

Social Network Security: Issues, Challenges, Threats, and Solutions

2017-09-11

Presented by

Shailendra Rathore

(rathoreshailendra@seoultech.ac.kr)

Abstract

- A comprehensive survey of different security and privacy threats that target every user of social networking sites.
- Various threats that arise due to the sharing of multimedia content within a social networking site.
- Discuss current state-of-the-art defense solutions that can protect social network users from these threats.
- 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.

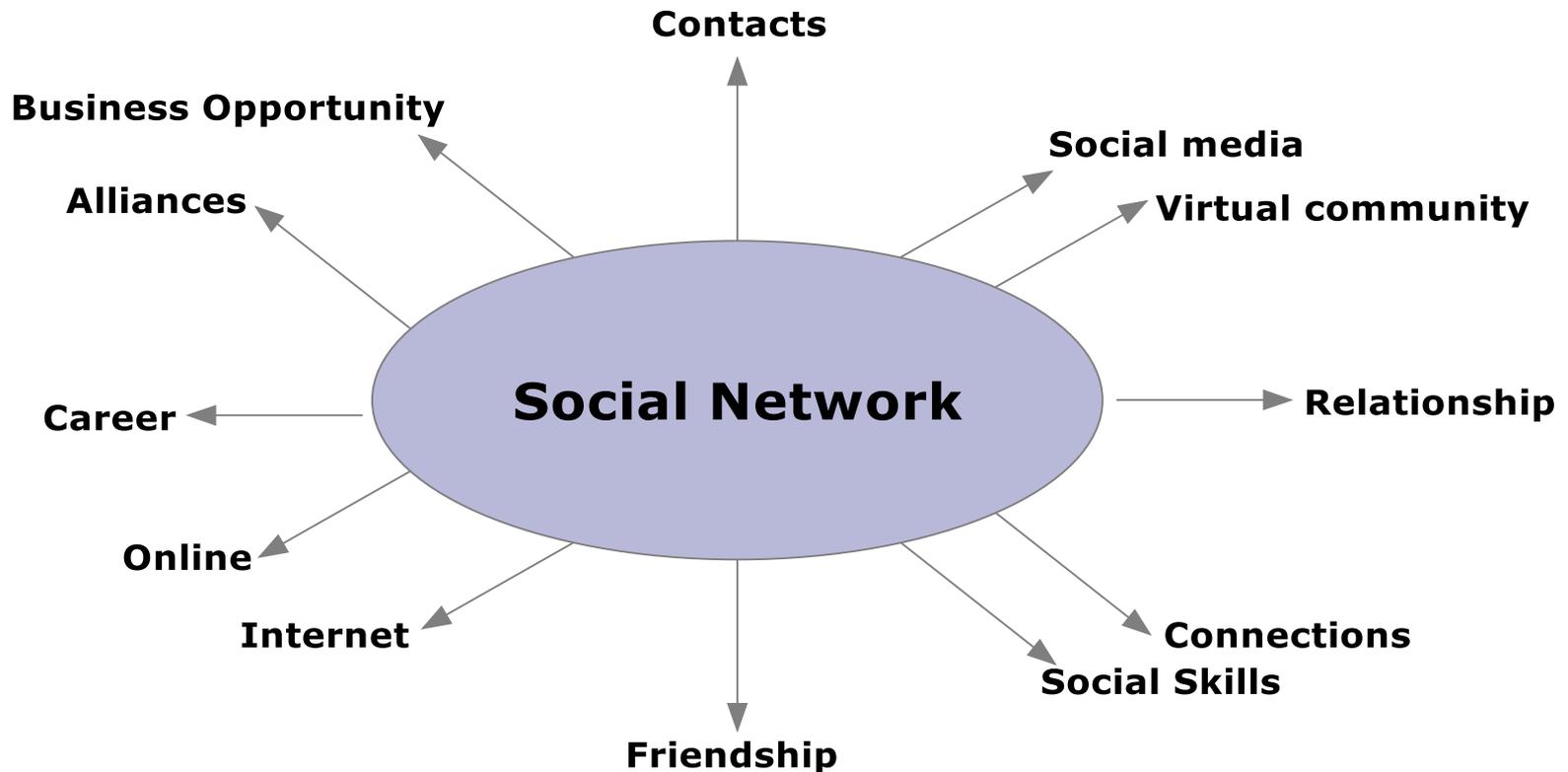


Fig.1. The fundamental concept of SNSs.

