Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review

Azah Anir Norman
Department of Information Systems
Faculty of Computer Science and Information Technology
University of Malaya, 50603 Kuala Lumpur
azahnorman@um.edu.my

Suraya Hamid
Department of Information Systems
Faculty of Computer Science and Information Technology
University of Malaya, 50603 Kuala Lumpur
suraya_hamid@um.edu.my

Maw Maw
Department of Information Systems
Faculty of Computer Science and Information Technology
University of Malaya, 50603 Kuala Lumpur
hanifa@um.edu.my

Suraya Ika Tamrin
Department of Information Systems
Faculty of Computer Science and Information Technology
University of Malaya, 50603 Kuala Lumpur
surayaika@siswa.um.edu.my

***Abstract*—During the decade, interactions among people have gradually changed as a result of the popularity, availability and accessibility of social networking sites (SNSs). SNSs enhance our lives in terms of relaxation, knowledge, and communication. On the other hand, the information security and privacy of SNS users have been threatened with most users not aware of this fact. The rate of cyber-attack committed via SNS is dramatically high. Finding a solution to provide better security for social network users has become a major challenge. This review is conducted with the objective to collect and investigate all credible and effective researches that have studied security problems and solutions on SNSs. We aim to extract and discuss the prominent security features and techniques in the selected research articles to provide researchers and practitioners with a concise collection of the security solutions. In this review, we conduct a secondary study by accessing the previous studies devoted to security threats of SNSs and new security techniques to protect them from attacks. We apply the standard guidelines of systematic literature review by working thoroughly on 84 previous studies including journal papers and conference proceedings published in high impact journals. The results show that 2013 is the peak period in which security problems on SNSs obtained attentions from researchers and 23 significant security problems in SNSs were discovered. Facebook and Twitter are the two SNSs mostly referred to by researchers regarding security problems. We found that people (users) and SNSs themselves are the two main causes for today's security and privacy issues on SNSs. In conclusion, the security and privacy issues on SNSs are still an unsolved problem and there is as yet no solid and complete solution for absolutely removing those issues on SNSs.**

Keywords*—Social networking sites (SNS); security; privacy; security techniques; systematic literature review (SLR)

I. INTRODUCTION

Web 1.0 has been replaced by Web 2.0. Web 2.0 was introduced in 1999 and has been used widely since 2004 [1]. Web 2.0 does not differ technically from Web 1.0. It shapes the web as a collaborative platform for all users and allows them to have two-way communication. In other words, the Web has changed from an information providing system to a more communication-oriented and community-building one.

As one of the consequences of the introduction of Web 2.0, social networking sites (SNSs) have become popular. SNSs are platforms on which people can share knowledge, interests, and hobbies among friends and can also create new friendships internationally. The very first SNS, SixDegree.com launched in 1997 [2] and there are currently more than two hundred SNSs according to the available statistics.

The statistical data show how the following numbers of monthly active users on popular SNSs: Facebook: 1.28 billion, Google+:540 million, Instagram: 200 million, LinkedIn: 187 million and Pinterest: 40 million respectively [3]. According to reports, over 1.8 billion Internet users have accessed various social networks in 2014. That means that 26% of the world population is involved in social activities on SNSs [4].

As a result, the rate of user-generated data on the web has expanded massively. Since the most common feature of an SNS is the ability to create and share a personal profile, it is easy to obtain unauthorized access to the personal data of SNS users. Thus, privacy and security problems on SNS have become an essential matter to be considered.

A. *Security on SNSs*

As with other technologies, security and privacy are the most important qualities requirements of social networks. As SNSs are web-based services, the security standards of SNSs are determined based on the security measurements of Web Service Security (WSS), the security of client and server applications that communicate across the World Wide Web. An SNS can be considered secured when the user information and personal data are prevented from being threatened by misuse, unauthorized access, interference with services and other similar threats. The common security goals on SNSs are primarily: confidentiality, integrity and availability (CIA).

New UMRG Program 2013, University of Malaya, research grant number: RP004E-13HNE

- Confidentiality is another term of privacy. It ensures that private data or sensitive information of users cannot be accessed by unauthorized users. Encryption and access control lists (ACLs) are used to enforce confidentiality [5]. Another significant method for ensuring confidentiality is to use the Secure Socket Layers/Transport Layer Security (SSL/TLS) protocols [6].
- Integrity maintains the consistency, accuracy and originality of data, preventing data from intentional or unintentional modification by unauthorized parties. Integrity is an important security measure, especially for data passed across networks. Hashing, cryptography, and message authentication codes are used to verify integrity [5].
- Availability ensures that the correct information reaches to the correct person at the correct time. In other words, the system remains available for authorized users whenever they need it [5], [6].

The sociability of SNSs potentially threatens the privacy of users' personal data. The occurrence of security and privacy problems on SNSs has prompted social service providers to attempt to solve those problems for their users by enhancing privacy preferences and options to restrict privacy levels [7].

