at: https://pdfs.semanticscholar.org/f602/caa6f711f573692 46fefa0d608d10bc7e35e.pdf (last accessed: 16 December 2019)

[20] L. Jin, Y. Chen, T. Wang, P. Hui, and A.V. Vasilakos, “Understanding user behavior in online social networks: a survey,” IEEE Communications Magazine, Volume: 51, Issue: 9, pp. 144-150, Sep. 2013.

[21] M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: threats and solutions,” IEEE Communications Surveys & Tutorials, Volume: 16, Issue: 4, Fourth quarter pp. 2019-2036, 2014.

[22] I. Kayes and A. Iamnitchi, “A Survey on Privacy and Security in Online Social Networks,” arXiv preprint arXiv:1504.03342, 2015, available at: https://arxiv.org/abs/1504.03342 (last accessed: 16 December 2019)

[23] S. Deliri and M. Albanese, “Security and privacy issues in social networks,” Data Management in Pervasive Systems, pp. 195-209, 2015.

[24] S. Rathore, P.K. Shamra, V. Loia, Y.-S. Jeong, and J.H. Park, “Social network security: Issues, challenges, threats, and solutions,” Information Sciences, Volume 421, pp. 43-69, December 2017.

[25] “Number of social network users worldwide from 2010 to 2021 (in billions),” Statista Inc., available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (last accessed: 16 December 2019)

[26] K. Ignatiev, “Statistics on Parental Control Alerts for Various Countries,” https://securelist.com/page/107/?calendar=2010-12&chapter=8 (last accessed: 16 December 2019)

[27] M. Peppers, “I was expressing my frustration with the high cost of living in New York: top Lacoste salesman is fired after posting his paycheck on Instagram,” available at: https://www.dailymail.co.uk/femail/article-2385623/I-expressing-frustration-high-cost-living-New-York-Top-Lacoste-salesman-fired-posting-paycheck-Instagram.html (last accessed: 05 December 2019.

[28] L. Smith, “126 Amazing Social Media Statistics and Facts,” Published 13 June, 2019, available at: https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/ (last accessed: 6 December, 2019)

[29] C.B. Moon, J.Y. Lee, D.-S. Kim, and B.M. Kim, “Analysis of Mood Tags for Multimedia Content Recommendation in Social Networks,” 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), 2-5 July 2019, Zagreb, Croatia, Croatia.

[30] H.R. Hasan, K. Salah, “Combating Deepfake Videos Using Blockchainand Smart Contracts,” IEEE Access, Volume 7, 2019, pp. 41596-41606.

[31] W.M. Abduallah, A.M.S. Rahma, and A.-S.K. Pathan, “Mix Column Transform based on Irreducible Polynomial Mathematics for Color Image Steganography: A Novel Approach,” Computers and Electrical Engineering, Volume 40, Issue 4, Elsevier, DOI: 10.1016/j.compeleceng.2014.02.007, pp. 1390-1404, 2014.

[32] A. Haque, A.V. Ayyar, and S. Singh, “A meta data mining framework for botnet analysis, International Journal of Computers and Applications,” Vol. 41, 2019, Taylor & Francis, pp. 392-399, 2019.

[33] V. Natarajan, S. Sheen, and R. Anitha, “Multilevel Analysis to Detect Covert Social Botnet in Multimedia Social Networks,” The Computer Journal, Volume: 58, Issue: 4, pp. 679-687, April 2015.

[34] O.V. Laere, S. Schockaert, and B. Dhoedt, “Georeferencing Flickr resources based on textual meta-data,” Information Sciences, Volume 238, pp. 52-74, 20 July 2013.

[35] N. Ramzan, H. Park, and E. Izquierdo, “Video streaming over P2P networks: Challenges and opportunities,” Signal Processing: Image Communication, Volume 27, Issue 5, pp. 401-411, May 2012.

[36] F.M. Awuor, C.-Y. Wang, and T.-C. Tsai, “Motivating Content Sharing and Trustworthiness in Mobile Social Networks,” IEEE Access, Volume: 6, pp. 28339-28355, 2018.

[37] L. González-Manzano, A.I. González-Tablas, J.M. de Fuentes, and A. Ribagorda, “CooPeD: Co-owned Personal Data management,” Computers & Security, Volume 47, Elsevier, pp. 41-65, November 2014.

[38] F. Ahmed and M. Abulaish, “A generic statistical approach for spam detection in Online Social Networks,” Computer Communications, Volume 36, Issues 10–11, pp. 1120-1129, June 2013.