1. Introduction

- Data sharing is another key feature of a SNS where users are able to share their interests, videos, photos, activities, and so on.
- 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 seconds 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.
- Recently, Facebook CEO Mark Zuckerberg's Pinterest and Twitter accounts were hacked, where the hacker used his LinkedIn password of "dadada." [67].

1. Introduction

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
Hongyu Gao et al. [38]	2011	Yes	Limited	No	Yes	Limited
Ed Novak et al. [23]	2012	Yes	Limited	Limited	Yes	Limited
Long Jin et al. [66]	2013	Limited	Limited	No	Limited	Limited
Michael Fire et al. [74]	2014	No	Yes	No	Yes	Yes
Imrul Kayes et al. [42]	2015	Limited	Yes	No	Yes	Limited
Sepideh Deliri et al. [101]	2015	No	Limited	No	Limited	No

2. SNS security issues and challenges

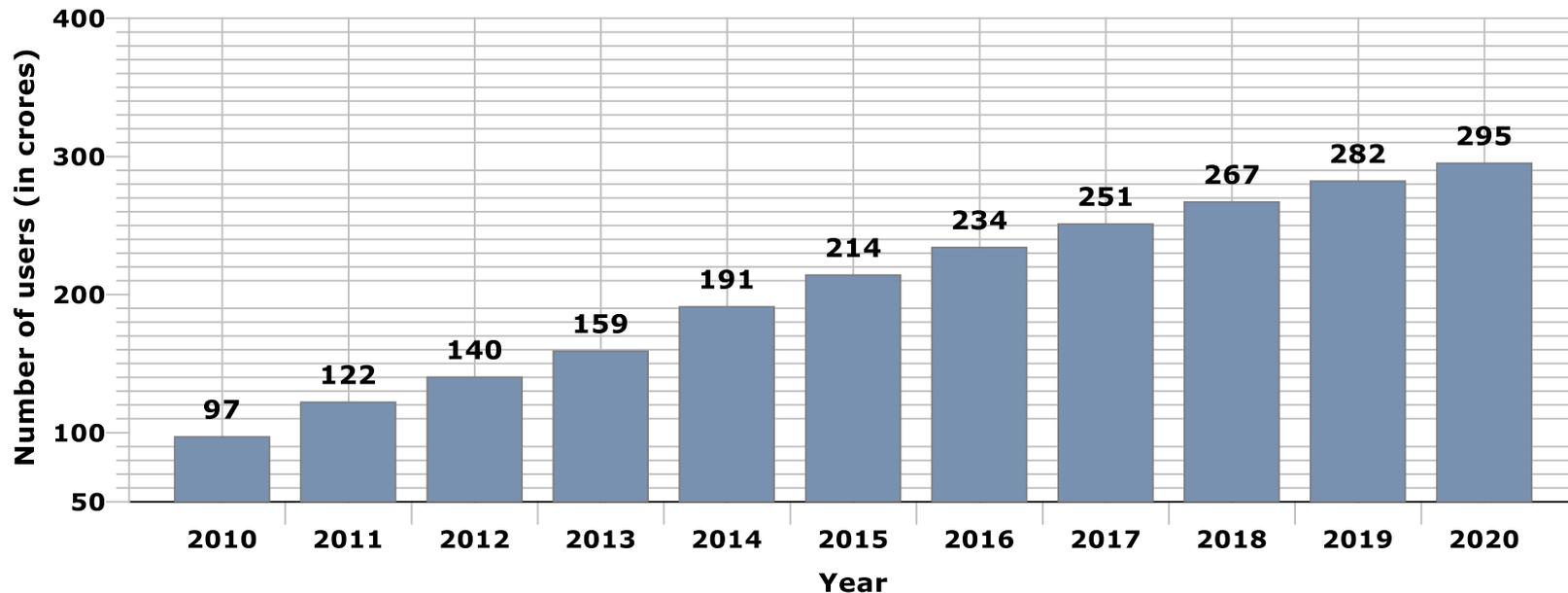


Fig.2. Number of SNSs user worldwide from 2010 to 2016 with prediction until 2020 (Statista's report [110])

2. SNS security issues and challenges

- Sophos' security threat report 2011 reveals that Facebook has the biggest security risks that are significantly ahead of MySpace, Twitter, and LinkedIn.
- Facebook 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.

