Information Sciences 421 (2017) 43–69

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Social network security: Issues, challenges, threats, and solutions

Shailendra Rathore[a], Pradip Kumar Sharma[a], Vincenzo Loia[b], Young-Sik Jeong[c], Jong Hyuk Park[a,*]

[a] Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Republic of Korea
[b] Department of Management and Innovation Systems, University of Salerno, Italy
[c] Department of Multimedia Engineering, Dongguk University, Seoul 04620, Republic of Korea

ARTICLE INFO

Article history:
Received 5 April 2017
Revised 17 August 2017
Accepted 19 August 2017
Available online 23 August 2017

Keywords:
Social network service
Security and privacy
Multimedia data
Security threats

ABSTRACT

Social networks are very popular in today's world. Millions of people use various forms of social networks as they allow individuals to connect with friends and family, and share private information. However, issues related to maintaining the privacy and security of a user's information can occur, especially when the user's uploaded content is multimedia, such as photos, videos, and audios. Uploaded multimedia content carries information that can be transmitted virally and almost instantaneously within a social networking site and beyond. In this paper, we present a comprehensive survey of different security and privacy threats that target every user of social networking sites. In addition, we separately focus on various threats that arise due to the sharing of multimedia content within a social networking site. We also discuss current state-of- the-art defense solutions that can protect social network users from these threats. We then present future direction and discuss some easy-to-apply response techniques to achieve the goal of a trustworthy and secure social network ecosystem.

1. Introduction

A Social Network Service (SNS) is a kind of web service for establishing a virtual connection between people with similar interests, backgrounds, and activities. A SNS allows its users to find new friends and expand their circle of friends. Data sharing is another key feature of a SNS where users are able to share their interests, videos, photos, activities, and so on. In recent years, SNS such as Twitter and Facebook have become desired media of communication for billions of online users. These services combine user-created profiles with a communication mechanism that enables users to be connected with their friends, families, and colleagues. The prominence of these services is due to the fact that users can update their personal information, interact with other users, and browse other member's profiles. SNSs can be very beneficial for users because they shrink economic and geographical borders. In addition, they can be utilized for achieving goals related to job searching, entertainment, education. However, the popularity of SNSs creates a high risk for their users. The large amount of personal data that users share on SNSs makes them a desirable target for attackers. Attackers can obtain sensitive personal

* Corresponding author.
E-mail addresses: rathoreshailendra@seoultech.ac.kr (S. Rathore), pradip@seoultech.ac.kr (P.K. Sharma), loia@unisa.it (V. Loia), ysjeong2k@gmail.com (Y.-S. Jeong), jhpark1@seoultech.ac.kr, parkjonghyuk1@hotmail.com (J.H. Park).

http://dx.doi.org/10.1016/j.ins.2017.08.063
0020-0255/

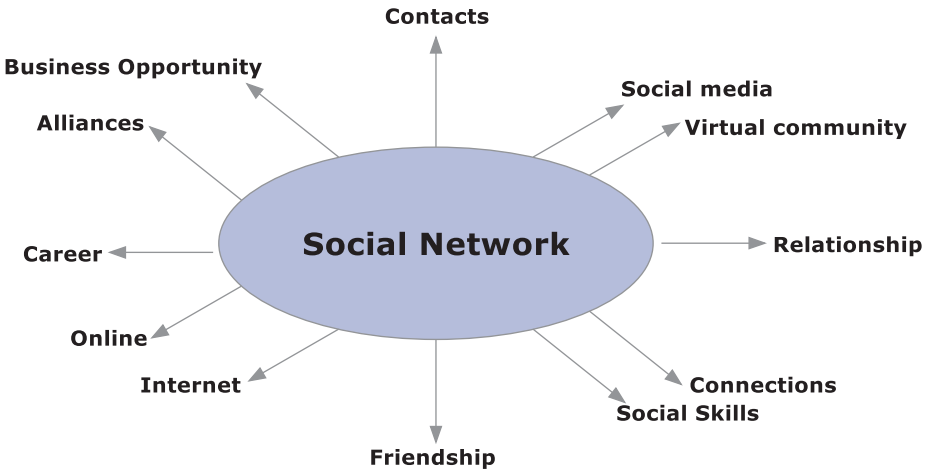

Fig. 1. The fundamental concept of SNSs.

data simply by using a SNS and can carry out many kinds of attacks, such as spam, malware, socialbots, and identity theft. Moreover, attackers can find other significant data, such as bank account information, by analyzing the user's personal data and can commit internet crimes, such as bank fraud. According to an analysis by Raggo [82], SNS attacks can range from account hijacking, fraud, and impersonation attacks to malware distribution. A sophisticated attack can compromise the enterprise networks. The fundamental concept of a SNS is shown in Fig. 1.

In many SNSs, such as Facebook, mainly multimedia data is produced and shared. According to a report from Zephoria Digital Marketing (ZDM) [126], approximately 136,000 photos are uploaded every 60 s on Facebook. A set of statistics from SocialMediaToday [50] show that the average viewing and sharing rate of videos on Facebook is increasing day by day. Currently, approximately 8 billion videos per day are viewed on Facebook, which is double the amount viewed in 2015. Due to the vast amount of multimedia data available on Facebook, security risks are also increasing. A malicious user can share malicious information on a SNS by concealing it within multimedia data. Moreover, by doing so, an attacker can easily find the user's important information, such as user identity and location [91].

Some SNSs, like Twitter, do not allow users to disclose significant private information, but attackers can infer the sequence of a user's posted content on a SNS and can reveal their undisclosed private information. In 2005, MySpace was attacked by the Sammy worm, which exploited the vulnerabilities in MySpace and transmitted very quickly. It did not steal users' personal information, but it still had a dangerous effect on MySpace's general operations. In April 2009, Twitter was attacked by the Mikeyy worm, which also did not steal users' personal information, but instead replaced their data with some unusable data. In May 2009, Facebook was attacked by the Koobface worm, which stole significant information, such as a user's password [121].

The Internet Security Threat Report (ISTR) [113] stated that the increasing use of SNSs by hackers cannot be ignored. In 2015, such services turned into a source for spam and malware, and were utilized as a way of making illegal money on the web. Recently, Facebook CEO Mark Zuckerberg's Pinterest and Twitter accounts were hacked, where the hacker used his LinkedIn password of "dadada." [67]. Similarly, attackers infiltrated the SNS accounts of Delta Air Lines Inc. and Newsweek by posting fake messages [2]. After conducting an analysis of the aforementioned attack statistics, we concluded that SNSs are the best way for an attacker to commit cybercrimes.

With the increasing amount of traditional threats and threats due to multimedia data in SNSs, many researchers and security corporations have proposed various solutions to mitigate these threats. Such solutions include watermarking [13], steganalysis [26], and digital oblivion [62] for protecting SNS users against threats due to multimedia data. On the other hand, various solutions, such as spam detection [127] and phishing detection [103], have been proposed to mitigate traditional threats. However, many built-in security solutions, such as authentication mechanisms [78] and privacy settings [54], and commercial solutions, such as minor monitor [43] and social protection application [71], also serve as safeguards against both types of threats in SNSs.

Many security researchers have studied and discussed the security issues in SNSs. Gao et al.'s research [38] categorized major security issues in SNSs into four categories: (a) Privacy issues, (b) Viral marketing, (c) Network structural-based attacks, and (d) Malware attacks. Their research included an in-depth discussion on each issue and the corresponding defense mechanisms. Novak et al. [23] surveyed the major security and privacy issues in SNSs. They discussed the existing techniques that protect SNS users against various entities, such as SNS providers, third party application developers, advertisers, and other users. They also provided a clear overview of the SNS inference of link prediction, location hubs, and user attributes. Jin et al. [66] studied user behavior in SNSs from four viewpoints: (a) malicious behavior, (b) mobile social behavior, (c) traffic activity, and (d) connection and interaction. They discussed the major challenges and motivations of user behaviors and provided a review on existing schemes for SNS security. Fire et al.'s research [74] presented a comprehensive survey of

Table 1
Contribution of our study related with existing surveys.

Research work	Year	Security issues and challenge	Security threats	Multimedia content threats	Existing SNSs security solutions	Discussion and security suggestions
Gao et al. [38]	2011	Yes	Limited	No	Yes	Limited
Novak et al. [23]	2012	Yes	Limited	Limited	Yes	Limited
Jin et al. [66]	2013	Limited	Limited	No	Limited	Limited
Fire et al. [74]	2014	No	Yes	No	Yes	Yes
Kayes et al. [42]	2015	Limited	Yes	No	Yes	Limited
Deliri et al. [101]	2015	No	Limited	No	Limited	No

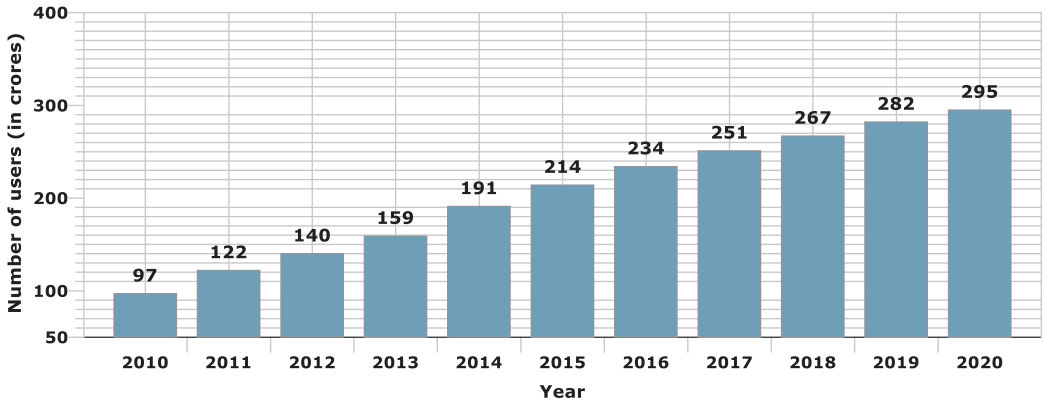

Fig. 2. Number of SNSs user worldwide from 2010 to 2016 with prediction until 2020.

various privacy and security threats in SNSs. They mainly divided the latest security threats into four categories: (a) classic threats, (b) modern threats, (c) combination threats, and (d) threats targeting children. They also provided a high-level taxonomy of existing solutions that can protect SNS users against these threats. Kayes et al.'s research [42] described the taxonomy of traditional security and privacy attacks in SNSs based on social network stakeholders. They categorized various attacks as attacks on SNS infrastructure and attacks on SNS users. They also discussed existing defense mechanisms for mitigating these types of attacks and the challenges that comes with using these mechanisms. Deliri et al. [101] studied the most common attacks in SNSs, including sybil, malware, phishing, and identity theft attacks. They also proposed some countermeasures for mitigating these attacks.

Other studies [23,38,42,66,74,101] have focused on traditional security threats in SNSs and not on security threats that occur due to multimedia data. In this paper, we examine the traditional security threats and the security threats that occur due to multimedia data in SNSs. We also discuss possible solutions for mitigating these threats. Table 1 provides a comparison of the several existing studies in terms of security issues, challenges, threats, discussions, security suggestions, and existing defensive solutions. Our study differs significantly from other existing studies in terms providing an integrated discussion, extensiveness, and comprehensiveness. In addition, it provides a high-level taxonomy of the most recent security solutions.

Besides concentrating on specific SNS threats, we also focus on providing a comprehensive view of various recent SNS security threats, such as ones that target minors and huge organizations. The major goal of our study is to achieve a trustworthy, efficient, and secure SNS ecosystem. The high level description of SNS threats and their solutions provide a quick understanding of basic SNS security concepts and perspectives. Our analysis of several topics provides the means to discuss open issues and challenges, and consider more factors related to enhancing security in SNSs. We analyzed which security issues need to be addressed and identified opportunities for future research work.

This paper is organized as follows; Section 2 describes various security issues and challenges in SNSs. Section 3 provides classification and description of various SNS security threats. In Section 4, we discuss several possible and existing solutions for SNS security. The future direction and some easy-to-apply response techniques are presented in Section 5. Finally, we conclude our research in Section 6.

2. SNS security issues and challenges

In recent years, SNSs have become a popular medium of communication. The number of SNS users worldwide is continuously increasing every year. Statista's report [110] provided the quantity of SNS users globally from 2010 to 2016 with predictions until 2020, which is shown in Fig. 2. This escalation in the number of SNS users has also resulted in a tremen-

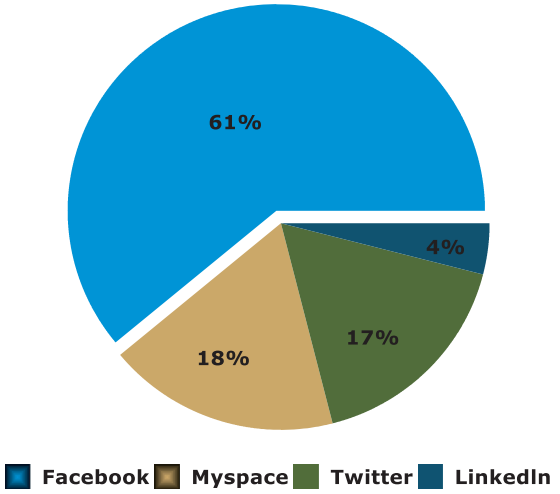

Fig. 3. Sophos security threat report- 2011.

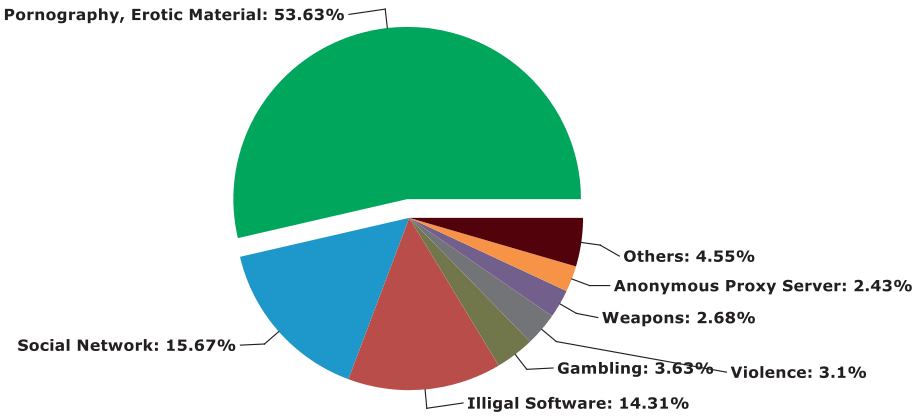

Fig. 4. Analysis of parental control component triggered by various real world security risks.

dous increase in security vulnerabilities, which affect a user's confidentiality, authenticity, and privacy. Various security organizations have released different statistics and reports on SNS security.

According to Sophos' security threat report 2011 [106], Facebook has 0.5 billion users. This report reveals that Facebook has the biggest security risks that are significantly ahead of MySpace, Twitter, and LinkedIn, as shown in Fig. 3. It is the most popular site for active users on the web. Due to this popularity, a large amount of users are targeted by adversaries via various types of attacks, such as malware, phishing, spamming, and more. These attacks are continually proliferating.

Furthermore, the Kaspersky Security Network (KSN) [59] has described a parental control component that supports parents in precaution their kids from the concealed risks of abandoned use of computers and the internet. A worldwide analysis of this component with various real world security risks demonstrates that it is prompted most often by social network risks, as shown in Fig. 4. This indicates that SNSs act as an escalating noticeable role in kids' lives and parents are increasingly worried that their children are more vulnerable to security risks with the use of SNSs.