[39] X. Du, Q. Liu, Z. Li, Z. Qin, and J. Tang, “Cauchy Matrix Factorization for Tag-Based Social Image Retrieval,” IEEE Access, Volume: 7, pp. 132302-132310, 2019.

[40] McGuire, M., “Social Media Platforms and The Cybercrime Economy, Into The Web of Profit,” Bromium, available at: https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf (last accessed: 11 December 2019)

[41] E.D. Frauenstein and S.V. Flowerday, “Social network phishing: Becoming habituated to clicks and ignorant to threats?,” 2016 Information Security for South Africa (ISSA), 17-18 Aug. 2016, Johannesburg, South Africa.

[42] M. Nauman, N. Azam, and J. Yao, “A three-way decision making approach to malware analysis using probabilistic rough sets,” Information Sciences, Volume 374, pp. 193-209, 20 December 2016.

[43] M. Nakerekanti and V.B. Narasimha, “Analysis on Malware Issues in Online Social Networking Sites (SNS),” 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 15-16 March 2019, Coimbatore, India, India

[44] M.R. Faghani and H. Saidi, “Malware propagation in Online Social Networks,” 2009 4th International Conference on Malicious and Unwanted Software (MALWARE), Montreal, QC, Canada, 13-14 Oct. 2009.

[45] I. Yusof and A.-S.K Pathan, “Mitigating Cross-Site Scripting Attacks with a Content Security Policy,” IEEE Computer, Volume: 49, Issue: 3, pp. 56-63, March 2016.

[46] B. Wang, J. Jia, L. Zhang, and N.Z. Gong, “Structure-Based Sybil Detection in Social Networks via Local Rule-Based Propagation,” IEEE Transactions on Network Science and Engineering, Volume: 6, Issue: 3, pp. 523-537, 2019.

[47] S. Shehnepoor, M. Salehi, R. Farahbakhsh, and N. Crespi, “NetSpam: A Network-Based Spam Detection Framework for Reviews in Online Social Media,” IEEE

Transactions on Information Forensics and Security, Volume: 12, Issue: 7, pp. 1585-1595, 2017.

[48] M.R. Faghani and U.T. Nguyen, "A study of clickjacking worm propagation in online social networks," Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), 13-15 Aug. 2014, Redwood City, CA, USA.

[49] K. Ghazinour, S. Matwin, and M. Sokolova, "Monitoring and recommending privacy settings in social networks," Proceedings of the Joint EDBT/ICDT 2013 Workshops, March 18-22, 2013, pp. 164-168.

[50] O. Peled, M. Fire, L. Rokach, and Y. Elovici, "Entity matching in online social networks," 2013 International Conference on Social Computing, 8-14 Sept. 2013, Alexandria, VA, USA.

[51] M. Diomidous, K. Chardalias, A. Magita, P. Koutonias, P. Panagiotopoulou, and J. Mantas, "Social and Psychological Effects of the Internet Use," Acta Informatica Medica, 24(1), pp. 66-68, 2016.

[52] R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Preventing private information inference attacks on social networks," IEEE Transactions on Knowledge and Data Engineering, Volume: 25, Issue: 8, pp. 1849-1862, Aug. 2013.

[53] M.R. Khayyambashi and F.S. Rizi, "An approach for detecting profile cloning in online social networks," 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, 17-18 April 2013, Kish Island, Iran.

[54] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, Volume 22, pp. 113-122, 2015.

[55] H. Dreßing, J. Bailer, A. Anders, H. Wagner, and C. Gallas, "Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims," Cyberpsychology, Behavior, and Social Networking, Volume 17, Number 2, pp. 61-67, 2014.

[56] "Christchurch mosque shootings," available at: https://en.wikipedia.org/wiki/Christchurch_mosque_shootings#cite_note-Gelineau_Gambrell2-6 (last accessed: 26 November 2019)

[57] "Top 10-2017 A5-Broken Access Control," available at: https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control (last accessed: 12 December, 2019)

[58] A.E. Omolara, A. Jantan, O.I. Abiodun, K.V. Dada, H. Arshad, and E. Emmanuel, "A Deception Model Robust to Eavesdropping Over Communication for Social Network Systems," IEEE Access, Volume: 7, pp.100881-100898, 2019.

[59] Y. Bokobza, A. Paradise, G. Rapaport, R. Puzis, B. Shapira, and A. Shabtai, "Leak sinks: The threat of targeted social eavesdropping," 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 25-28 Aug. 2015, Paris, France.

[60] P. Chaudhary, B.B. Gupta, and S. Gupta, "Cross-site scripting (XSS) worms in Online Social Network (OSN): Taxonomy and defensive mechanisms," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 16-18 March 2016, New Delhi, India.