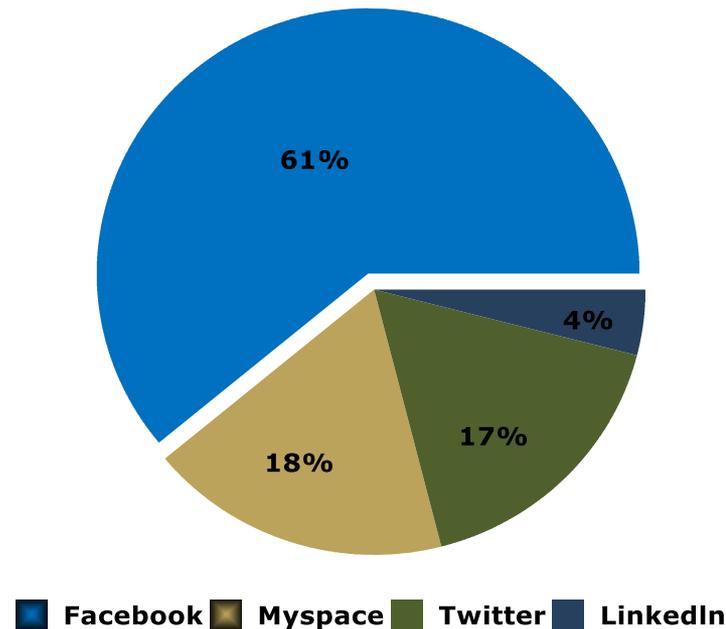


Fig.3. Sophos security threat report- 2011.

2. SNS security issues and challenges

- 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.
- 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.

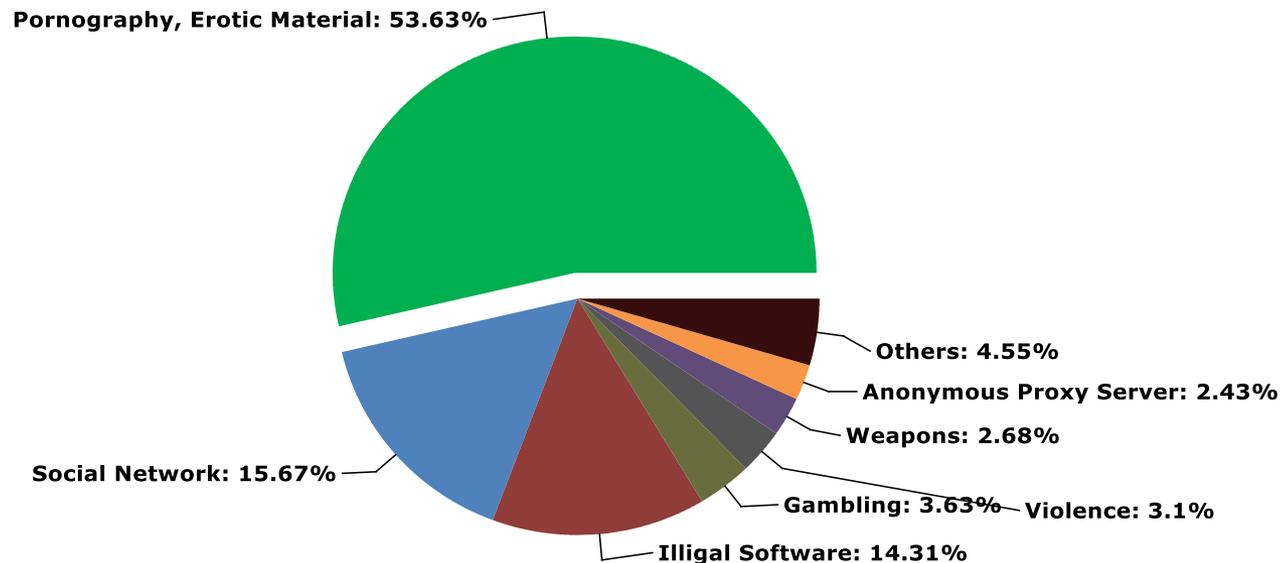


Fig.4. Analysis of parental control component triggered by various real world security risks.