According to the internet security threat report [113], SNSs have become the favorite target of scammers in the past few years. They use various scamming techniques to scam SNSs users via the usage of manual sharing; fake offerings, like jacking; fake applications; and fake plugins. However, manual sharing is being used more widely in recent years. Fig. 5 shows the percentage utilization of each scamming technique for the last three years [113].

Some significant features of SNSs, such as sharing pictures, commenting, tagging, and blogging, make them a significant part of the daily lives of billions of web users, who as a result are exposing themselves to several kinds of privacy and security issues. These security and privacy issues are as described below.

2.1. Internet threats

Users share a huge amount of personal data on SNSs, and this data might reveal them to various internet threats, such as identity theft, spamming, phishing, online predators, internet fraud, and other cybercriminal attacks. As reported in the

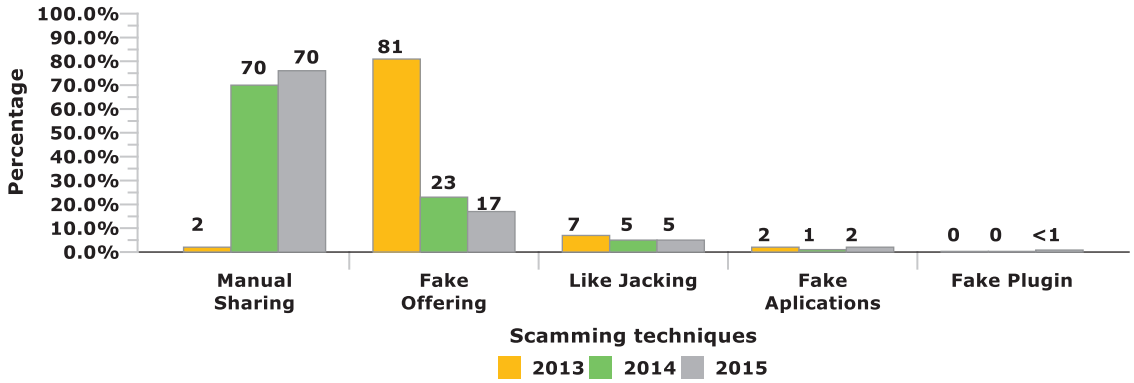

Fig. 5. The percentage utilization of various SNSs scamming techniques for last three years.

internet security threat report 2016 [113], SNSs have become the most promising target of attackers for identity theft. In this type of attack, an attacker exploit a user's confidential data, such as his or her social security number, full name, telephone number, and address, without his or her permission, for conducting cybercrimes, such as a theft or scam. Presently, the default privacy features of many SNSs, which set whole user's personal information to be accessible to everybody. Due to this, an attacker can simply access data about the user's friends and then pretend to be mutual a trustworthy friend. Moreover, an attacker can persuade the user to demand additional commercial and sensitive information. Besides identity theft, the trend of spear phishing attack in SNSs was initiated in 2007 [114]. In this attack, adversaries try to obtain a user's financial information by using private data that he or she shared on their SNS. Adversaries may also break into the SNS accounts of famous celebrities and then utilize these accounts to interact with their friends. Furthermore, the usage of third party applications in SNSs also acts as a great security threat. For example, many SNSs, such as Facebook, provide game applications to its users. These applications require the user's credit card details; personal information, such as phone number; and email ID for completing the registration process. A user providing his or her telephone number and credit card details may increase the risk of identity theft and spear phishing, or this can damage the user's reputation if the applications distract from its claimed objective.

2.2. Reputation and credibility issues

Reputation is a type of communal assessment by a community of an individual, an association, or a group of people. It plays a vital role in many areas, such as corporate, social status, online groups. As numerous people rely on SNSs for recording their life and for keeping in touch with their friends. In addition, SNSs can be used for sharing views, videos, and images beyond a user's circle of friends. With this high utilization of SNSs, online reputation of users is also accelerated over web. Subsequently, reputation of users also influences user's status and credibility in actual life. SNSs can damage the reputation of businesses and huge organizations, where if a single thoughtless message is posted by any employee of the company this can damage the reputation of the employee and the company. There are a number of incidents that demonstrate how SNSs can affect their users' reputations. For instance, in December 2013, an employee of Lacoste was fired from his job due to posting his paycheck on Instagram [81]. Other examples of how SNSs can harm an organization's reputation include the backlash by the employees of British entertainment retailer, HMV, on Twitter [52].

Furthermore, several companies use SNSs for hiring good workers and many job seekers update their personal information on SNS sites. This updated information might be exploited by adversaries due to the lack of SNS security measures. Moreover, users may lose their job chances due to incorrect data in their SNS profile. According to the latest study by CareerBuilder [16], 60% of recruiters use SNSs to research desired candidates or employees. SNSs not only affect the status and credibility of its users, but can sometimes create big problems for them. For instance, a teacher's aide at a Georgia elementary school was sacked for posting a racist tirade about Michelle Obama on Facebook [58].

2.3. Profiling issues

Many companies gather data from a variety of third party resources, such as SNS, for constructing complete profiles of individuals with the intention of selling products and individual's behavior recording. All of this is typically accomplished without the individual's permission. In addition, to continue SNS services, SNS providers also need to fight with making money via advertising or marketing. According to a recent survey by Smith [61], 38% of companies spent more than 20% of their advertising budgets on SNSs in 2015, and Facebook and Twitter display the most ads. This statistic demonstrates that sellers are keen to utilize rapidly increasing SNSs for advertising and promoting their goods. Many SNSs have constructed a complex network of advertising instead of social relationship. Even though, gathering freely available SNSs user's information is not banned, SNS users are not able to determine how their shared information will be used. For example, a user's

information may be vended to a government authority for the purpose of law enforcement or may be used by sellers for marketing. This collected information may influence users as SNS profiles contain a huge volume of a user's private data, such as his or her daily preferences, health information, shopping preferences, social security number, and so on.

3. Security threats in SNS

Nowadays, the Utilization of SNSs is increasing rapidly worldwide. SNSs such as Facebook, Flickr allow billions of users to share their personal information and multimedia data with friends, relatives and other online users. User's information, including multimedia data is being captured and illegally used by malicious users and third party organizations for escalating their revenue. There are many security threats in SNSs which put user's shared data at risks. These threats can be classified into three major categories. The first category includes *multimedia content threats* in which multimedia data shared on SNSs are used to expose SNSs users. The second category covers *traditional threats* in which traditional attack techniques or weaknesses of SNSs infrastructure are used to attack on SNSs users. The third category includes *social threats* in which attackers establish social relationship with SNSs users to jeopardize them. This Section discusses the security state of SNSs thoroughly by describing all three aforementioned categories of threats. Each subsection of this section represents a category of security threats as shown in Fig. 6. Moreover, each subsection is further divided into certain topics that group security threats common in some property.

3.1. Multimedia content threats

Data sharing is an important feature in SNSs, where users are able to share their photos, videos, activities, interests, and so on. One of the vital components of this type of data sharing is multimedia data. Modern SNSs permit their users to share high-resolution videos and images. However, the advancement in multimedia retrieval techniques, such as location estimation, face recognition, web searches, and geotagging, can increase the chances of these items being illegally utilized. For instance, a shared picture can reveal a user's location via the usage of geotagging. In this subsection, we describe various multimedia threats that can be used by an attacker to obtain a user's sensitive information from their multimedia data that they share on a SNS.

3.1.1. Multimedia content exposure

Users are typically cautious when revealing their textual data over SNS. Hence, very few users upload their IDs and home address. However, they are not as aware when it comes to posting multimedia data, which also discloses an enormous amount of sensitive information. For example, if a user posts pictures of his or her home, an intruder can find the user's home address by using these. Another case would be where a user updates his or her status on SNS indicating that he or she is away not at home (for example, on vacation, at a bar or a concert), which implies that the home is open to the intruder. A shared picture from a recent activity can show the present location of the user and how long he or she will not be at home, which provides extra benefits to the intruders. Users also have to be cautious that intruders might scan uploaded photos for valuable assets or objects. Therefore, valuables depicted in a video or photo can result in unsolicited attention from intruders. Another type of information disclosure involves the user sharing a photo that contains other people without their permission, which may violate their privacy. A number of recently developed techniques, such as face and speech recognition, can reveal several people without their permission or their being notified [88]. User information can be easily obtained from shared multimedia content and a lot of a user's personal information can be inferred, as illustrated in [77].

3.1.2. Shared ownership

Shared multimedia data onto SNS may relate to multiple users [65]. For instance, two friends might take a photo together at an event and either of them could upload the photo onto SNS with his or her privacy settings and without the consent of the other. This may expose the privacy of other friend because such a photo belongs to both friends. Since only one user can decide upon his or her preferred privacy settings for the multimedia data that belongs to multiple users, it could be shared with the preferred privacy settings that are selected by one of the users. The preferred privacy settings are not selected by the intersection of each individual user's privacy settings, which would be reasonable.

3.1.3. Manipulation of multimedia content

SNSs provide a platform to their users where they can share a lot of multimedia data, and this data might be malleable and distorted by untrustworthy users [9]. Nowadays, there are a number of tools available for distorting multimedia data such as [105]. By using these tools, a malicious user can tamper the personal pictures of legitimate users to harm or ridicule them.

3.1.4. Steganography

This is the practice of hiding data within other media in order to conceal it. With the growing technology and science, the steganography has become very popular and has many legitimate applications. Viejo et al.'s research [12] described a clear phenomenon of secret communication between users in which they hide their messages within uploaded images in SNSs. This phenomenon shows that not only is steganography possible in SNSs, but that the overhead is also affordable.

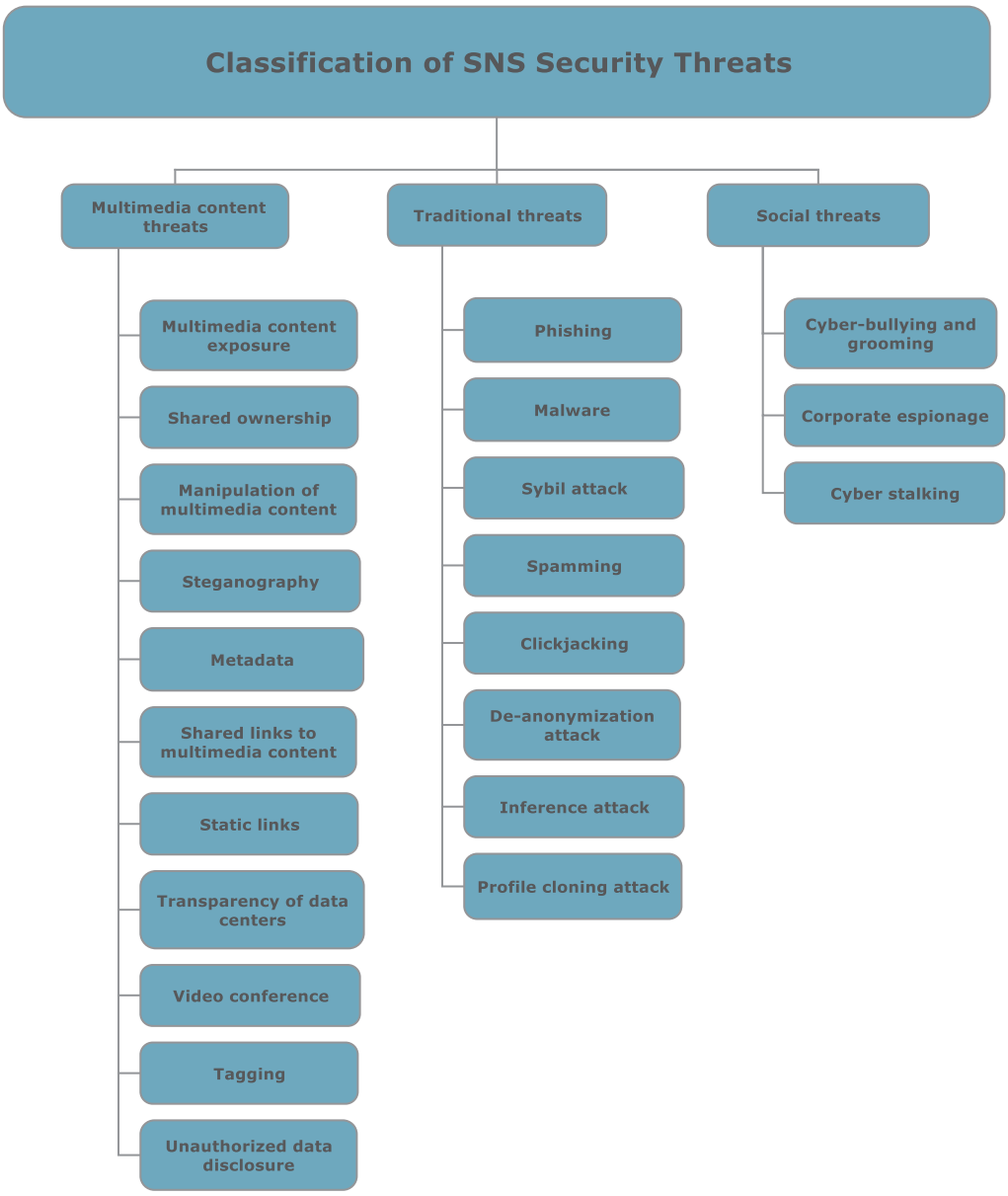

Fig. 6. Classification of SNSs security threats.

However, it can be maliciously used within SNSs due to its capability of covering malicious activities. A malicious user can share malicious information by concealing it within multimedia data. This types of behavior can jeopardize the reputation of SNSs. Moreover, it can affect legitimate users and associate them with crimes that they did not actually commit. For instance, a picture with embedded malicious messages might be shared by a malicious user within SNSs and a legitimate user might download this picture without being aware that it contains a maliciously embedded object.

3.1.5. Metadata

This is a type of data that contains and delivers information about other data. In SNSs, multimedia contents act as metadata because these contents might contain enormous amounts of other valuable data, such as IDs and location. While this might be valuable for the user, it also might expose the user to attacks if it is disclosed. One type of multimedia metadata that could reveal users are geo-location tags. Several of the latest mobile phones insert the GPS (Global Positioning System) coordinates in the clicked pictures, which disclose the location information of the user. The location of the user might further reveal other information about him or her, such as religious or political beliefs, medical condition(s), and much more. Moreover, geotagged pictures might result in human casualties, as described in [46]. In many cases, picture

metadata may disclose information about the picture's owner and camera that they used. Each SNS manages multimedia metadata in a different way. For instance, Facebook removes all metadata before uploading the picture, while Google+ retains all metadata except for the GPS coordinates. Flickr shares the GPS coordinates in an image by default for showing the pictures of other users at the same location [93].

3.1.6. Shared links to multimedia content

Due to the extensive variety of multimedia formats, such as JPEG and PNG, it is very difficult for one framework to support all formats. Moreover, many of these might be susceptible to different types of attacks, or they might have data that requires manual checking (i.e., interactive flash videos). Usually, SNSs do not support all multimedia formats and users cannot share an arbitrary multimedia file in any format. For example, a user can only share a picture on Facebook as a JPEG or PNG. It does not widely support GIFs, as they are animated. However, SNSs provide a feature in which users can share multimedia content in an unsupported format by posting a link to the content. A malicious user can exploit this feature and replace the link's associated content with external malicious content. Unfortunately, a legitimate user may access this link and redirect to the external malicious content. The malicious content may result in malicious codes being installed on the user's computer or in their being redirected to a malicious website that tries to steal their confidential information [103].