[61] C. Wüest, "The Risks of Social Networking," symantec report, available at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf (last accessed: 12 December, 2019)

[62] K. Thongkor, N. Mettripun, T. Pramoun, and T. Amornraksa, "Image watermarking based on DWT coefficients modification for social networking services," 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 15-17 May 2013, Krabi, Thailand.

[63] N. Singh, T. Sharma, A. Thakral, and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), 22-23 June 2018, Paris, France.

[64] V. Tiwari, "Analysis and detection of fake profile over social network," 2017 International Conference on Computing, Communication and Automation (ICCCA), 5-6 May 2017, Greater Noida, India.

[65] M.A. Wani, N. Agarwal, S. Jabin, and S.Z. Hussin, "Analyzing Real and Fake users in Facebook Network based on Emotions," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 7-11 Jan. 2019, Bengaluru, India, India.

[66] L.N. Antonoff, D.G. Hariyani, J.J. Johnson, K.W. Ong, H. Saliba, and S.J. Matlock, "Systems and Methods For Detection and Removal of Metadata and Hidden Information in Files," US Patent, US7640308B2, Dec. 29, 2009.

[67] B. Greschbach, G. Kreitz, and S. Buchegger, "The devil is in the metadata—new privacy challenges in decentralised online social networks," 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 19-23 March 2012, Lugano, Switzerland.

[68] S. Tayeb, A. Week, J. Yee, M. Carrera, K. Edwards, V. Murray-Garcia, M. Marchello, J. Zhan, and M. Pirouz, "Toward metadata removal to preserve privacy of social media users," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 8-10 Jan. 2018, Las Vegas, NV, USA.

[69] P. Savla and L.D. Martino, "Content analysis of privacy policies for health social networks," 2012 IEEE International Symposium on Policies for Distributed Systems and Networks, 16-18 July 2012, Chapel Hill, NC, USA.

[70] J. Backes, M. Backes, M. Dürmuth, S. Gerling, and S. Lorenz, "X-pire!-a digital expiration date for images in social networks," arXiv preprint, arXiv:1112.2649 (2011), available at: https://arxiv.org/abs/1112.2649 (last accessed: 13 December, 2019)

[71] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity," Information Sciences, Volume 321, pp. 162-178, 10 November 2015.

[72] A.C. Squicciarini, M. Shehab, and J. Wede, "Privacy policies for shared content in social network sites," The VLDB Journal, volume 19, pp. 777–796, 2010.

[73] E. Palomar, L. González-Manzano, A. Alcaide, and Á. Galán, "Implementing a privacy-enhanced attribute-

based credential system for online social networks with co-ownership management," IET Information Security, Volume: 10 , Issue: 2 , 3, pp. 60-68, 2016.

[74] P. Bródka, M. Sobas, and H. Johnson, "Profile Cloning Detection in Social Networks," 2014 European Network Intelligence Conference, 29-30, Wroclaw, Poland, Sept. 2014.

[75] M.A. Devmane and N.K. Rana, "Detection and prevention of Profile Cloning in Online Social Networks," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 9-11 May 2014, Jaipur, India.

[76] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, "PhishAri: Automatic realtime phishing detection on twitter," 2012 eCrime Researchers Summit, 23-24 Oct. 2012, Las Croabas, Puerto Rico.

[77] A.H. Wang, "Don't follow me: Spam detection in Twitter," 2010 International Conference on Security and Cryptography (SECRYPT), 26-28 July 2010, Athens, Greece

[78] W. Wei, F. Xu, C.C. Tan, and Q. Li, "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks," IEEE Transactions on Parallel and Distributed Systems, Volume: 24 , Issue: 12 , pp. 2492-2502, Dec. 2013.

[79] "Facebook Phishing Protector Add-on Issue," available at: http://forums.mozillazine.org/viewtopic.php?f=38&t=3023789 (last accessed: 13 December, 2019)

[80] U.U. Rehman, W.A. Khan, N.A. Saqib, and M. Kaleem, "On Detection and Prevention of Clickjacking Attack for OSNs," 2013 11th International Conference on Frontiers of Information Technology, 16-18 Dec. 2013, Islamabad, Pakistan.

[81] W. Xu, F. Zhang, and S. Zhu, "Toward worm detection in online social networks," Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC'10), December 06-10, 2010, Austin, Texas, USA, pp. 11-20.

[82] "2019 Internet Security Threat Report," Vol. 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf (last accessed: 5 December 2019)