2. SNS security issues and challenges

- 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].

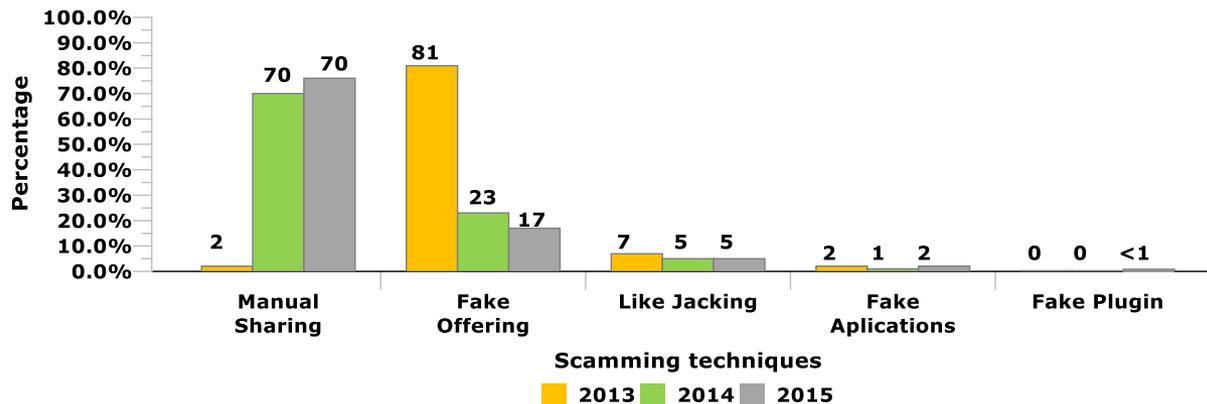


Fig.5. The percentage utilization of various SNSs scamming techniques for last three years.

2. SNS security issues and challenges

Internet threats

- Identity theft, spamming, phishing, online predators, internet fraud, and other cybercriminal attacks
- Exploit a user's confidential data, such as social security number, full name, telephone number, and address
- Goal is to obtain a user's financial information, such as user's credit card details.

Reputation and credibility issues

- SNSs can damage the reputation of businesses and huge organizations
- Users may lose their job chances due to incorrect data in their SNS profile.

Profiling issues

- Companies gather data from SNS, for constructing complete profiles of individuals with the intention of selling products.
- Gathered 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