3.1.7. Static links

Generally, most SNS users use static links to share multimedia data, which is because these links provide an efficient and optimal way for data to be distributed. However, sharing the static link can affect the privacy of users and create the possibility for many attacks to take place [15]. When a user shares the static link of a picture with a group of selected users, every member of the group has access to the picture and can share it without the permission of the picture's owner. A member can also copy and paste the link in order to share the picture outside of the SNS. Another major issue with sharing a static link is that in many SNSs, it may still continue to exist for many days even after the content associated with the link has been deleted. A network administrator can benefit from this issue and can easily see what users are browsing, as the content associated with the link is available in his or her log files.

3.1.8. Outsourcing and transparency of data centers

The transparency of stored media is a major issue that can affect the privacy of SNS users in two ways. First, the multimedia data stored in a SNS is not encrypted. Therefore, if a malicious user has a direct link to this data, he or she can access it without going through an authorization process. Second, the data stored in a SNS can be viewed by the service provider. Larger SNSs, such as LinkedIn or Facebook, have their own personal data centers. However, small SNSs do not have these, and so they store their data in third party storage, such as a cloud-based data center. This third-party storage decreases maintenance costs and scalability. Nevertheless, many privacy and security concerns might be possible [109]. The end-users might trust a SNS, but it is difficult to trust a third-party service provider that has access to their data. The user's data may be distributed to a government authority for the purpose of law enforcement or used by merchants for marketing.

3.1.9. Video conference

Nowadays, many SNSs support both chat and video conferencing services, as video conferencing can provide more interaction between users. However, with this, more information can be disclosed. A malicious user can intercept the broadcast video stream by exploiting the possible vulnerabilities in the underlying communication architecture [89]. Moreover, one of the participants of the video conference can easily record the conference to blackmail the other participant (victim) or to distort the conference data and display it accordingly. The malicious user can arbitrarily access the webcam of the victim by using malware and by taking advantage of the vulnerabilities of the communication protocols.

3.1.10. Tagging- link ability from shared multimedia data

SNSs provide a tagging feature within shared multimedia data to increase interactions among users and to enable additional fine-grained search capabilities. A user can tag videos and pictures that he or she finds suitable and link them with some additional information. However, this tagging feature could introduce some privacy risks for end users. For instance, there are many SNS users who do not want to upload any pictures of themselves on any SNS site. However, someone in their friends list can share their picture via tagging and visually identify them [4]. The main issue is that tagging can link someone who does not belong to any SNS and does not want to share any of their personal information with a SNS [65]. Also, a spammer or malicious user can tag large number of users in a single post, such as a picture or video, in order to spread the malicious content to a large audience with little effort [25].

3.1.11. Unauthorized data disclosure

Many SNSs provide a data sharing facility to their users. Generally, data sharing means revealing the data to a definite set of users. When a user shares text data with a group of users it might be that a member of the group reveals the data [47]. Usually, this type of disclosure is not considered to be legal because it can be manipulated. Similarly, multimedia data is also malleable, when a user shares a picture with a certain group of users, any member of the group can download it and re-upload with his or her new privacy settings. Thus, a picture that the primary uploader only wants to share with a select group of people may end up being publicly shared.

3.2. Traditional threats

Traditional threats are unique to the SNS environment and include various traditional attack techniques, such as phishing, malware, to obtain a user's personal information. This information is very beneficial for an attacker, as he or she can gather other confidential information, such as a user's social security number, login password, and bank account details. Once an attacker obtains this information, he or she can commit other crimes and serious attacks, such as phishing and identity theft. In this section, we describe various traditional threats that can be used by attackers to gain a user's personal information.

3.2.1. Phishing

This is where attackers use fake websites and emails to expose a user's sensitive private information. They attempt to create an identical false copy of an original website. According to a report by SECURELIST [115], the anti-phishing system of Kaspersky lab detected 30,807,071 phishing threats in the second quarter of 2015 and 509,905 signatures of phishing URLs were submitted to the lab databases over this period. Attackers can also use SNSs to carry out a phishing attack. In this case, an attacker first collects a user's personal information from SNSs and based on this he or she sends a fake message, which looks legitimate, to the user via SNS. This fabricated message can contain an attacker's demands, such as the user's credit card number, password, and more. When the user receives this type of message, he or she will think that it is from legitimate user or a friend, and accesses the message and provides the sensitive information as attacker want through the message. When it comes to a SNS, the attacker needs to bring the victim to a fake page in order to launch a phishing attack. To do so, the attacker can use different techniques, such as sharing a phishing page URL with an attractive title and picture. For example, a user might receive a post on his or her Facebook wall with content like "Click here to see leaked naked pictures of X." (Here "X" is the name of a famous actor or singer.) By clicking on this post, the user may end up being redirected to a phishing website.

3.2.2. Malware

This is a malicious program that consists of Trojan horses, viruses, and worms. Generally, SNSs work upon the connections of different user's systems. Therefore, malware can simply transfer between different users' systems via these connections [80]. Many SNSs do not have the proper mechanism to determine whether a URL is malicious or not. A malicious URL can redirect the user to fake websites, and, later, transmit malware to user's computer in order to steal his or her confidential data. Faghani et al. [83] analyzed the malware propagation in SNSs and identified the parameters which are responsible for malware propagation. The parameters involve various characteristics of social network graph, such as number of vertices, number of edges, maximum degree, average shortest path, longest path. The authors also described the impact of each parameter on the speed of malware propagation in SNSs.

3.2.3. Sybil attack and fake profile

With this type of attack, attackers create a huge amount of fake identities that help them to achieve major benefits in the distributed system and peer-to-peer system. A Sybil attack is a major problem for SNS security because it contains a large number of users who are connected as peers communicating in a peer-to-peer network, which means that one online entity can manage and handle several fake identities in a SNS. By operating these fake identities, attackers can outvote the legitimate users like Byzantine failure defenses. For instance, an attacker can boost the reputation and popularity of an SNS account by voting it as being the "best". A Sybil attack can reduce reputation values, corrupt information, and outvote legal SNS users [31].

3.2.4. Spamming

In a spamming attack, attackers send unsolicited messages (spam) in bulk to internet users. This type of attack appears to be more successful in SNS compared to traditional spamming attack where email is used to spread spam. This is due to the social relationships that exist between users in SNS, which means that it is easy to persuade the targeted user to read junk data and trust it to be safe. Spam can range from advertising to phishing messages. According to a report from Nexgate [87], YouTube and Facebook deliver the most spam content out of all SNSs at a ratio of 100:1.

3.2.5. Clickjacking

This is an emerging threat to SNSs where attackers hide malicious applications behind the sensitive user's interfaces or buttons to steal the clicks of users and use them for malicious purposes. Clickjacking has variations, but the most popular are Likejacking and Cursorjacking. In Likejacking, an attacker associates malicious codes scripts with Facebook's "Like" button, which appears on the user's profile. Cursorjacking uses the user interface redressing technique to alter the location of the cursor, where the attacker swaps the actual cursor with a bogus one to redirect the user to a malicious website [84].

3.2.6. De-anonymization attack

In several SNSs, like Facebook and Twitter, users can safeguard their anonymity and privacy by using an alias or false name. The de-anonymization attack uses different methods, such as user group membership, network topology, and tracking cookies, to disclose the user's true identity. This attack is also possible in SNSs where a third party can find the user's identity by linking the information that the user has disclosed in a SNS. Many researchers have proposed techniques that

can be used by an attacker for performing this type of attack in a SNS. Ghazinouret al. [53] demonstrated that an attacker can expose a user's identity by using tracking methods, such as tracking cookies. Wondracek et al.'s research [33] presented a new de-anonymization attack method where an attacker can exploit the group membership information in SNSs to discover users' true identities. They empirically evaluated their method on the Xing SNS and successfully identified 42% of users. Moreover, Peled et al. [92] proposed an algorithm for matching user profiles across multiple SNSs and discovering the users' identities. The effectiveness of their proposed algorithm was tested on Xing and Facebook.

3.2.7. Inference attack

This is where an attacker infers a user's private information by exploiting other information that has been published about the user on SNS. An attacker can carry this out by using data mining techniques on publicly available SNS data, such as data from a user's friends list and network topology. Mislove et al. [10] proposed methods for estimating a SNS user's attributes by exploiting another user's attributes. They evaluated their methods on Facebook and collected different users' attributes, such as geographical information, personal preferences, and educational information. Fire et al.'s research [75] presented an algorithm for carrying out an inference attack on organizations. It infers the social relationships between the employees of organizations by using employee data that is publicly available on popular SNSs, such as LinkedIn and Facebook. This algorithm demonstrates that an attacker can use SNSs for finding the internal secret information of organizations and can successfully perform an inference attack. Heatherly et al. [97] proposed a method for predicting a user's undisclosed private information by exploiting released SNS data. They also suggested three sanitization approaches to prevent inference attacks and the unauthorized disclosure of private information using released SNS datasets.

3.2.8. Profile cloning attack

In this attack, an attacker clones a pre-existing user profile either in the same SNS or a different one. By using this cloned profile, the attacker can send friend requests to the contacts of the real user and form a trusting relationship with the user's friends. The attacker might exploit this in order to gather sensitive and private information about the user's friends or to commit several types of internet scams, such as cyber bullying, cyber stalking, and blackmail. The attacker can use the images and other personal information of the real user's profile to create this cloned profile [99].

3.3. Social threats

When it comes to online social threats, attackers can maliciously exploit the social relationship feature of a SNS and interact in various ways with different kinds of users, such as minors and the employees of a corporation. For instance, an attacker can attract minors through expressing sympathy, love, and care, or offering online gifts, cash, etc. Their motivations for using doing so include blackmail, sharing pornography, engaging in cyber harassment, and spying. In this section, we describe various social threats that exploit different online social relationships for a variety of reasons.

3.3.1. Cyberbullying and cyber-grooming

Cyberbullying is the deliberate and repetitive online harassing or harming of someone. Cyber-grooming is when an adult tries to establish an online, emotional connection with a child in order to sexually abuse them. Minors are highly susceptible to these types of online predators and attacks due to their vulnerable age [72]. Cyberbullying can cause depression in teenagers. Online predators might attempt to lure a teenager through expressing sympathy, love, and care, or by spending a significant amount of time online and offering online gifts, cash, and more. Many security experts believe that online predators have attempted fraud on thousands of academic students around the world. One of the most dangerous cyberbullying crimes was the Megan Meier case, which led to the a teenage girl committing suicide. In this case, the criminal succeed in creating a fake profile that they also used in another cyber-grooming crime [5].

3.3.2. Corporate espionage

A corporate espionage can perform automated social engineering attacks using SNSs. A social engineer can gather valuable information, such as an employee's position within a company, email addresses, full names, etc., by using SNSs instead of classic social engineering approaches and infiltrating an organization. Krombholz et al.'s research [56] described social engineering attack by using SNSs. The authors showed that the information of an employee in a given target organization can be gathered from SNSs in an automated manner and significantly exploited for automated social engineering attack.

3.3.3. Cyberstalking

A SNS user can disclose their personal information, such as their phone number, home address, location, and schedule, in their SNS profile. This information can be exploited by malicious users for cyberstalking. For instance, a malicious user can blackmail his or her victim through making phone calls or sending instant messages via a SNS. Moreover, users frequently reveal location-based information through their images and attackers can gather this information, which they can abuse and use to carry out dangerous cyberstalking attacks. Dreßing et al. [35] studied the impact cyberstalking attack on users of the German SNS, StudiVZ. The authors stated that cyberstalking impacts the mental health of the SNSs users and should be taken as a serious threat to provide a secure SNS ecosystem.

Table 2
Summary of SNSs security threats, description, impacts and related studies.

Category	Type of threats	Description	Impacts	References
Multimedia content threats	Multimedia content exposure	Shared multimedia data on SNSs can directly disclose enormous amount of user's sensitive information such as user's home address, recent activities.	Information disclosure, Reputation loss, Location leakage, Cyber harassment, Profiling, Safety loss.	[77,88]
	Shared ownership	Multimedia data shared in SNS may relate to multiple users and only one user can decide the preferred privacy settings for the multimedia data.	Content ownership loss.	[65]
	Manipulation of multimedia content	In SNSs, a malicious user can tamper the personal pictures of legitimate users to harm or ridicule them.	Reputation loss, Extortion/Blackmailing, Cyber harassment.	[9,105]
	Steganography	A malicious user can share malicious information by concealing it within multimedia data such as picture.	Reputation loss, Information disclosure, Safety loss.	[12]
	Metadata	Multimedia contents act as a metadata because these contents may reveal other valuable data such as IDs, location.	Information disclosure, Location leakage, Reputation loss, Cyber stalking, Profiling, Safety loss.	[46,93]
	Shared links to multimedia content	SNSs provide a feature in which users can share multimedia content in unsupported format such as GIFs format by posting a link to the content. A malicious user can exploit this feature and can replace the link's associated content with the external malicious content.	Reputation loss, Information disclosure, Account loss.	[103]
	Static links	Most of the users in SNSs use static links to share the multimedia data. A malicious user can easily copy and paste the static link to share the multimedia data beyond the SNSs.	Multimedia data disclosure, Data ownership loss.	[15]
	Outsourcing and transparency of data centers	The multimedia data stored in the SNSs is not encrypted. Therefore, a malicious user can access the data without going through any authorization process. Moreover, small SNSs store their data in third party storage such as cloud-based data center. Many privacy and security concerns might be possible.	Multimedia data disclosure, Profiling, Data ownership loss.	[109]
	Video conference	The malicious user may intercept the broadcast video stream by exploiting the possible vulnerabilities in underlying communication architecture.	Reputation loss, Information disclosure, Blackmailing, Cyberbullying, and Cyber stalking.	[89]
	Tagging	Tagging may link the people with SNSs who are not the members of any SNSs and do not want to share any of their personal information.	Multimedia data disclosure, Location leakage, Reputation loss, Cyberbullying, Cyber stalking.	[4,25,65]
	Unauthorized data disclosure	In SNSs, a user can share picture to a certain group of users. Unfortunately, any member of the group may download the shared picture and re-upload with his new privacy settings. Thus, a picture may simply be exposed to public.	Reputation loss, Information disclosure, Location leakage, Content ownership loss, Identity theft, Extortion/Blackmailing, Cyber stalking, Profiling, Safety loss.	[47]
Traditional threats	Phishing	In SNSs, attacker needs to bring the victim to a fake page for launching phishing attack. For bringing victim to the fake page, attacker can use different techniques such as sharing phishing page URL with an attractive title and picture on SNSs.	Confidential information disclosure, Account loss, Pornography, Cyber stalking.	[115]
	Malware	Many SNSs do not have proper mechanisms to determine whether a URL is malicious or not. The malicious URLs can redirect the user to fake websites, and later, transmit malware to user's computer for stealing confidential data of user.	Confidential information disclosure, Account loss, Data ownership loss, Reputation loss.	[80,83]

(*continued on next page*)

Table 2 (*continued*)

Category	Type of threats	Description	Impacts	References
	Sybil attack and fake profile	Malicious users can manage and handle several fake identities in SNSs. By operating these fake identities, they can outvote the legitimate users.	Outvote the legitimate users, Reputation loss, Corrupt user's information, Extortion/Blackmailing, Pornography, Cyber harassment.	[31]
	Spamming	In SNSs, Attackers can send unsolicited messages (spam) in a bulk amount to the SNSs users.	Reputation loss, Account loss.	[87]
	Clickjacking	Attackers hide malicious applications behind the sensitive user's interfaces or buttons to steal the clicks of users and use them for the malicious purposes.	Reputation loss, Data disclosure, Click stolen, Decrease user's experience.	[84]
	De-anonymization attack	Attackers use the methods such as user group memberships, network topologies, tracking cookies to disclose the user's real identity in SNSs.	Identity disclosure, Relationship disclosure, Reputation loss, Profiling.	[33,53,92]
	Inference attack	An attacker infers user's private information by exploiting other published information about the user on SNSs.	Private information leakage, Location leakage, Identity disclosure, Relationship disclosure, Reputation loss, Profiling.	[10,75,97]
	Profile Cloning attack	Attacker clones an already existing user's profile to gather sensitive private information about the user's friends or to commit several types of internet scam.	Reputation loss, Sensitive information leakage, Cyberbullying, Cyber stalking, Extortion/Blackmailing, Account loss, Cyber harassment.	[99]
Social threats	Cyber-bullying and grooming	Adults try to establish an emotional connection with children through the internet for abusing them sexually.	Reputation loss, Cyber stalking, Account loss, Extortion/Blackmailing, Cyber harassment, Teen depression, Pornography, Safety loss.	[5,72]
	Corporate espionage	A social engineer can gather precious information such as employee's position within the company, email addresses, full name, and many more about company employees by using SNSs and can infiltrate the company.	Affect the company's and employee's reputation, Information leakage, Disclosure of company policies, Profiling.	[56]
	Cyber stalking	Cyber stalkers can get user's personal such as phone number, home address from SNSs and can use these information for achieving various goals like blackmailing, cyber harassment.	Reputation loss, Data disclosure, Blackmail, Cyber harassment, Safety loss, Location leakage.	[35]

Table 2 provides a summary of the different categories of SNS threats. The type of threats and their impact on users are typically described according to the textual description in the their related studies by various security organizations and academia.