However, the security measurements or security goals are not entirely fulfilled. Heartbleed vulnerability [8] and the recent Sony picture data leakage [9] are significant evidence for this fact. Similarly, security issues are encountered more frequently on SNSs as the number of SNSs increases. These issues motivates us to study SNS scenarios using systematic literature reviews (SLRs) [10] to determine why security issues on SNSs are still a problem and why the attempts of researchers have not fully succeeded, by investigating a number of SNS security threats and security techniques.

The remainder this paper is organized as follows. In Section 2, the details of the methods used in this SLR, and the research questions and the search and selection process of relevant sources are presented. Section 3 presents the results related to our research questions. Section 4 discusses the relevant points in detail.

II. Research Methodology

This research conducts a secondary data analysis using an SLR guided by [10]. EndNote reference management software is used for storing and referencing in order to accumulate, organize, evaluate and synthesize all of the current primary studies systematically. We follow the three main steps of SLR planning, conducting the review, and reporting the results. First, we formulate and define research questions related to security problems and techniques on SNSs. Second, we search for the relevant literature through various databases and extract related facts. Finally, we write a report of our systematic review of security issues and techniques on SNSs.

A. Research Questions

We formulated four research questions (RQs) in our SLR study as follows:

RQ1: In which year, could the researchers find the most security problems and techniques on SNSs?

RQ2: What significant security concerns and threats on SNSs have the researchers found, and what remedies have they proposed since 2004?

RQ3: On which SNSs, do researchers mostly conduct the most experiments?

RQ4: Do the proposed security mechanisms achieve the security goals on SNSs? If not, why do the proposed techniques fail?

To answer RQ1, we determine how many studies have been published in this specific area over the past decade. We compare the publications published in each year from 2004 to 2015. We assume that a decade is a sufficiently long period to answer our first RQ, but we also include the literature published in the first three months of 2015 to improve the solution.

To answer RQ2, we search the literature related to security vulnerabilities, attacks, and issues found on SNSs from journals published since 2004, as we expect a decade of studies to provide reasonable exposure. In addition, we want to know how researchers have tried to solve security problems on SNSs and what security techniques have been proposed. We classify the different security tools, mechanisms and frameworks applied on SNSs in the hope of solving the security and privacy problems. We analyze what kinds of solution were proposed in previous studies as well.

We set RQ3 because we want to know which SNSs have been suffering most from security problems. We determine this fact by examining the datasets the researchers use most and the SNSs they point out most in relation to security problems.

Regarding to RQ4, we want to analyze whether the proposed security mechanisms provide the necessary solutions to the problems. If there is still a gap between the security problems and the solutions proposed, we want to know the relevant factors. Hence, we want to identify the hidden reasons for the continuing occurrence of security issues on SNSs.

B. Search Process

Carrying out an SLR requires conducting a comprehensive literature search to determine all possible evidences from the results of previous primary studies. We decided to search manually in electronic databases. We selected five databases that collected high impact articles and that researchers have been used most for their article searches. Those five databases are shown in Table 1.

TABLE I. Databases

No	Database	Links
1.	ScienceDirect	http://www.sciencedirect.com/science/search
2.	IEEE Xplore	http://ieeexplore.ieee.org/search/advsearch.jsp
3.	ACM Digital Library	http://dl.acm.org/advsearch.cfm?
4.	SpringerLink	http://link.springer.com/advanced-search
5.	Scoupus	http://www.scoupus.com/

We search for relevant sources of literature in journals and conference proceedings from the databases listed in the table. In order to find our intended literature, we use the specific terms that are included in our research questions. Our SLR study is divided into two parts, one that deals with security problems, and one that deals with security solutions. The keywords and terms used in the search process are shown in Fig. 1.

We limited our search process, to the year from 2004 to 2014 as we assume that a decade would provide a sufficient literature for our SLR study and would cover all of the security attacks and remedies on SNSs. We refer to some online articles regarding security composition and background security architectures of SNSs. Some references of particular literature items that we found to be relevant to the scope of our study are also included in our SLR.

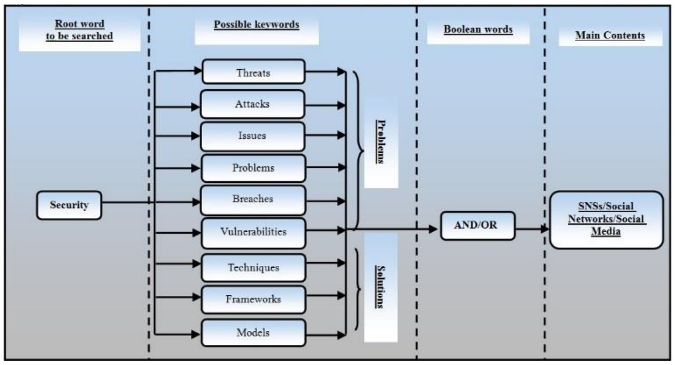

Fig. 1. Model of keywords used in the search process.

We take synonyms into account in order not to miss any relevant literature. For example, we interchange the word "threat" with five different synonyms. We use AND/OR Boolean characters to ensure that no evidence is missed. We set a search query for an efficient search as follows:

1) Security (threat OR problems OR issues OR vulnerabilities OR attacks OR breaches) "AND" (social networks OR social networking sites OR social media)

2) Security attacks AND Facebook

3) Security issues AND social networking sites

We checked through the reference list from each article and included some papers relevant to our SLR study.