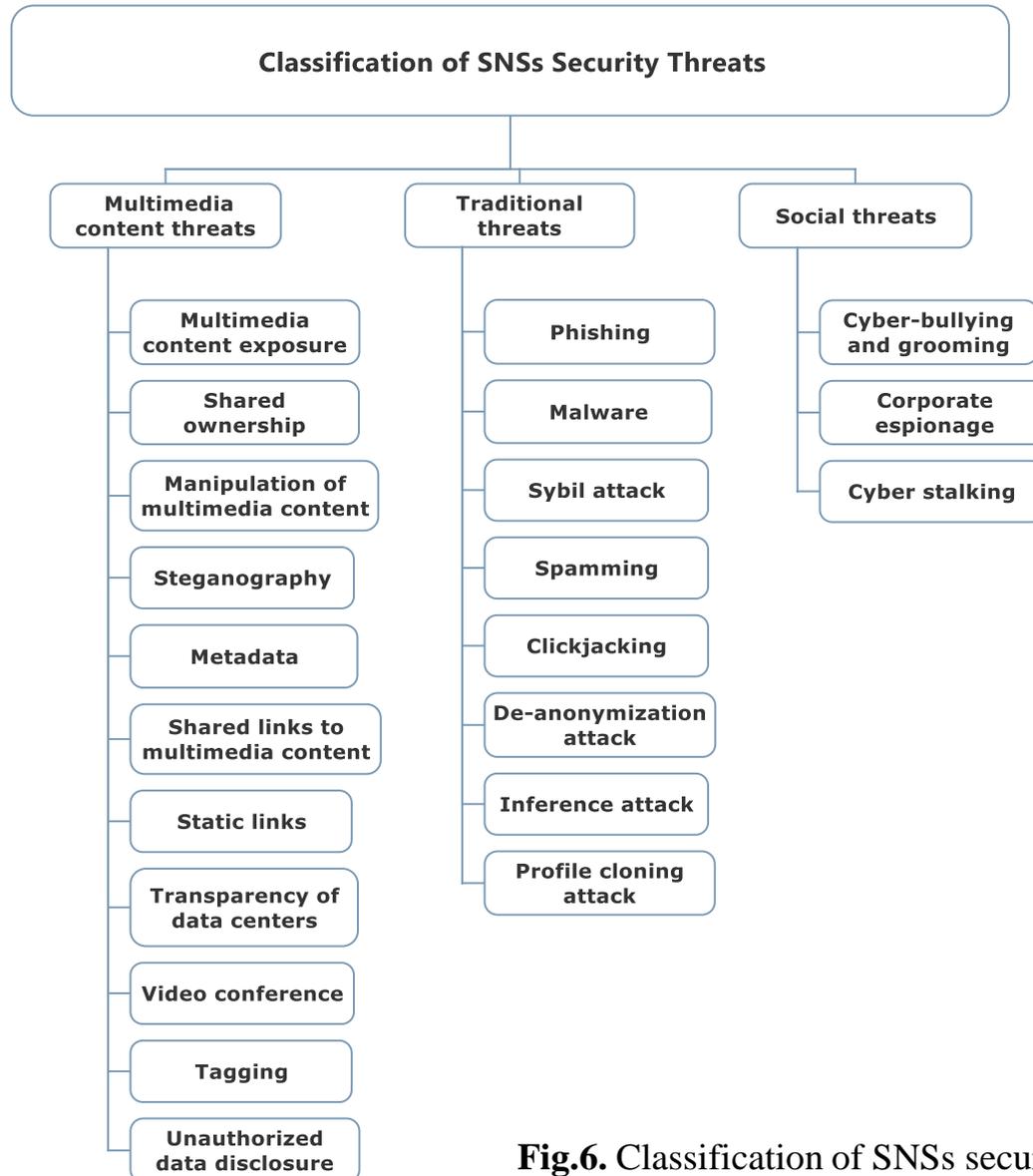


Fig.6. Classification of SNSs security threats.

Multimedia Content Threats

Type of threats	Description	Impacts	References
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]

Multimedia Content Threats

Type of threats	Description	Impacts	References
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

Type of threats	Description	Impacts	References
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]
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]

Traditional Threats

Type of threats	Description	Impacts	References
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

Type of threats	Description	Impacts	References
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]