4. Analysis of SNS security solutions

In the past few years, SNS security has attracted the attention of many security researchers in both the industry and academic fields. A variety of solutions have been proposed to deal with these aforementioned security threats. In this Section, we discuss and provide several methods and approaches proposed in the literature on SNS security to counter the fruitful security solutions and to achieve trustworthy, secure, better privacy conscious SNSs ecosystem. The list all methods and approaches are shown in Fig. 7 and described as below.

4.1. Watermarking

Digital watermarking is a method of embedding data into media content with the purpose of proving ownership of it. Typically, the watermarking process can be invisible or visible. Visible watermarking is usually visible text or a logo that clearly identifies the owner and is embedded in the image. This type of watermarking tends to cover the bulk of the data and is difficult to remove. Some SNS such as Badoo [73] uses visible watermarking. Invisible watermarking is invisible to the human eye and can be robust, semi-fragile, and fragile. In robust watermarking, the data can be recovered after a malicious attack or signal processing is carried out. Fragile watermarks cannot be recovered or authenticated after common signal processing is done [8]. Semi-fragile watermarks are a hybrid of robust and fragile watermarks. Zigomitros et al. [13] proposed a scheme that uses dual watermarks to protect the user's privacy in SNSs. In this scheme, a multimedia file is watermarked with a dual semi-fragile and robust watermark. These watermarks contain information such as media ID and user ID. The presence of watermarks in the multimedia file allows a user to track many activities, such as if other users are re-uploading

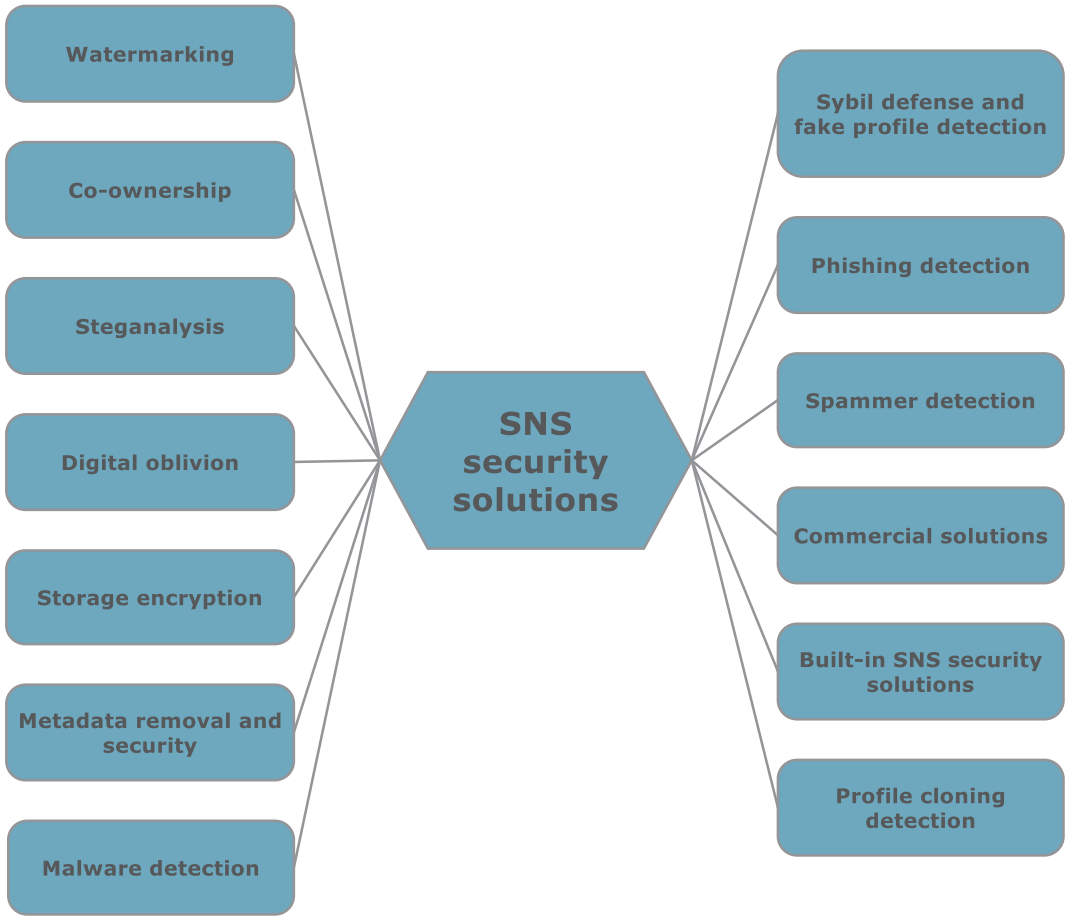

Fig. 7. Security and privacy solutions for SNS.

their multimedia file or modifying it. Patsakis et al. [19] proposed a novel distributed scheme for multimedia data sharing on SNSs that reduces a user's privacy disclosure. The scheme uses a public watermarking techniques on multimedia content to provide unified privacy policies across multiple SNSs. Ho Sin et al. [18] proposed a framework that uses a dual watermarking scheme to record the ownership information of shared multimedia files in SNSs. Thongkor et al. [63] introduced a digital watermarking approach based on the Discrete Wavelet Transform (DWT) coefficient modification for SNSs.

4.2. Co-ownership

The co-ownership model allows multiple users to apply their privacy settings to co-owned videos and pictures. This model has been recognized by many research works [3,4,40]. Squicciarini et al. [4] came up with a technique to enable collective privacy policies for shared multimedia content in SNSs. They used the Clarke-Tax mechanism, which is based on path distances. Later on, Squicciarini et al. [3] implemented the Collaborative Privacy Management (CoPE) tool as an application to ensure the privacy of pictures shared and generated by SNS users. CoPE provides a collaborative measurement of privacy policies based on the option with the highest number of votes. They also presented a user study of this within Facebook, which showed that users like the concept of collaborative privacy management and that it is useful for protecting the privacy of their shared multimedia data. Hu et al. [40] proposed a multiparty authorization mechanism for Facebook. This mechanism defines the logical representation and evaluation of access control policies. Logical representation manages policy conflicts by creating a balance between two parameters. One is the requirement for privacy protection and the other is the user's desire to share data. González-Manzano et al. [65] introduced a Co-owned Personal Data Management approach that applies the concept of object decomposition to ensure the fine-grained user's privacy.

4.3. Steganalysis

SNSs allow users to upload large and high resolution multimedia data. However, suspicious users can use this data as cover objects to spread malicious information. Therefore, it is considered essential to use steganalytic software or mecha-

nisms to find this information within multimedia data. However, many SNSs do not use these types of mechanisms or many times output of such mechanisms is not notified to the users. Many traditional steganalysis mechanisms have been proposed to identify malicious pictures. These mechanisms are based on supervised machine learning techniques in which a large dataset of pictures is accumulated to train a general model, and then these pictures can be classified by using the trained model. Natarajan et al. [118] proposed a multilevel identification approach that identifies malicious profiles in SNSs. This approach analyzes the huge amount of image data in each profile. However, because it is very difficult to analyze this much data, this approach has the issue of real-time deployment. For large SNSs, Li et al. [26] proposed a mechanism that uses high-order joint features and clustering ensembles. The features are trained over a number of hierarchical sub-clusterings, and the output of each clustering is integrated as a cluster ensemble by using the majority voting approach. This cluster ensemble is used to classify suspicious steganographers in SNSs. Recently, Venkatachalam et al. [91] proposed a novel method to detect Stegobot profiles in SNSs. This technique uses a combination of social graph features, profile-based features, and multimedia image content-based features to identify the behavior of suspicious profiles. They proved the effectiveness of their technique on Google+, Twitter, Flicker, and Facebook.

4.4. Digital oblivion

This is a method where an expiration time is placed on digital data so that no one can access the data after it has expired. Nowadays, users publish more and more private data on SNSs and, subsequently, the data storage capacity of SNSs is increasing day by day. Therefore, digital oblivion can be used to protect the privacy of large amounts of data. Several solutions have been proposed to provide digital oblivion in SNSs. Backes et al. [44] developed a scalable, fast, and novel tool called X-pire!, which enables users to upload their images along with an expiration date on SNS such as Flickr and Facebook. The images cannot be accessed after the expiration date is reached. The tool also provides a convenient way by which users can dynamically shorten or prolong the expiration date of their images. Recently, Stokes et al. [62] designed a system that offers digital oblivion facility to SNS users. They implemented digital oblivion as means to authenticate the User to Content (U2C) relationship. They considered the two following U2Cs for digital oblivion in SNSs: 1) the presence of personal data in the uploaded content, and 2) data that has already been uploaded. The combinations of several methods, such as trust management, image tags, watermarking, and digital signature, are used for the authentication stage. Reimann et al. [107] proposed a scheme that implements the timed revocation of user-uploaded data online. The major advantage of this scheme is that it uses the existing infrastructure, unlike the X-pire! tool, and it can implement much longer time-spans on user data. Domingo-Ferrer et al. [48] suggested a set of protocols where the owner of the data inserts an expiration date before publishing his or her data online and can track if somebody is exploiting and/or distributing the data after the expiration date.

4.5. Storage encryption

As we described in Section 3, many SNSs do not have their own data centers and they usually store the user's data in third party data centers. These centers can share this data with other data distributors or many political and geospatial events might reveal the user's data to other organizations without their permission or notifying them. This issue is very critical because many medical and health SNSs exist [36]. Users share a lot of sensitive information on these SNSs and if this information is exposed it can impact users both mentally and economically. Savla et al. [95] analyzed the privacy policies of 35 health related SNSs and the results show that 9% of these did not have a privacy policy. Therefore, a user's data should be stored in an encrypted form to protect it from malicious providers or other organizations. There are several cryptographic techniques that can be implemented in SNSs and allow users to efficiently store and recover their data without exposing it to a third-party service provider, such as a cloud service provider [124]. There are other solutions that mainly focus on the encryption of multimedia data [85]. The major benefit of these solutions is that if somebody successfully obtains the direct link to the shared multimedia data, they cannot access the data until they have the right decryption key.

4.6. Metadata removal and security

Many approaches exist for removing metadata and mitigating the leaking of metadata privacy in SNSs. Boston et al. [51] proposed a method for editing metadata in a file, where the user requests to edit the metadata in a file and to produce an updated file with it. Similarly, Schepis et al. [11] implemented a technique for multimedia metadata security. This technique encrypts multimedia metadata and stores it in the multimedia file. In [14], the authors provided a summary of identified metadata privacy leakages in Decentralized Online Social Networks and various techniques to protect against these leaks. Moreover, solutions proposed in [28] describe an anonymous messaging platform that allows users to share their data over SNSs without exposing metadata information, such as the name of the owner of the data or the data source, to other users.

4.7. Malware detection

A lot of detection mechanisms that detect the online propagation of malware over web have been proposed. However, these mechanisms cannot be applied to detect the spreading of malware in SNSs because it exhibits unique propagation

vectors. Faghani et al. [83] identified the parameters that are related to malware propagation in SNSs, which mainly include graph parameters. Xu et al. [122] proposed a malware detection system for SNSs, which leverages both the topological properties of a SNS and the propagation characteristics of malware. The system relies on a maximum coverage algorithm, in which a detection system adds decoy friends with a group of legitimate SNS users in order to monitor communication between users. When any evidence of suspicious malware propagation in the communication is received by decoy friends, the detection system executes a network and local correlation mechanism to separate malware propagation from legitimate user communication. However, the main challenge of this detection system is determining how many decoy friends should be deployed in large SNSs, such as Facebook, where billions of users exist. Yan et al. [34] analyzed propagation of malware in SNSs based on a dataset collected from location-based SNSs. Based on this analysis, they examined the performance of various server-oriented and user-oriented defense mechanisms against malware propagation in SNSs. Recently, Zhu et al. [41] proposed a Malware Propagation and Prevention Model (MPPM) for SNSs. This model defines the relationships between malware detection, users' habits, and malware propagation in SNSs. They described different states of SNS nodes based on the characteristics of SNSs and several malware prevention rules by using dynamic evolution equations. They also introduced the detection factor to control the propagation of malware.

4.8. Sybil defense and fake profile detection

Nowadays, a Sybil attack in SNS is a serious threat. To stop this kind of attack, many defense mechanisms have been proposed. Wei et al. [120] introduced SybilDefender, which uses network topology for defending against Sybil attacks. It is scalable and efficient for large SNSs, and relies on performing a limited amount of arbitrary walks within the social graphs. They tested their mechanism on real-world topologies and claimed that it is effective and efficient in detecting the Sybil nodes in SNSs. Gao et al. [94] developed SybilFrame, a defense system to mitigate the risk of Sybil attacks in SNSs. This system has the capability of incorporating prior information about users as nodes and their relationships as edges in the social graph. Wang et al. [32] proposed a scheme that identifies Sybil nodes by using the neighbor similarity trust relationship. Other decentralized algorithm, such as GateKeeper [90], has been proposed to identify Sybil nodes in SNSs, which uses the concept of random routes. SybilInfer [27] is a centralized Sybil defense mechanism that uses a Bayesian inference method to determine Sybil probability.