4. Analysis of SNS security solutions

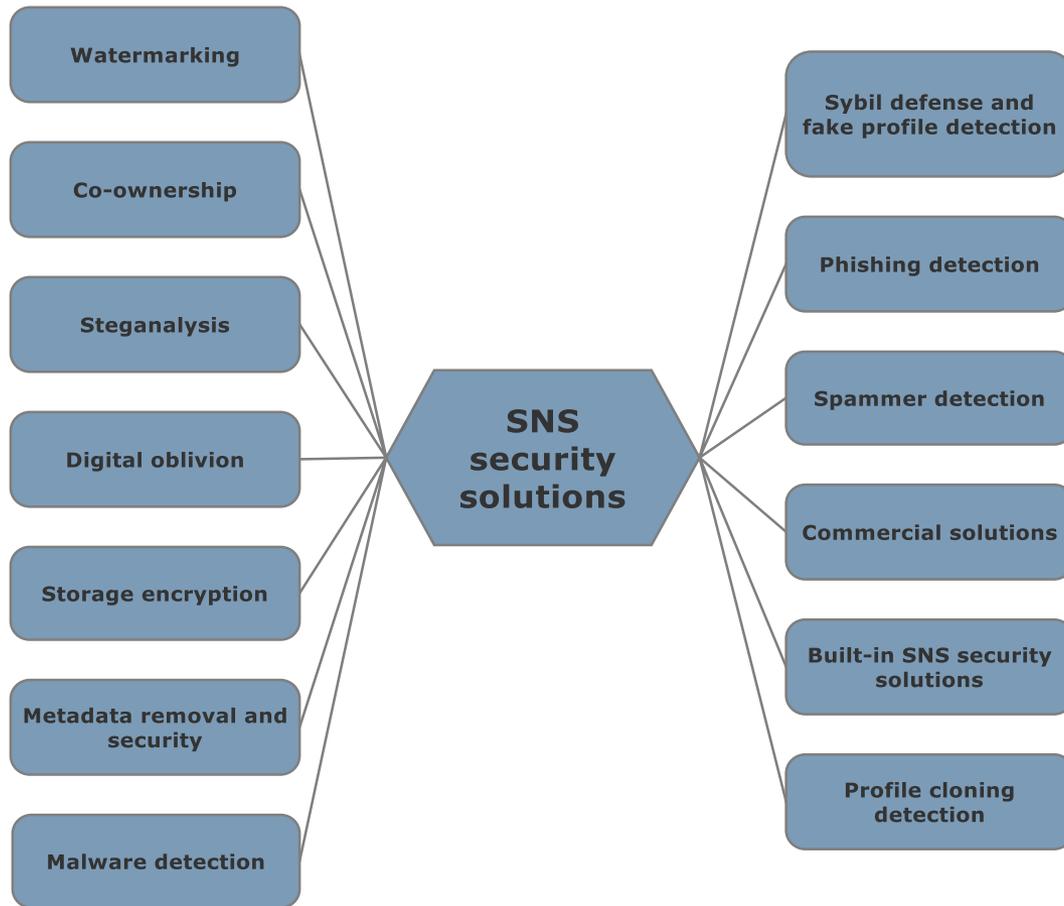


Fig.7. Security and privacy solutions for SNS

4. Analysis of SNS security solutions

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]

4. Analysis of SNS security solutions

Solution	Description	Key methods	References
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 SybillInfer, Bayesian inference method.	[27, 32, 90, 94, 120]
Phishing detection	It includes various anti-phishing methods to detect and prevent phishing attacks in SNSs.	Machine learning technique, PhishAri technique, WarningBird system, Two-phase unsupervised learning algorithm.	[1, 45, 79, 103, 112]

4. Analysis of SNS security solutions

Solution	Description	Key methods	References
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.	Face recognition technology, CloneSpotter system.	[30, 99, 128]

4. Analysis of SNS security solutions

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

5. Future direction and suggestion of security responses

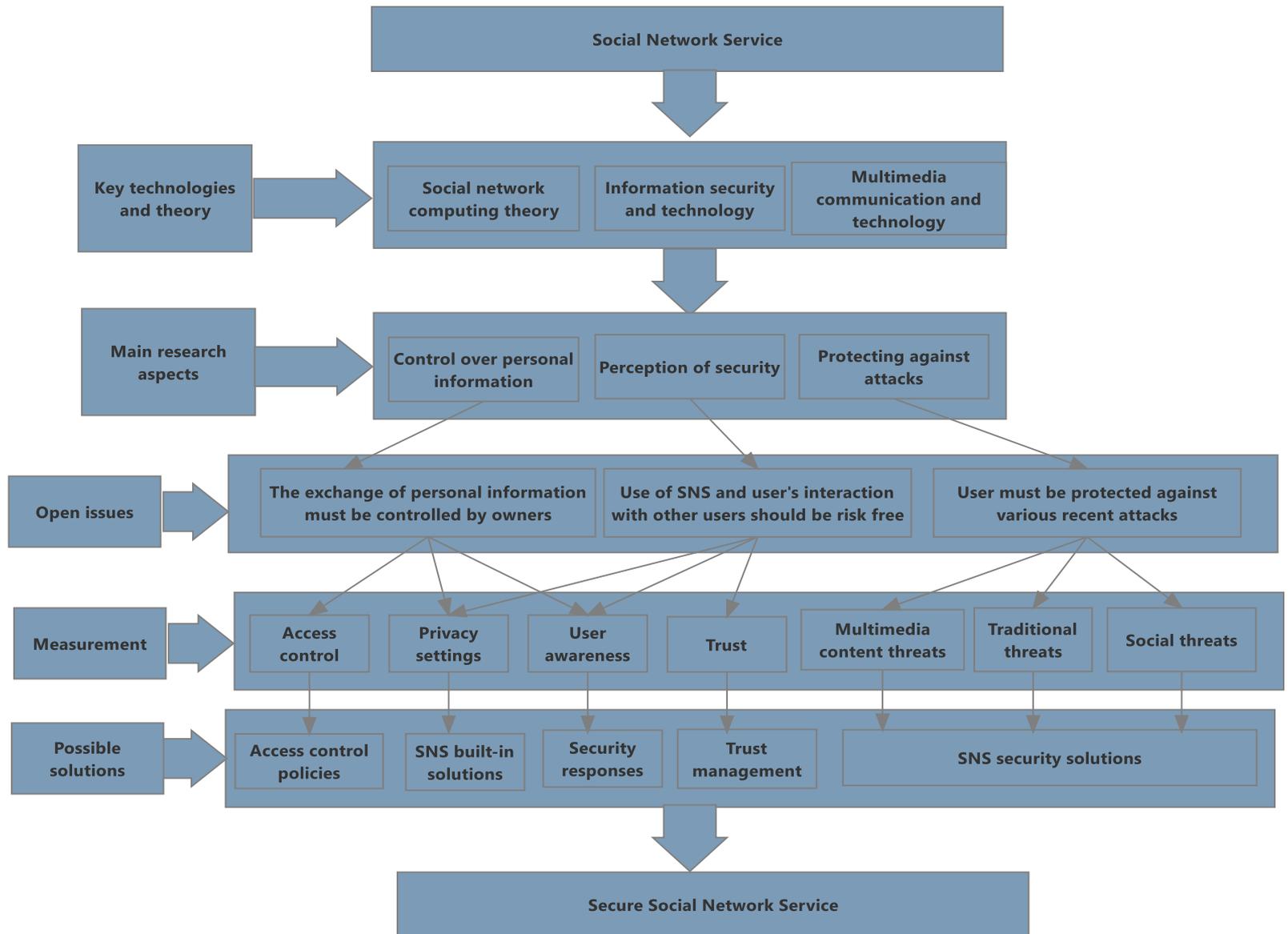


Fig.8. Proposed research roadmap to measure and optimize the security of SNS

5. Future direction and suggestion of security responses

Comparison of various security attacks on SNSs

Parameters Attacks	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

5. Future direction and suggestion of security responses

Comparison of various security attacks on SNSs

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
Attacks							
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

SNSs security threats and their corresponding 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 espionage	Cyber stalking
Solutions																						
Watermarking			✓								✓											✓
Co-ownership		✓								✓												
Steganalysis				✓										✓	✓							
Digital oblivion	✓					✓						✓	✓			✓						
Storage encryption							✓	✓			✓						✓	✓	✓	✓	✓	✓
Metadata removal and security	✓				✓												✓	✓				
Malware detection						✓			✓				✓		✓	✓						
Sybil defense and fake profile detection										✓	✓		✓	✓	✓	✓			✓	✓		✓
Phishing detection						✓						✓	✓	✓	✓	✓						

SNSs security threats and their corresponding solutions.

Threats	Solutions	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
	Spammer detection				✓		✓				✓		✓	✓	✓	✓	✓						
	FB phishing protector				✓		✓						✓				✓						
	Social guard privacy scan	✓				✓					✓				✓			✓	✓	✓	✓		✓
	Net Nanny social														✓						✓		✓
	Minor monitor														✓						✓		✓
	Web security software				✓		✓						✓	✓		✓	✓						
	Social protection application	✓	✓			✓		✓				✓											