4.9. Phishing detection

Phishing affects the security and privacy of many traditional web applications, such as websites, SNSs, emails, and blogs. Therefore, a lot of anti-phishing methods have been developed to detect and prevent phishing attacks. Most of these methods are based on the machine-learning technique in which features of websites are used to identify the phishing websites [79]. With the significant growth of phishing attacks on SNSs, some researchers have proposed solutions for detecting phishing attacks on SNSs. Aggarwal et al. [1] proposed the phishAri technique for the real-time identification of phishing that occurs on Twitter. This technique can classify tweets posted with URLs into the two categories of phishing or legitimate by using the tweet's content and some specific features, such as mentions, hashtags, tweet length, number of followers, number of tweets, and how long the account has existed. Lee et al. [103] developed WarningBird, which detects suspicious URLs posted on Twitter. It can prevent phishing attacks that hide themselves by exploiting the conditional redirection of URLs. The authors used correlated URL chains in a number of tweets to detect phishing. Recently, Yeong Jeong et al. [112] proposed an unsupervised technique for detecting phishing attacks within Twitter. This technique uses a two-phase unsupervised learning algorithm. Similarly, Cao et al. [45] identified forwarding-based malicious URLs in SNSs by using the three feature sets of forwarding-based features, conventional URLs features, and graph-based features.

4.10. Spammer detection

In the past few years, social spam has attracted the attention of numerous security researchers from industry and academic fields. A considerable amount of work has been done to detect spam and protect SNSs against it. In 2010, Hai Wang et al. [6] proposed graph and content-based features for detecting spam profiles on Twitter. They collected a real dataset from publicly available information on Twitter and used it as an input for machine-learning classifiers to distinguish spam from legitimate postings. In the same year, Lee et al. [57] proposed a novel social honeypot-based approach for identifying spam on MySpace and Twitter. This approach collects real datasets from social networking communities using the deployment of social honeypots. In 2011, Jin et al. [123] introduced a data-mining based technique to detect spam in SNSs. This technique uses content, text, and social network features for identifying spam posted by spammers. They proposed the General Activity Detection (GAD) clustering algorithm for identifying spam within a huge dataset containing image and text features. In 2012, Gao et al. [39] proposed an online spam filtering system for identifying a spam campaign rather than individual spam messages. Ahmed et al. [25] introduced a generic statistical scheme for identifying spam profiles in Facebook and Twitter. They proposed a set of 14 generic statistical features to validate the effectiveness of their scheme. Miller et al. [127] applied a data stream clustering method for detecting spammers in SNSs. Recently, Kacholia et al. [117] developed a tool for detecting spam in video-hosting SNSs. It detects spam in the metadata associated with the user-generated video by using the concept of clustering. Liu et al. [68] developed a smart spammer detection tool that relies on the topic model of

Table 3
An overview of various commercial solutions for SNSs security.

Manufacturer	Product	Key features	Pricing	Platform
Diego Casorran	FB Phishing Protector [70]	Uses as Firefox add-on to protect Facebook users against phishing attacks.	Free	Firefox add-on
Check Point	SocialGuard Privacy Scan [17]	Identifies privacy concerns in Facebook user's profile by scanning recent activities of the user's profile.	Free	Facebook application
Net Nanny	Net Nanny Social [86]	Helps parents to protect their children from SNSs risks such as online predators, cyber bullying, and pornography.	Paid software	Personal computer and smart phone
Infoglide	MinorMonitor [43]	Provides parents an easy and quick dashboard view of Facebook activities of their kids.	Free	Web service
Several security corporations such as Symantec, McAfee, Panda, Kaspersky	Web Security Software [74]	Involves firewall, IDS, anti-virus and other protection software which help SNSs users in protecting their personal computer against risks such as phishing, clickjacking, and malware.	Free for trail period and paid for licensing	Personal computer
McAfee	Social Protection Application [71]	Helps Facebook users to manage and control the privacy of their photos.	Free	Android device

Latent Dirichlet Allocation (LDA). They identified spammers based on the following two topic features: a) the Global Outlier Standard Score (GOSS) that exposes the interest of users on global topic, and b) the Local Outlier Standard Score (LOSS) that reveals users' interest in a local topic. The major advantage of this approach is that it detects smart spammers who pose as legitimate users.

4.11. Commercial solutions

Several security companies have developed security solutions for SNSs to protect against various and increasing security threats. Table 3 provides a summary of various commercial solutions for SNS security and important information, such as manufacturer, product, key features, pricing, and platform, about these solutions. FB Phishing Protector [70] is used as a Firefox add-on to detect suspicious activities, such as the injection of malicious browser script in Facebook, and it protects users against phishing scams. Check Point Software developed a Facebook application called SocialGuard Privacy Scan [17], which identifies privacy concerns in a Facebook user's profile by scanning their recent activities. For example, it can detect posts that reveal the user's personal information. Net Nanny Social [86] is a type of SNS monitoring software that helps parents protect their children against internet risks, such as online predators, cyberbullying, and pornography. By using this software, parents can monitor the social media activities of their children on SNS such as Facebook. Similarly, MinorMonitor [43] is a web-based software that provides parents with a dashboard view of their child's Facebook activities. It uses a knowledge-based analytic mechanism to identify these activities. Nowadays, several security corporations, such as Symantec, McAfee, Panda, Kaspersky, and AVG provide web security software for SNS users. This software incorporates firewalls, an intrusion detection system, anti-virus programs, and other protection software that help users protect their personal computers against risks, such as phishing, clickjacking, and malware [74]. Recently, McAfee introduced a Social Protection application [71], which helps Facebook users manage and control the privacy of their photos. A user can upload his or her photos using this application and can customize the privacy of the photos (for example, who can view, download, print, save, and screen capture images).

4.12. Built-in SNS security solutions

SNSs support various built-in security solutions, such as user privacy settings, authorization mechanisms, report abusive content, etc. SNSs provide authentication mechanisms in order to ensure that the person who is logging in or registering is a legitimate user and not a malicious one (socialbot). Nowadays, many authentication mechanisms, such as multi-factor authentication [22], and CAPTCHA [69] are used. Many SNSs, such as Facebook and Twitter, use a two-factor authentication mechanism that requires a login password and for the user to provide a verification code, which is sent to his or her mobile device. This reduces the chances of an account being compromised [78]. In addition, several SNSs provide a privacy settings option to their users. By using it, users can customize their privacy settings and protect their personal data from other applications or users. For example, a user can configure his or her privacy settings and select which group (for example, only friends, public, only me) can view his or her personal details, posts, pictures, and so on. Moreover, SNSs such as Facebook allow their users to accept or restrict the access of third party applications to their private information [54]. Many SNSs provide internal security mechanisms for protecting their users against scams, fake profiles, spammers, and other risks [20,24,98,104,116]. For instance, Facebook uses the Facebook Immune System (FIS) to protect its users against security threats. FIS uses the adversarial learning method for executing the real-time checking and classifying of read and write actions on Facebook [116]. Also, many SNSs offer the option to report policy violations or abusive content by other users. This option protects minors against cyber harassment and other security attacks, such as spam [24].

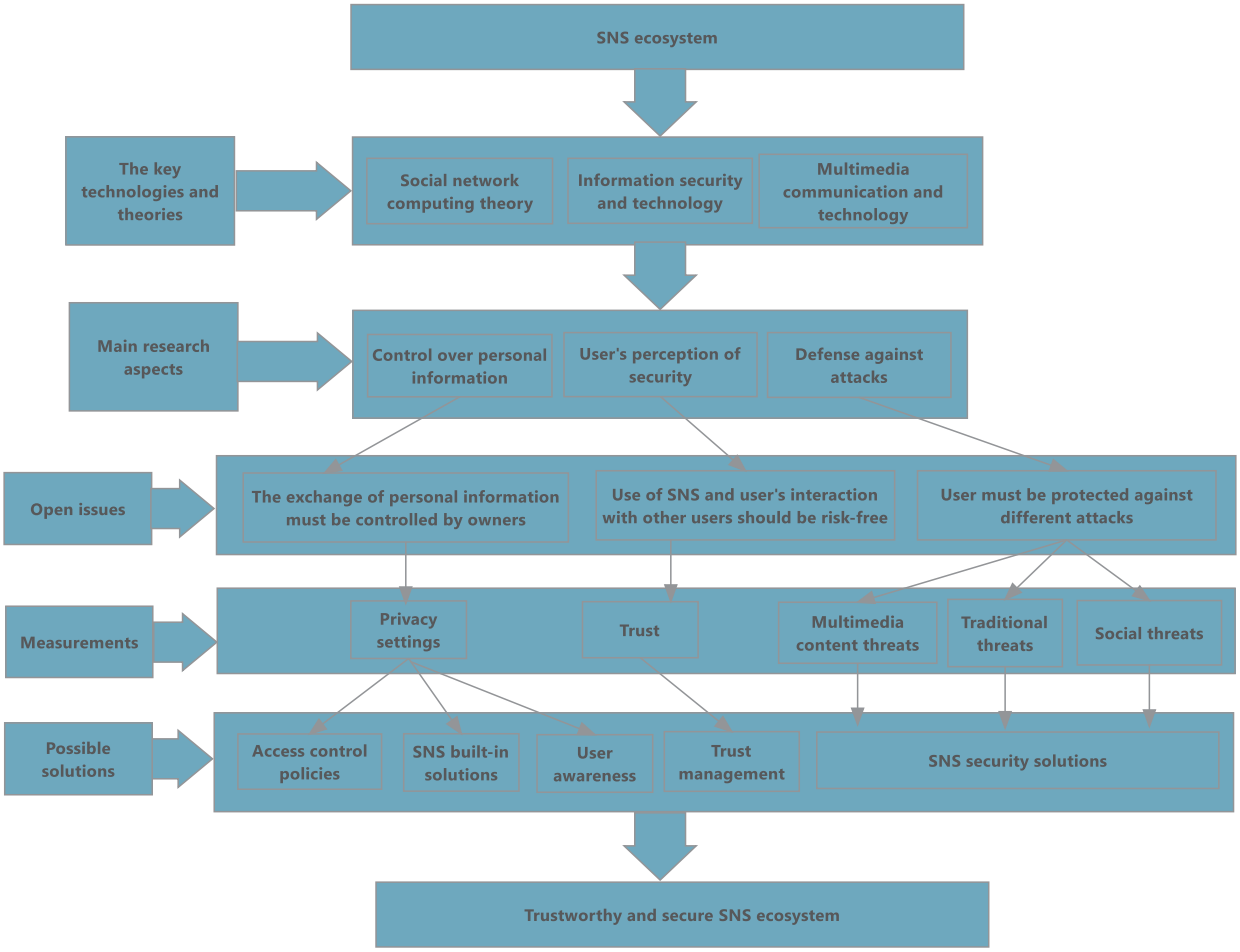

Fig. 8. Proposed research roadmap to measure and optimize the security of SNS.

4.13. Profile cloning detection

SNSs, like Facebook, are currently developing a feature that automatically notifies their users about the cloned profile, which can be identified by using face recognition technology [99]. Kontaxis et al. [30] introduced an approach for discovering SNS profile cloning and developed a prototype that tests whether or not a user is the victim of a cloning attack. Shan et al. [128] proposed a profile cloning detector called the CloneSpotter system, which can be deployed in the server side of SNSs. It detects cloning attacks by exploiting the user's information, such as their login IP.

Table 4 summarizes existing and possible security solutions for SNSs. It provides a short description for each solution. The key methods identified in the table typically described according to the textual description of each solution in respective section. The Table also includes research studies of various security organizations and academia to provide SNS security solutions.

5. Future direction and suggestion of security responses

5.1. Future direction

As we have already discussed, a number of security and privacy threats can put SNS users at risk. There are many researches that presented their own solutions to protect users against these threats. However, these researches still lack to provide suitable qualitative and quantitative analysis of SNS security. With regard to basic characteristics of recent SNS and limitations in previous researches, in this section, we present a novel research direction, which emphasize on how to measure and optimize the security of SNS to achieve the goal of building a trustworthy, efficient, and secure SNS ecosystem. The proposed research roadmap consists of five layers and is shown in Fig. 8. There are various key technologies and theories used to design SNS platform that is described by 1st layer. The security in SNS can be defined with respect to three main research aspects (2nd layer) and corresponding open issues (3rd layer). The measurements and possible solutions to alleviate

Table 4
Summary of SNSs security solutions, description, key methods and related studies.

Solution	Description	Key methods	References
Watermarking	Watermarking is a method of embedding data into media content with the purpose of proving ownership of the media content. The presence of watermarks in the multimedia file allows a user in SNSs to trace many activities such as if other users re-uploading his multimedia file or modify it.	Invisible and visible watermarking, Semi-fragile and fragile watermarking, Dual watermarking scheme, Public watermarking techniques, Digital watermarking approach based on discrete wavelet transform coefficients modification.	[8,13,18,19,63]
Co-ownership	Co-ownership model in SNSs allows multiple users to apply their privacy policies on the co-owned videos, pictures.	Clarke-tax mechanism, Collaborative privacy management, Most highly voted option, Multiparty authorization mechanism, and Object decomposition technique.	[3,4,40,65]
Steganalysis	Steganalysis is a mechanism to find malicious information within multimedia data.	Steganalytic software, Supervised machine learning techniques, Multilevel identification approach, High-order joint features and clustering ensembles, Stegobot profile detection.	[26,91,118]
Digital oblivion	Digital oblivion is a method in which an expiration time is placed on digital data so that anyone cannot access the data after expiration time of data.	X-pire tool, Authentication of "user to content relationship", Timed revocation, A set of protocols, Methods such as Vanish, Ephpub.	[44,48,62,107]
Storage encryption	Storage encryption allows SNSs users to efficiently store and recover their data on SNSs without exposing any data to the third party service provider such as cloud service providers.	Cryptographic techniques, Various encryption schemes for cloud storage such as attribute-based encryption, proxy re-encryption. Various techniques for encryption of multimedia data.	[85,95,124]
Metadata removal and security	This solution provides various approaches for metadata removal and for mitigating the metadata privacy leakage in SNSs.	Various methods for editing metadata in multimedia file, Encryption of multimedia metadata, Anonymous messaging platform.	[11,14,28,51]
Malware detection	Malware detection includes various mechanisms to detect malware propagation in SNSs.	Identification of graph parameters, Machine learning technique, Maximum coverage algorithm, Various server-oriented and user-oriented defense mechanisms, Several malware prevention rules.	[34,41,83,122]
Sybil defense and fake profile detection	Recently, many security researchers have developed tools and techniques to detect fake profiles and defense against Sybil attacks. Most of the techniques either rely on performing a limited amount of arbitrary walks within the social graphs or the concept of random routes.	Network topology analysis, SybilDefender, SybilFrame, SybilLimit, SybilGuard, GateKeeper SybilInfer, Bayesian inference method.	[27,32,90,94,120]
Phishing detection	It includes various anti-phishing methods to detect and prevent phishing attacks in SNSs. Most of these methods are based on machine learning technique in which several features of SNSs like number of followers, age of account is used to identify the phishing attacks.	Machine learning technique, PhishAri technique, WarningBird system, Two-phase unsupervised learning algorithm.	[1,45,79,103,112]
Spammer detection	The fundamental concept of the existing approaches for spammer detection in SNSs is to extract a feature set that separate spam users from legitimate ones and supply that feature set into different machine learning classifier models for identifying inappropriate activities.	Machine learning technique, Social honeypot based approach, Data-mining based technique, General activity detection clustering algorithm, Supervised matrix factorization technique, Latent dirichlet allocation model.	[6,25,39,57,68,123,117,127]
Commercial solutions	Commercial solutions include various security products which have been developed by several security companies to protect SNSs users against security threats.	FB phishing protector, Social guard privacy scan, Net nanny social, Minor monitor, Web security software, Social protection application.	[17,43,70,71,74,86]
Built-in SNS security solutions	Many SNSs provide various in-built security solutions such as user privacy settings, authorization mechanisms, report abusive content.	Multi-factor authentication, Photos-of-friends identification, CAPTCHA, Two Factor authentication, Facebook immune system.	[20,22,24,54,69,78,98,104,116]
Profile cloning detection	Many SNSs such as Facebook are currently developing a feature that automatically detects cloned profile and notifies their users about such profile. The cloned profile can be identified using face recognition technology.	Face recognition technology, CloneSpotter system.	[30,99,128]

each open issue are provided in 4th layer and 5th layer, respectively. The security of SNS relies on three main research aspects as described below.

(1) *Control over personal information:* For a secure SNS, the flow of personal information exchanged and transferred by user should be controlled. This can be achieved, when a user has direct control over how his/her information spread and share. In modern SNS, the direct control over shared information is measured by using privacy settings. A user can apply his/her privacy settings and control over shared information in SNS. As, we described in SNS built-in solution (Section 4), how users can protect their personal data by applying privacy settings defined by the SNS. However, many times privacy settings are not effective to control over the user's personal information. This is due to the lack of user awareness or privacy settings is not properly defined in many SNS. In addition, the issue of an SNS user does not have any control on the information that other users expose about him/her still exists. For example, tagging pictures of friend's are one key feature that are available in many modern SNS. However, they have no explicit privacy tool and technique that provide access control for this tagging Feature. In our opinion, an innovative privacy and access control policy is still needed to handle the access and privacy of user's sensitive information in SNS. Recently, many approaches have been proposed for privacy and access control in SNSs. Villata et al.'s research [111] presented an access control scheme for social semantic web. It relied on a social semantic SPARQL security for access control vocabulary ontology that permits users of SNSs to set the access control rules for their data. Pang et al. [49] focused on the public information in SNSs and proposed a novel access control model that provides different types of logics for expressing access control policies in SNSs. Imran-Daud et al. [76] proposed a content-driven privacy-preserving access control approach in which semantics of the textual publication is used to detect the sensitive textual content and the privacy settings for the content are defined automatically according to their sensitivity. Many researchers, such as Petrlic et al. [100] and Shen et al. [96] proposed privacy-friendly and security architectures that preserve the user's privacy and provide security to their data in the cloud computing environment. These architectures can be adopted to mitigate outsourcing and transparency of data centers threat (described in Section 3.1) in SNSs.

(2) *User's perception of security*: It is described as the measurement of user's trust that the use of SNS and interacting with other users are secure and risk-free. Generally, it relies on the user's interaction with unknown parties. In SNS, a user can be connected with other users virtually means that they never met before establishing connection on SNS. In this situation, it is essential for user understand the benefits/risks associated with the virtual interaction for secure and risk-free use of SNS. The suitable measurement of benefits/risks is trust. The trust management provides user a risk-free way of interacting with other users and establishing trustworthy relationship. Many researchers have presented their views to manage and compute the social trust in SNS. Some of them consider the structure of a given SNS to evaluate the trust propagation among its users. Others concentrate only on the interaction among users to measure trust values. These two methods (structural and interactional) are basic for evaluating trust in SNS. Recently, hybrid method that uses both interactional and structural aspects for measuring trust in SNS is investigated. In our observation, the trust management in SNS is most promising research direction and a more effective trust measurement technique is still required in SNS. Recently, Fu et al. [37] proposed an interaction-based social trust model that describes social trust in terms of single independent host, multiple competing hosts as an optimal control problem, and a non-cooperative differential game. Zhang et al.'s research [129] presented a trust model for multimedia SNS. The proposed model is based on some share character factors, such as user share similarity, feedback weighting factor, and credible feedback of digital contents. The trust is calculated by using three approaches: multiple recommendation trust synthetic strategy, a direct trust calculation window mechanism, and recommended path finding algorithm.

(3) *Defense against attacks:* This research aspect describes the protection of user against different attacks. In Section 3, we described several threats that can compromise the security and privacy of SNS users. These threats try to accomplish one or more of the following objectives: a) Collect a user's personal information, such as home address, geo-location, recent activity, political and religious views, by inferring shared multimedia data in SNSs and exploiting this information for purposes that include cyber harassment, destroying someone's reputation, extortion, and burglary; b) use various traditional attack techniques, such as fake websites and emails, malicious programs, fake identities, and more, to gain control over the user's profile and utilize this control as a spreading platform to target the user's friends and to steal their confidential information; and c) Exploit the social relationship on SNSs with the malleable entity like children and company employee to accomplish various goals such as cyber harassment, spy the company.

The type of threats that we have described in this paper are the cause of various SNS security attacks. Table 5 provides a summarizes and comparison of different type of attacks. In Table 5, "Nature of attack" represents if an attack is automated or manual, and "Attack difficulty" denotes that a technological effort is required to perform the attack. We divided attack difficulty into the three categories of High, Average, and Low. High refers to certain types of attacks, such as malware and clickjacking, which require a huge amount of technical resources and knowledge to create the malicious payload and propagation vector. Average refers to attacks, such as a video conference, which require limited resources and knowledge. Low refers to attacks, such as cyberstalking and inference, which require very little knowledge about networking and computer systems. "Risk to data privacy" refers to whether an attack affects the privacy of user's data or not. Similarly, "Risk to data integrity" refers to whether an attack modifies the user's data or not. Table 5 also compares the impact level of attacks on SNS users. We defined these three impact levels as being High, Average, and Low. The impact level of an attack is determined based on the user's amount of personal loss, such as sensitive information leakage or a loss of reputation, due to the

Table 5
Comparison of various security attacks on SNSs.

Attacks	Parameters						
	Nature of attack	Attack difficulty	Risk to data privacy	Risk to data integrity	Attack impact on user	Effectiveness of server-side security deployment	Effectiveness of user-side security deployment
Multimedia content exposure	Manual	Low	Yes	No	Average to high	Poor	Strong
Metadata	Automated	Low	Yes	No	High	Medium	Medium
Unauthorized data disclosure	Manual	Low	Yes	Yes	Low	Strong	Medium
Shared ownership	Manual	Low	Yes	No	Low	Poor	Strong
Manipulation of multimedia content	Automated	Low to average	Yes	Yes	Average	Poor	Strong
Steganography	Manual	Average	Yes	Yes	High	Strong	Medium
Shared links to multimedia content	Automated	Low	Yes	Yes	Average to high	Medium	Medium
Static link	Automated	Low	Yes	No	Low	Strong	Medium
Outsourcing and transparency of data centers	Automated	Low	Yes	No	Average to high	Strong	Poor
Video conference	Manual	Average	Yes	Yes	High	Medium	Medium
Tagging	Automated	Low	Yes	No	Low	Poor	Strong
Phishing	Automated	Low	Yes	Yes	High	Poor	Strong
Malware	Automated	High	Yes	Yes	High	Medium	Medium
Sybil attack and fake profiles	Automated	High	No	Yes	Average	Strong	Poor
Spamming	Automated	Low	No	No	Low	Strong	Poor
Clickjacking	Automated	High	Yes	Yes	High	Medium	Medium
De-anonymization attack	Manual	Average	Yes	Yes	Average to high	Medium	Strong
Inference attack	Manual	Low	Yes	No	Low	Medium	Strong
Cyber-bullying and grooming	Manual	Low	No	No	High	Poor	Strong
Corporate Espionage	Automated, Manual	Average	Yes	No	Low to average	Poor	Strong
Cyber stalking	Manual	Low	Yes	No	Average to high	Poor	Strong

Table 6
SNSs security threats and their corresponding solutions.

Solutions \ Threats	Multimedia content exposure	Shared ownership	Manipulation of multimedia content	Steganography	Metadata	Shared links to multimedia content	Static links	Outsourcing and transparency of data centers	Video conference	Tagging	Unauthorized data disclosure	Phishing	Malware	Sybil attack (Fake profiles)	Spamming	Clickjacking	De-anonymization attack	Inference attack	Profile cloning attacks	Cyber-bullying and grooming	Corporate eespionage	Cyber stalking
Watermarking			✓								✓								✓			
Co-ownership		✓								✓												
Steganalysis				✓										✓	✓							
Digital oblivion	✓					✓						✓	✓			✓						
Storage encryption							✓	✓			✓						✓	✓	✓	✓	✓	✓
Metadata removal and security	✓				✓												✓	✓				
Malware detection						✓			✓				✓		✓	✓						
Sybil defense and fake profile detection										✓	✓		✓	✓	✓	✓			✓	✓		✓
Phishing detection						✓						✓	✓	✓	✓	✓						
Spammer detection				✓		✓				✓		✓	✓	✓	✓	✓						
FB phishing protector				✓		✓						✓				✓						
Social guard privacy scan	✓				✓					✓				✓			✓	✓	✓	✓		✓
Net Nanny social														✓						✓		✓
Minor monitor														✓						✓		✓
Web security software				✓		✓						✓	✓		✓	✓						
Social protection application	✓		✓		✓		✓				✓											
Authentication mechanisms												✓		✓	✓				✓			
Privacy settings	✓				✓					✓	✓			✓	✓		✓	✓		✓	✓	✓
Report users				✓		✓				✓		✓	✓	✓	✓	✓			✓	✓		✓
Profile cloning detection	✓				✓						✓			✓	✓		✓		✓	✓	✓	✓

attack. We categorized the effectiveness of server and user side security deployment into Strong, Medium, and Poor, which describe how effective the sever-side and user-side security mechanisms are when it comes to mitigating an attack.

In Section 4, various security solutions, which safeguard SNS users against various security threats, were presented. Table 6 shows how various security threats that were covered in Section 3 could be addressed by existing solutions. It is clearly shown in Table 6 that most of the multimedia security threats in SNSs can be resolved with very well-known solutions. However, most of the security solutions, such as watermarking or steganalysis, cannot be fully adopted by many

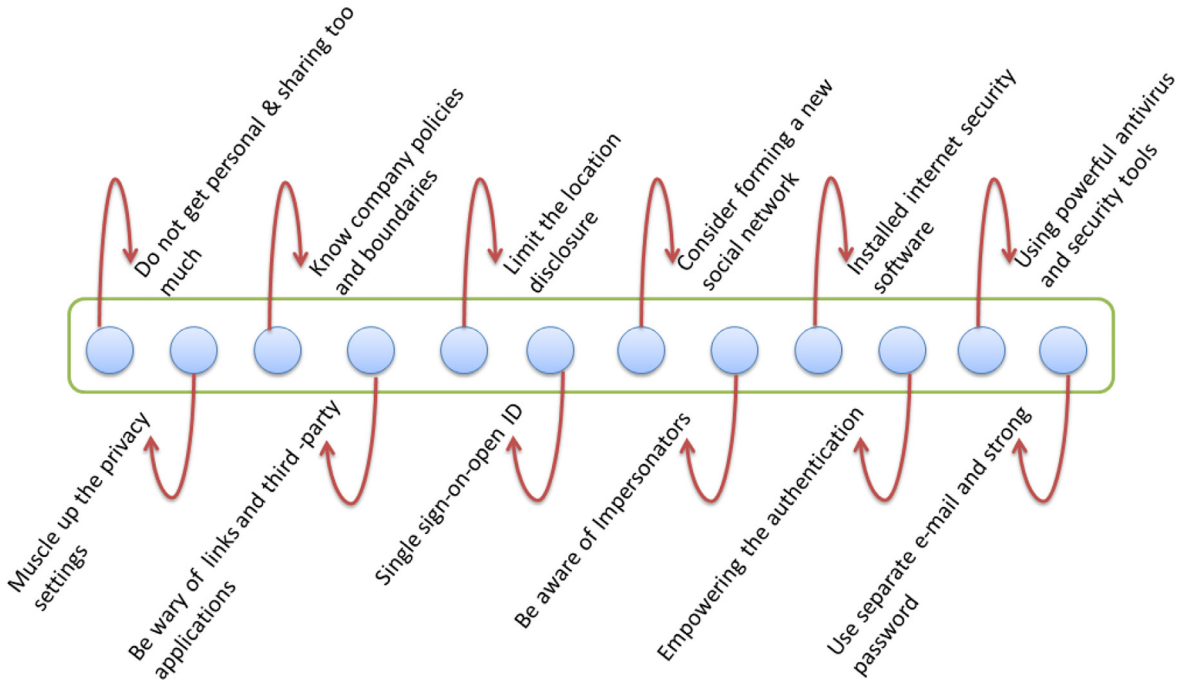

Fig. 9. Security responses for SNSs users.

SNSs. The major reason for this is that the processing cost for these solutions is quite high compared to other traditional solutions, such as phishing and malware detection. Steganalysis and the watermarking of the user's shared data require additional processing costs. The cost issue arises when these solutions are applied to all of multimedia content uploaded on SNSs. However, these solutions can be used as "freemium" services where their basic features can be used at no cost and additional features can be obtained via subscription. User alertness is another major issue in SNSs, as many do not provide any mechanism that alerts their users about possible threats that result from sharing of different types of sensitive data, such as images and videos. However, user alertness can be accomplished by regularly providing recent news about various SNSs security updates, such as recent attacks, defense solutions, user responsibilities, and prevention tools.

As a future direction for SNS security, a variety of data leak prevention mechanisms [29] and position monitoring system [21] can be used to monitor and analyze the information shared by SNS users. These mechanisms can be used to let them know which of their pieces of shared information is sensitive and what must be removed from a SNS. Also, various graph-based anomaly detection techniques [64], content modeling algorithm [60], and community detection mechanism [102] can be utilized to resolve the problem of detecting fake user accounts or compromised accounts. The cognitive psychology concept can be used to evaluate the spread of misinformation, disinformation, and propaganda in SNSs [55]. Moreover, various authentication solutions such as [119,108] that have been proposed for lightweight secure group communication in wireless sensor network can be used to provide better authentication service in SNSs. According to Kamilaris et al.'s research [7], SNS is capable to deliver many real-life pervasive applications such as sharing home devices in a domestic environment, area monitoring in a working environment, energy awareness through social comparisons. However, these applications have some security issues such as lack of privacy, access control, which can be mitigated by using existing privacy solutions for SNS [125].

5.2. Suggestion of security responses

We recommend some easy-to-apply response techniques that can help users boost their privacy and security in SNSs, such as Facebook. These easy-to-apply response techniques are shown in Fig. 9 and are described below.

- *Do not get personal and share too much:* Users should not post too many personal and sensitive details, such as their home address, family information, phone number, and job details. It is also recommended that SNS users hide their friends list, and avoid posting photos and videos of their homes and relatives. It is extremely important that users take care to not reveal their confidential information, such as credit card number, passport details, and bank account information.
- *Tighten the privacy settings:* All SNSs have default privacy setting. Nevertheless, for some SNSs such as Facebook, the default privacy settings are not sufficient enough to secure their users' accounts. Users should carefully read the privacy policy of the SNS that they are using and control who can see their personal information.

Usually, Facebook allows its users to update and control their privacy settings, for example, determine who can see their posts and their friends list.

Know company policies and boundaries: As already discussed in Section 2, there are several reports of individuals who lost their occupations and reputations because of sharing unauthorized information on SNSs. This can be easily avoided when an employee knows their employer's policies about what their employer's standards are in regards to videos, pictures, or messages that they post online. This protects the organization's reputation and prevents it from losing data and intellectual property.

Be wary of links and third-party applications: A malicious user can share links and short URLs, which may contain malicious codes and script, on a SNS. These shared links may collect a user's personal information or their friend's details. Therefore, it is recommended that users try to ignore links shared by their friends, online advertising, and tweets. Moreover, third party applications, such as games, frequently demand and collect user's personal information for providing their services. This collected information may be shared with outsiders or other third party agencies. To avoid this, we suggest that users do not install new and unnecessary games and quiz applications on their SNS account.