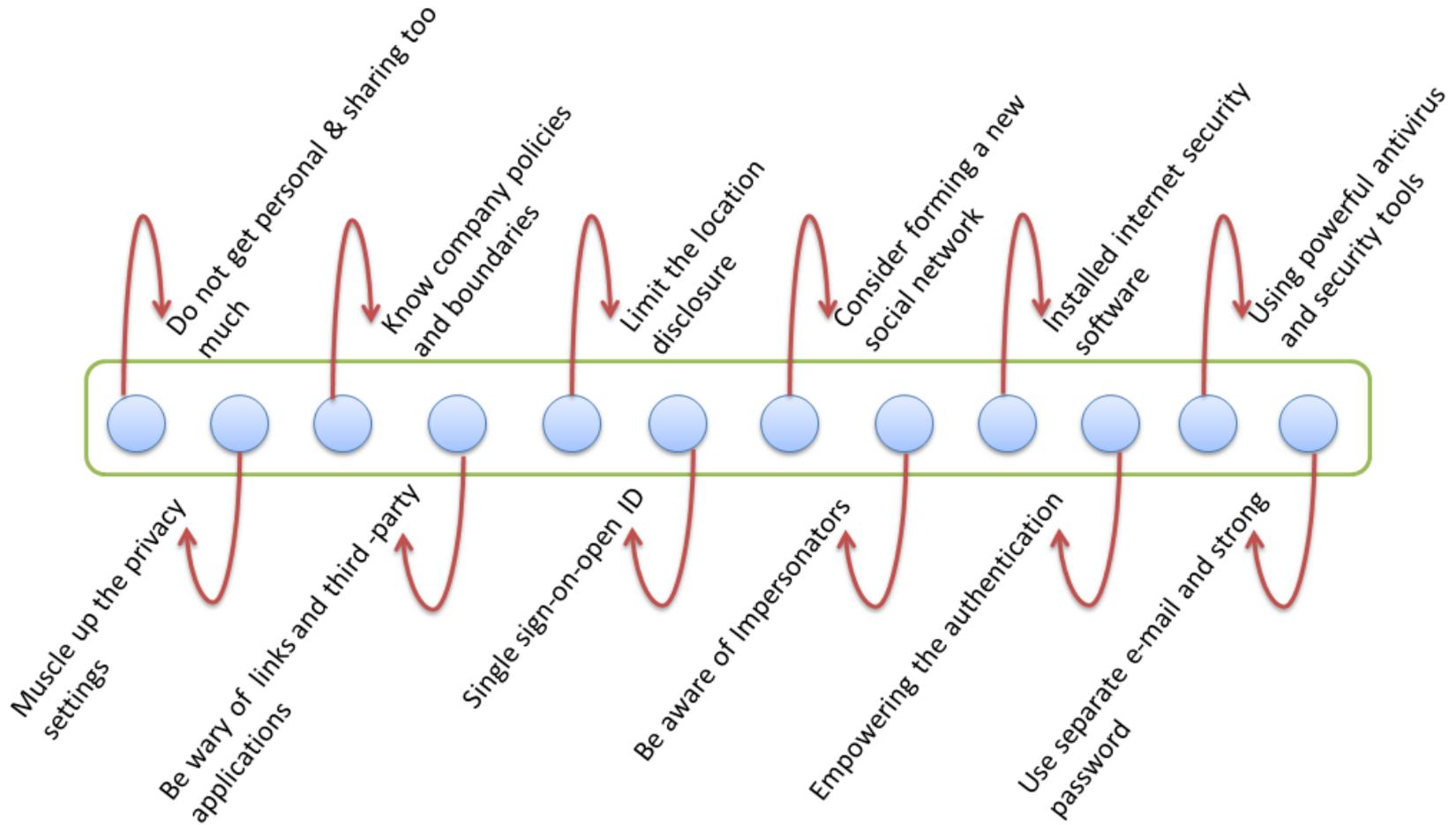


Fig.9. Security responses for SNSs users

6. Conclusion

- Studied 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.
- Summarized various recent attack statistics and security reports that have been released by several security organizations and blogs.
- Described three classes of threats: Multimedia content threats, Traditional threats, and Social threats.
- Conducted a analysis of the possible and existing schemes for protecting SNS users against these threats.
- compared various SNS security attacks based on certain parameters
- Discussed some open research challenges and future direction.
- Presented some easy-to-apply response techniques that can be easily followed by SNS users to better protect themselves against various security threats.

Findings

- 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.

Reference

- Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, and Jong Hyuk Park. "Social Network Security: Issues, Challenges, Threats, and Solutions." *Information Sciences*, vol. 421, pp. 43-69, 2017

Question
???