Limit location disclosure: For better protection, SNS users should not share their present and future location information, as this can be easily accessed and used by criminals. Also, uploaded multimedia content may reveal the user's location; so, it is strongly recommended that users avoid sharing their location online and disable geotagging on their mobile devices. Users should upload their multimedia content with care and remove all sensitive metadata within the multimedia content before uploading it.

Single sign-on open ID: Utilizing a solitary sign-on for different stages is one way individuals can reduce the probability of their password(s) getting into the hands of identity thieves. Open ID is the most well-known single sign-on to manage different accounts.

Consider creating a new social network: Facebook and Twitter are not the only SNS platforms available. However, they are overwhelmingly popular and attract a substantial collection of individuals with different motivations. Those who are keen on communicating with a smaller, more intimate group of people should create their own social network instead. There are many services, such as Ning, MeetUp, FamilyLeaf, etc., available that make it easy to launch your own social network in a matter of minutes.

Install internet security software: As covered in Section 4, many SNS security threats, such as malware, cyberbullying, and cyber-grooming, can be mitigated by using the security software offered by several security corporations, such as Infoglide, Net Nanny, and Check Point. Also, Facebook and Twitter offer their own security tools, which users can access to better protect themselves.

Use a separate e-mail address and a strong password: Security is as important for one's SNS account as it is for one's computer or any other account. Usually, many SNS users use weak passwords for their account, which may allow hackers to gain unauthorized access. Hackers can use a hacked SNS account to post spam or perform various security attacks, such as phishing or corporate espionage. Typically, SNS users can create strong passwords for their account and prevent hackers from gaining unauthorized access. We suggest that passwords consist of no less than eight characters, which are both letters and numbers, and that they are changed approximately every three months.

6. Conclusion

SNSs have become a desired medium of communication for billions of web users, as such services allow people to share their interests, photos, videos, and engage with friends without geographical and economic limitations. However, these services can expose users to serious cyber security risks. In this paper, we provided a state-of-the-art study on several kinds of privacy and security issues in SNSs that arise from some of their significant features, such as sharing pictures, commenting, tagging, and blogging. To understand the issues, we summarized various recent attack statistics and security reports that have been released by several security organizations and blogs. Furthermore, we addressed the security state of SNSs by describing three classes of threats: Multimedia content threats, Traditional threats, and Social threats. Subsequently, we conducted a analysis of the possible and existing schemes for protecting SNS users against these threats. We also compared various SNS security attacks based on certain parameters and discussed some open research challenges and future direction. Finally, we presented some easy-to-apply response techniques that can be easily followed by SNS users to better protect themselves against various security threats. We suggest that SNS users follow our response techniques and educate themselves and their colleagues on any recent security threats.

Based on the analysis of recent security issues and solutions in this paper, our findings suggest that SNSs provide a new research direction with many opportunity, such as investigating new types of privacy and security threats, and designing and assessing innovative SNSs security solutions. The future research direction presented in this paper can be used to improve the current state-of-the-art SNSs security solutions.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2013-0-00684) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

[1] A. Aggarwal, A. Rajadesingan, P. Kumaraguru, PhishAri: automatic realtime phishing detection on twitter, in: eCrime Researchers Summit (eCrime), IEEE, 2012, pp. 1–12.
[2] A. Barinka, Bad Day for Newsweek, Delta Amid Social-Media Hackings, (https://www.bloomberg.com/news/articles/2015-02-10/newsweek-s-twitter-account-briefly-hacked-by-cybercaliphate-). Online; accessed 04 April 2017.
[3] A.C. Squicciarini, H. Xu, X.L. Zhang, CoPE: enabling collaborative privacy management in online social networks, J. Am. Soc. Inf. Sci. Technol. 62 (3) (2011) 521–534.
[4] A.C. Squicciarini, M. Shehab, J. Wede, Privacy policies for shared content in social network sites, VLDB J. 19 (6) (2010) 777–796.
[5] A. El Asam, M. Samara, Cyberbullying and the law: a review of psychological and legal challenges, Comput. Hum. Behav. 65 (2016) 127–141.
[6] A. Hai Wang, Don't follow me: spam detection in twitter, in: Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE, 2010, pp. 1–10.
[7] A. Kamilaris, G. Taliadoros, A. Pitsillides, D. Papadiomidous, The practice of online social networking of the physical world, Int. J. Space-Based Situated Comput. 2 (4) (2012) 240–252.
[8] A.M. Alattar, N.D. Memon, C.D. Heitzenrater, Media Watermarking, Security, and Forensics, Spie Press, 2015.
[9] A. Mendelson, Does social media distort reality?, (http://www.scoop.it/t/social-media-versus-reality). Online; accessed 04 April 2017.
[10] A. Mislove, B. Viswanath, K.P. Gummadi, P. Druschel, You are who you know: inferring user profiles in online social networks, in: Proceedings of the Third ACM International Conference on Web Search and Data Mining, 2010, pp. 251–260.
[11] A.P. Schepis, A. Caola, Techniques for multimedia metadata security, U.S. Patent No. 9,268,964, 2016.
[12] A. Viejo, J. Castella-Roca, G. Rufián, Preserving the user's privacy in social networking sites, in: Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Berlin Heidelberg, Springer, 2013, pp. 62–73.
[13] A. Zigomitros, A. Papageorgiou, C. Patsakis, Social network content management through watermarking, in: Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012, pp. 1381–1386.
[14] B. Greschbach, G. Kreitz, S. Buchegger, The devil is in the metadata—new privacy challenges in decentralised online social networks, in: Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2012, pp. 333–339.
[15] B. Sams, Facebook photo exploit allows you to view any albums of non-friends, (https://www.neowin.net/news/facebook-photo-exploit-allows-you-to-view-any-albums-of-non-friends). Online; accessed 04 April 2017.
[16] CareerBuilder, Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade, (http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?ed=12%2F31%2F2016&id=pr945&sd=4%2F28%2F2016). Online; accessed 04 April 2017.
[17] Check Point Software, SocialGuard Privacy Scan, (https://www.facebook.com/games/sgprivacy/). Online; accessed 04 April 2017.
[18] C. Ho Sin, N.A. Kim, B.W. Go, K.S. Min, J.D. Lee, J.H. Park, Realizing the right to be forgotten in an SNS environment, in: H. Jeong, M.S. Obaidat, N. Yen, J. Park (Eds.), Advances in Computer Science and Its Applications, Lecture Notes in Electrical Engineering, 279, Springer, Berlin, Heidelberg, 2014, pp. 1443–1449.
[19] C. Patsakis, A. Zigomitros, A. Papageorgiou, E. Galván-López, Distributing privacy policies over multimedia content across multiple online social networks, Comput. Netw. 75 (2014) 531–543.
[20] D.H. Lee, Personalizing information using users' online social networks: a case study of CiteULike, J. Inf. Process. Syst. 11 (1) (2015) 1–21.
[21] D.V. Medhane, A.K. Sangaiah, ESCAPE: effective scalable clustering approach for parallel execution of continuous position-based queries in position monitoring applications, IEEE Trans. Sustain. Comput. (2017) 1–13, doi:10.1109/TSUSC.2017.2690378.
[22] D. Wang, N. Wang, P. Wang, S. Qing, Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity, Inf. Sci. 321 (2015) 162–178.
[23] E. Novak, Q. Li, in: A Survey of Security and Privacy in Online Social Networks, College of William and Mary Computer Science, 2012, pp. 1–32. Technical Report.
[24] Facebook, How to Report Things, (https://www.facebook.com/help/reportlinks). Online; accessed 03 April 2017.
[25] F. Ahmed, M. Abulaish, A generic statistical approach for spam detection in Online Social Networks, Comput. Commun. 36 (10) (2013) 1120–1129.
[26] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, C. Gu, Steganalysis over large-scale social networks with high-order joint features and clustering ensembles, IEEE Trans. Inf. Forensic Secur. 11 (2) (2016) 344–357.
[27] G. Danezis, P. Mittal, SybilInfer: detecting sybil nodes using social networks, in: NDSS, 2009, pp. 1–15.
[28] G. Fanti, P. Kairouz, S. Oh, K. Ramchandran, P. Viswanath, Metadata-conscious anonymous messaging, IEEE Trans. Signal Inf. Process. Netw. 2 (4) (2016) 582–594.
[29] G. Katz, Y. Elovici, B. Shapira, CoBAn: a context based model for data leakage prevention, Inf. Sci. 262 (2014) 137–158.
[30] G. Kontaxis, I. Polakis, S. Ioannidis, E.P. Markatos, Detecting social network profile cloning, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2011, pp. 295–300.
[31] G. Noh, H. Oh, Y.M. Kang, C.K. Kim, PSD: Practical Sybil detection schemes using stickiness and persistence in online recommender systems, Inf. Sci. 281 (2014) 66–84.
[32] G. Wang, F. Musau, S. Guo, M.B. Abdullahi, Neighbor similarity trust against sybil attack in P2P e-commerce, Trans. Parallel Distrib. Syst. 26 (3) (2015) 824–833.
[33] G. Wondracek, T. Holz, E. Kirda, C. Kruegel, A practical attack to de-anonymize social network users, in: IEEE Symposium on Security and Privacy, 2010, pp. 223–238.
[34] G. Yan, G. Chen, S. Eidenbenz, N. Li, Malware propagation in online social networks: nature, dynamics, and defense implications, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 196–206.
[35] H. Dreßing, J. Bailer, A. Anders, H. Wagner, C. Gallas, Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims, Cyberpsychol, Behav. Soc. Netw. 17 (2) (2014) 61–67.
[36] HealthBoards:Health Message Boards, (http://www.healthboards.com/). Online; accessed 04 April 2017.
[37] H. Fu, H. Li, Z. Zheng, P. Hu, P. Mohapatra, Optimal system maneuver for trust management in social networks, arXiv preprint arXiv:1604.07139 (2016) 1–10.
[38] H. Gao, J. Hu, T. Huang, J. Wang, Y. Chen, Security issues in online social networks, IEEE Internet Comput. 15 (4) (2011) 56–63.
[39] H. Gao, Y. Chen, K. Lee, D. Palsetia, A.N. Choudhary, Towards online spam filtering in social networks, in: NDSS, 12, 2012, pp. 1–16.
[40] H. Hu, G.J. Ahn, J. Jorgensen, Multiparty access control for online social networks: model and mechanisms, IEEE Trans. Knowl. Data Eng. 25 (7) (2013) 1614–1627.
[41] H. Zhu, C. Huang, H. Li, MPPM: Malware propagation and prevention model in online SNS, in: IEEE International Conference on Communications Workshops (ICC), IEEE, 2014, pp. 682–687.
[42] I. Kayes, A. Iamnitchi, A Survey on Privacy and Security in Online Social Networks, arXiv preprint arXiv:1504.03342 (2015) 1–40.
[43] Infoglide, Minormonitor—Facebook Monitoring and Parental Control Software, (http://www.minormonitor.com/). Online; accessed 04 April 2017.
[44] J. Backes, M. Backes, M. Dürmuth, S. Gerling, S. Lorenz, X-pire!-a digital expiration date for images in social networks, arXiv preprint arXiv:1112.2649 (2011) 1–22.
[45] J. Cao, Q. Li, Y. Ji, Y. He, D. Guo, Detection of forwarding-based malicious urls in online social networks, Int. J. Parallel Program 44 (1) (2016) 163–180.
[46] J.C. Dressler, C. Bronk, D.S. Wallach, Exploiting military OpSec through open-source vulnerabilities, in: Proceedings of the Military Communications Conference, MILCOM, IEEE, 2015, pp. 450–458.
[47] J.D. Lee, C.H. Sin, J.H. Park, PPS-RTBF: Privacy protection system for right to be forgotten, J. Converg. 5 (2014) 37–40.

[48] J. Domingo-Ferrer, Rational enforcement of digital oblivion, in: Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society, ACM, 2011, pp. 2–10.
[49] J. Pang, Y. Zhang, A new access control scheme for Facebook-style social networks, Comput. Secur 54 (2015) 44–59.
[50] J. Savage, Top 5 Facebook Video Statistics for 2016 [Infographic], (http://www.socialmediatoday.com/marketing/top-5-facebook-video-statistics-2016-infographic). Online; accessed 4 April 2017.
[51] J.S. Boston, B.E. Rogowitz, M. Topkara, S.P. Wood, Editing metadata in a social network, U.S. Patent Application No. 12/354,651, 2010.
[52] J. Taylor, HMV staff backlash on Twitter, (http://oursocialtimes.com/hmv-staff-backlash-on-twitter/). Online; accessed 04 April 2017.
[53] K. Ghazinour, S. Matwin, M. Sokolova, Monitoring and recommending privacy settings in social networks, in: Proceeding of the Joint EDBT/ICDT 2013 Workshops, ACM, 2013, pp. 164–168.
[54] K. Ghazinour, S. Matwin, M. Sokolova, YOURPRIVACYPROTECTOR, A recommender system for privacy settings in social networks, arXiv preprint arXiv:1602.01937 (2016) 1–15.
[55] K. Krishna Kumar, G. Geethakumari, Detecting misinformation in online social networks using cognitive psychology, Hum.-Centric Comput. Inf. Sci. 4 (1) (2014) 1–22.
[56] K. Krombholz, H. Hobel, M. Huber, E. Weippl, Advanced social engineering attacks, J. Inf. Secur. Appl. 22 (2015) 113–122.
[57] K. Lee, J. Caverlee, S. Webb, Uncovering social spammers: social honeypots+ machine learning, in: Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval, ACM, 2010, pp. 435–442.
[58] K. Mettler, 'Poor Gorilla': Teacher's aide fired for racist Facebook posts about Michelle Obama, (https://www.washingtonpost.com/news/morning-mix/wp/2016/10/04/poor-gorilla-teachers-aide-fired-for-racist-facebook-posts-about-michelle-obama/). Online; accessed 04 April 2017.
[59] Konstantin Ignatiev, Statistics on Parental Control Alerts for Various Countries, (https://securelist.com/blog/incidents/57841/statistics-on-parental-control-alerts-for-various-countries/). Online; accessed 03 April 2017.
[60] K. Rog Kim, N.M. Moon, Content modeling based on social network community activity, J. Inf. Process. Syst. 10 (2) (2014) 271–282.
[61] K. Smith, Marketing: 96 Amazing Social Media Statistics and Facts for 2016, (https://www.brandwatch.com/blog/96-amazing-social-media-statistics-and-facts-for-2016/). Online; accessed 04 April 2017.
[62] K. Stokes, N. Carlsson, A peer-to-peer agent community for digital oblivion in online social networks, in: Proceedings of the Eleventh Annual International Conference on Privacy, Security and Trust (PST), 2013, pp. 103–110.
[63] K. Thongkor, N. Mettripun, T. Pramoun, T. Amornraksa, Image watermarking based on DWT coefficients modification for social networking services, in: Proceedings of the 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), IEEE, 2013, pp. 1–6.
[64] L. Akoglu, H. Tong, D. Koutra, Graph based anomaly detection and description: a survey, Data Min. Knowl. Discov. 29 (3) (2015) 626–688.
[65] L. González-Manzano, A.I. González-Tablas, J.M. de Fuentes, A. Ribagorda, Cooped: co-owned personal data management, Comput. Secur. 47 (2014) 41–65.
[66] L. Jin, Y. Chen, T. Wang, P. Hui, A.V. Vasilakos, Understanding user behavior in online social networks: a survey, IEEE Commun. Mag. 51 (9) (2013) 144–150.
[67] L. Keating, Hacking of Mark Zuckerberg's Social Media Accounts Teaches Us a Big Lesson: Always Choose a Good Password, (http://www.techtimes.com/articles/163422/20160607/hacking-mark-zuckerbergs-social-media-accounts-teaches-big-lesson-always.htm). Online accessed 04 April 2017.
[68] L. Liu, Y. Lu, Y. Luo, R. Zhang, L. Itti, J. Lu, Detecting "Smart" Spammers On Social Network: A Topic Model Approach, arXiv preprint arXiv:1604.08504 (2016) 1–6.
[69] L. Von Ahn, M. Blum, N.J. Hopper, J. Langford, CAPTCHA: using hard AI problems for security, in: International Conference on the Theory and Applications of Cryptographic Techniques, Berlin Heidelberg, Springer, 2003, pp. 294–311.
[70] Malavida, Facebook Phishing Protector, (http://facebook-phishing-protector.en.malavida.com/). Online; accessed 04 April 2017.
[71] McAfee, Mcafee Social Protection, (http://beta.mcafee.com/betamcafee/mspbeta_lp.aspx?cookieCheck=true). Online; accessed 04 April 2017.
[72] M. Diomidous, K. Chardalias, A. Magita, P. Koutonias, P. Panagiotopoulou, J. Mantas, Social and psychological effects of the internet use, Acta. Inform. Med. 24 (1) (2016) 66–68.
[73] Meet People on Badoo, Make New Friends, Chat, Flirt, (http://www.badoo.com). Online; accessed 04 April 2017.
[74] M. Fire, R. Goldschmidt, Y. Elovici, Online social networks: threats and solutions, IEEE Commun. Surv. Tut. 16 (4) (2014) 2019–2036.
[75] M. Fire, R. Puzis, Organization mining using online social networks, Netw. Spat. Econ. 16 (2) (2016) 545–578.
[76] M. Imran-Daud, D. Sánchez, A. Viejo, Privacy-driven access control in social networks by means of automatic semantic annotation, Comput. Commun. 76 (2016) 12–25.
[77] M. Kandias, L. Mitrou, V. Stavrou, D. Gritzalis, Which side are you on? A new Panopticon vs. privacy, in: Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE, 2013, pp. 1–13.
[78] M.M. Joe, B. Ramakrishnan, Novel authentication procedures for preventing unauthorized access in social networks, Peer-to-Peer Netw. Appl. (2016) 1–11, doi:10.1007/s12083-016-0426-7.
[79] M. Moghimi, A.Y. Varjani, New rule-based phishing detection method, Expert Syst. Appl. 53 (2016) 231–242.
[80] M. Nauman, N. Azam, J. Yao, A three-way decision making approach to malware analysis using probabilistic rough sets, Inf. Sci. 374 (2016) 193–209.
[81] 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, (http://www.dailymail.co.uk/femail/article-2385623/I-expressing-frustration-high-cost-living-New-York-Top-Lacoste-salesman-fired-posting-paycheck-Instagram.html). Online; accessed 04 April 2017.
[82] M. Raggo, Anatomy of a Social Media Attack, (http://www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680). Online; accessed 04 April 2017.
[83] M. Reza Faghani, H. Saidi, Malware propagation in Online Social Networks, in: Proceedings of the 4th International Conference on Malicious and Unwanted Software (MALWARE'09), 2009, pp. 8–14.
[84] M.R. Faghani, U.T. Nguyen, A study of clickjacking worm propagation in online social networks, in: Proceedings of the 15th International Conference on Information Reuse and Integration (IRI), IEEE, 2014, pp. 68–73.
[85] M. Tierney, I. Spiro, C. Bregler, L. Subramanian, Cryptagram: photo privacy for online social media, in: Proceedings of the first ACM conference on Online social networks, ACM, 2013, pp. 75–88.
[86] Net Nanny, Social Media Safety & Protection with Net Nanny Social, (https://www.netnanny.com/products/net-nanny-social/). Online; accessed 04 April 2017.
[87] Nexgate, Research Report 2013 State of social media spam, (http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf). Online; accessed 04 April 2017.
[88] N.N.G. de Andrade, A. Martin, S. Monteleone, All the better to see you with, my dear: facial recognition and privacy in online social networks, IEEE Secur. Priv. 11 (3) (2013) 21–28.
[89] N. Ramzan, H. Park, E. Izquierdo, Video streaming over P2P networks: challenges and opportunities, Signal Process. Image Commun. 27 (5) (2012) 401–411.
[90] N. Tran, J. Li, L. Subramanian, S.S. Chow, Optimal sybil-resilient node admission control, in: Proceedings of the INFOCOM, IEEE, 2011, pp. 3218–3226.
[91] N. Venkatachalam, R. Anitha, A multi-feature approach to detect Stegobot: a covert multimedia social network botnet, Multimed. Tools. Appl. 76 (4) (2017) 6079–6096.
[92] O. Peled, M. Fire, L. Rokach, Y. Elovici, Entity matching in online social networks, in: Proceedings of the International Conference on Social Computing (SocialCom), 2013, pp. 339–344.

[93] O. Van Laere, S. Schockaert, B. Dhoedt, Georeferencing Flickr resources based on textual meta-data, Inf. Sci. 238 (2013) 52–74.
[94] P. Gao, N.Z. Gong, S. Kulkarni, K. Thomas, P. Mittal, Sybilframe: a defense-in-depth framework for structure-based sybil detection, arXiv preprint arXiv:1503.02985 (2015) 1–17.
[95] P. Savla, L.D. Martino, Content analysis of privacy policies for health social networks, in: Proceedings of the International Symposium on Policies for Distributed Systems and Networks (POLICY), IEEE, 2012, pp. 94–101.
[96] Q. Shen, Y. Yang, Z. Wu, D. Wang, M. Long, Securing data services: a security architecture design for private storage cloud based on HDFS, Int. J. Grid Util. Comput. 4 (4) (2013) 242–254.
[97] R. Heatherly, M. Kantarcioglu, B. Thuraisingham, Preventing private information inference attacks on social networks, IEEE Trans. Knowl. Data Eng. 25 (8) (2013) 1849–1862.
[98] R. Jeyaraman, Fighting spam with BotMaker, (https://blog.twitter.com/2014/fighting-spam-with-botmaker). Online; accessed 04 April 2017.
[99] R. Krishnan, Facebook's latest feature Alerts You if Someone Impersonates Your Profile, (http://thehackernews.com/2016/03/fake-facebook-account.html). Online; accessed 04 April 2017.
[100] R. Petrlic, S. Sekula, C. Sorge, A privacy-friendly architecture for future cloud computing, Int. J. Grid Util. Comput. 4 (4) (2013) 265–277.
[101] S. Deliri, M. Albanese, Security and privacy issues in social networks, in: A. Picariello, F. Schreiber, L. Tanca (Eds.), Data Management in Pervasive Systems, Data-Centric Systems and Applications, Springer, 2015, pp. 195–209.
[102] S. Kaur, S. Singh, S. Kaushal, A.K. Sangaiah, Comparative analysis of quality metrics for community detection in social networks using genetic algorithm, Neural Netw. World 26 (6) (2016) 625–641.
[103] S. Lee, J. Kim, Warningbird: a near real-time detection system for suspicious urls in twitter stream, IEEE Trans. Dependable Secure Comput. 10 (3) (2013) 183–195.
[104] S. Marlow, Fighting Spam with Haskell, (https://code.facebook.com/posts/745068642270222/fighting-spam-with-haskell/). Online; accessed 04 April 2017.
[105] Software informer, Image Distortion Tool Downloads, (http://image-distortion-tool.en.informer.com/). Online; accessed 03 April 2017.
[106] Sophos, Security threat report 2011, (https://tavaana.org/sites/default/files/sophos-security-threat-report-2011.pdf). Online; accessed 04 April 2017.
[107] S. Reimann, M. Dürmuth, Timed revocation of user data: long expiration times from existing infrastructure, in: Proceedings of the ACM Workshop on Privacy in the Electronic Society, ACM, 2012, pp. 65–74.
[108] S. Singh, P.K. Sharma, S.Y. Moon, J.H. Park, Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions, J. Ambient Intell. Hum. Comput. (2017) 1–18, doi:10.1007/s12652-017-0494-4.
[109] S. Singh, Y.S. Jeong, J.H. Park, A survey on cloud computing security: issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222.
[110] Statista, Number of social media users worldwide from 2010 to 2020 (in billions), (https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/). Online; accessed 03 April 2017.
[111] S. Villata, L. Costabello, N. Delaforge, F. Gandon, A social semantic web access control model, J. Data. Semant. 2 (1) (2013) 21–36.
[112] S. Yeong Jeong, Y.S. Koh, G. Dobbie, Phishing Detection on Twitter Streams, in: Proceedings of the Pacific-Asia Conference on Knowledge Discovery and Data Mining, Springer International Publishing, 2016, pp. 141–153.
[113] Symantec, Internet Security Threat Report, (https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf). Online; accessed 04 April 2017.
[114] T.N. Jagatic, N.A. Johnson, M. Jakobsson, F. Menczer, Social phishing, Commun. ACM. 50 (10) (2007) 94–100.
[115] T. Shcherbakova, M. Vergelis, N. Demidova, Spam and Phishing in Q2 2015, (https://cdn.securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf). Online; accessed 04 April 2017.
[116] T. Stein, E. Chen, K. Mangla, Facebook immune system, in: Proceedings of the 4th Workshop on Social Network Systems, ACM, 2011, pp. 8–16.
[117] V. Kacholia, A. Garg, D. Stoutamire, Spam detection for user-generated multimedia items based on concept clustering, U.S. Patent No. 9,208,157, 2015.
[118] V. Natarajan, S. Sheen, R. Anitha, Multilevel analysis to detect covert social botnet in multimedia social networks, Comput. J. 58 (4) (2015) 679–687.
[119] W.B. Jaballah, M. Mosbah, H. Youssef, A. Zemmari, Lightweight secure group communications for resource constrained devices, Int. J. Space-Based Situated Comput. 5 (4) (2015) 187–200.
[120] W. Wei, F. Xu, C.C. Tan, Q. Li, SybilDefender: a defense mechanism for Sybil attacks in large social networks, IEEE Trans. Parallel Distrib. Syst. 24 (12) (2013) 2492–2502.
[121] W. Luo, J. Liu, J. Liu, C. Fan, An analysis of security in social networks, in: Proceeding of the Eighth International Conference on Dependable, Autonomic and Secure Computing, 2009, DASC'09, IEEE, 2009, pp. 648–651.
[122] W. Xu, F. Zhang, S. Zhu, Toward worm detection in online social networks, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACM, 2010, pp. 11–20.
[123] X. Jin, C. Lin, J. Luo, J. Han, A data mining-based spam detection system for social media networks, in: Proceedings of the VLDB Endowment, 4, 2011, pp. 1458–1461.
[124] X. Liu, Q. Liu, T. Peng, J. Wu, Dynamic access policy in cloud-based personal health record (PHR) systems, Inf. Sci. 379 (2017) 62–81.
[125] X. Xiao, C. Chen, A.K. Sangaiah, G. Hu, R. Ye, Y. Jiang, CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks, Future Gen. Comp. Sy. (2017). https://doi.org/10.1016/j.future.2017.01.035.
[126] Zephoria Digital Marketing, The Top 20 Valuable Facebook Statistics – Updated May 2016, (https://zephoria.com/top-15-valuable-facebook-statistics/). Online; accessed 04 April 2017.
[127] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, A.H. Wang, Twitter spammer detection using data stream clustering, Inf. Sci. 260 (2014) 64–73.
[128] Z. Shan, H. Cao, J. Lv, C. Yan, A. Liu, Enhancing and identifying cloning attacks in online social networks, in: Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, ACM, 2013, pp. 59–65.
[129] Z. Zhang, K. Wang, A trust model for multimedia social networks, Soc. Netw. Anal. Min. 3 (4) (2013) 969–979.

Shailendra Rathore He is a Ph.D. student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, South Korea. Currently, he is working in Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broadly research interest includes Information and Cyber Security, SNS, Artificial Intelligence, Digital Forensic, IoT. Previous to joining Ph.D. at SeoulTech, he has worked as an Executive – Technology at Crompton Greaves Global R & D, Mumbai, India from June, 2013 to July, 2014. He received his M.E. in Information Security from Thapar University, Patiala, India and B.Tech. in Computer Engineering from Rajasthan Technical University, Kota, Rajasthan, India.

Pradip Kumar Sharma He is a Ph.D. scholar at the Seoul National University of Science and Technology. He works in the Ubiquitous Computing & Security Research Group under the supervision of Prof. Jong Hyuk Park. Prior to beginning the Ph.D. program, he worked as a software engineer at MAQ Software, India. He worked on a variety of projects, proficient in building large-scale complex data warehouses, OLAP models and reporting solutions that meet business objectives and align IT with business. He received his dual Master's degree in Computer Science from the Thapar University, in 2014 and the Tezpur Univerity, in 2012, India. His current research interests are focused on the areas of ubiquitous computing and security, cloud computing, SDN, SNS, and IoT. He is also reviewer of Journal of Supercomputing (JoS).

Vincenzo Loia Dr. Vincenzo Loia received B.S. degree in computer science from University of Salerno, Italy in 1985 and the M.S. and Ph.D. degrees in computer science from University of Paris VI, France, in 1987 and 1989, respectively. From 1989 he is Faculty member at the University of Salerno where he teaches Situational Awareness, IT Project & Service Management. His current position is as Full Professor of Computer Science at Department of Management and Innovation Systems. He was principal investigator in a number of industrial R&D projects and in academic research projects. He is author of over 390 original research papers in international journals, book chapters, and in international conference proceedings. He edited four research books around agent technology, Internet, and soft computing methodologies.

Young-Sik Jeong Dr. Jeong is a professor in the Department of Multimedia Engineering at Dongguk University in Korea. He is a president of Korea Information Processing Society. His research interests include cloud computing, mobile computing, IoT (Internet of Things), and wireless sensor network applications. He received his B.S. degree in Mathematics and his M.S. and Ph.D. degrees in Computer Science and Engineering from Korea University in Seoul, Korea in 1987, 1989, and 1993, respectively. Since 1993, he has been serving as an IEC/TC 100 Korean Technical Committee member, as the IEC/TC 108 Chairman of Korean Technical Committee, and as an ISO/IEC JTC1 SC25 Korean Technical Committee member. Also He has been served as Editor-in-Chief of Journal of Information Processing Systems, an associate editor of international Journal of Communication Systems, Journal of supercomputing, Journal of Internet Technology, Journal of Human-centric Computing, and so on. He is also is a member of the IEEE. Personal website: http://ucloud-lab.dongguk.edu.

Jong Hyuk Park Dr. Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chairs, program committee, or organizing committee chair for many international conferences and workshops. He is a founding steering chair of some international conferences – MUE, FutureTech, CSA, UCAWSN, etc. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, The Journal of Information Processing Systems (JIPS) by KIPS, and Journal of Convergence (JoC) by KIPS CSWRG. He is Associate Editor / Editor of 14 international journals including 8 journals indexed by SCI(E). In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Hindawi, Emerald, Inderscience. His research interests include security and digital forensics, Human-centric ubiquitous computing, context awareness, multimedia services, etc. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, and PDCAT-11. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. Dr. Park' s research interests include Human-centric Ubiquitous Computing, Vehicular Cloud Computing, Information Security, Digital Forensics, Secure Communications, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.