C. Inclusion and Exclusion Criteria

By conducting an initial search through the use of predefined search strings, we obtained more than three hundred journal articles and conference proceedings papers. We set selection criteria on inclusion and exclusion of articles to choose the most relevant literature. The criteria are shown in Table 2.

Some literature appeared seemed to be relevant from checking the titles or keywords but was removed from the preliminary selection, because reading the abstract and introductions revealed that they deviated from the directions in responding to the research questions. The steps of refining qualified literature and results are shown in Fig. 2.

TABLE II. INCLUSION AND EXCLUSION CRITERIA

Inclusion Criteria		Exclusion Criteria	
1	Relevant directly to the research questions set	1	Written in non-English
2	Published between 2004 to 2014	2	Emphasized only on mobile social networks
3	Emphasized on security threats or attacks encountered only in social networking sites	3	Focused on people's behaviors in usage of social networks
4	Discussed about the ways to solve the security problems including both of technical mechanisms and policies or awareness	4	Focused on information diffusion in social networks
		5	Not answered to the research questions though the keywords are matched
		6	Chapters of the books and reviews

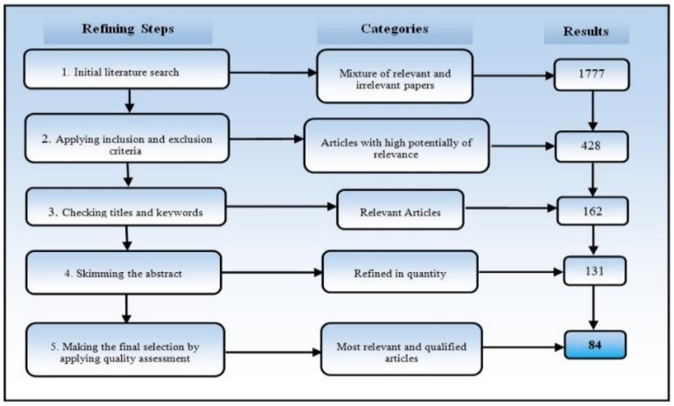
Refining Steps
Categories
Results
1. Initial literature search
Mixture of relevant and irrelevant papers
1777
2. Applying inclusion and exclusion criteria
Articles with high potentially of relevance
428
3. Checking titles and keywords
Relevant Articles
162
4. Skimming the abstract
Refined in quantity
131
5. Making the final selection by applying quality assessment
Most relevant and qualified articles
84

Fig. 2. Steps of refining qualified literature and results.

D. Quality Assessment

In this section, we discuss how we obtain the final selection of the literature. We conduct quality assessment on the articles collected, because the number collected is substantial and we want to include only those that are qualified and most relevant to the research area. We prepare a set of questionnaires in accordance with the guidelines of [10].

QA1: Do those studies actually focus on security problems or remedies for security problems?

QA2: Do those security problems or solutions emphasize only the domain of SNSs?

QA3: Are the security techniques or solutions discussed clearly with the aim of answering the research questions?

The quality of the studies is decided based on a score for the listed questionnaires. We follow the scoring procedure applied in [11] if "yes" the score is 1; if "partial" the score is 0.5; and if "no" the score is 0 for each questionnaire. Studies with scores of less than 2 are not considered for secondary study. The quality scores for the selected studies are listed in Table 3 (refer appendix).

E. Data Extraction

From each article, we extract the following information for analyzing the results. These facts are also very important and reflective in investigating our research questions.

- Title of the paper
- Year of publication
- Source/Library
- Authors
- Type of article (journal or conference proceeding and its name)
- Principal Security problem(s)
- Category of attack (if there is a specific name)
- Type of attack(s) (Human-based or technology-based)
- Affected standard principles of security (confidentiality, integrity, privacy, availability)
- Proposed solutions and details
- Type of solutions
- SNS(s) concerned

F. *Data Analysis*

The analysis of the principal studies is summarized in this section. We investigate which year was the most productive year in the researchers' determination of security and privacy issues (RQ1); the major security problems, including attacks, privacy leaks and potential attacks and the remedies for those problems proposed by the previous studies (RQ2); the SNSs experiencing the most problems, by checking the number of studies conducted on each SNS (RQ3); and the evidence showing which SNS security problems are ongoing and the main causes of SNS security issues (RQ4).

III. Results

In this section, we summarize our findings in the tables, graphs and text. Fig. 3 shows the statistical data for the number of publications in ten years. These facts helped us to answer RQ1. We show the percentage difference between journal and conference papers in Fig. 4.

The security issues/problems, and how they can harm SNS users or an SNS itself are listed in Table 4 (refer appendix), along with brief explanations. We identified four principal types of attacks that were dealt with in the previous studies conducted by previous researchers. The five most common attacks on SNSs are summarized in Section 4.2. Table 5 lists information regarding four principal groups of attacks on SNSs and the studies that discovered those attacks. Meanwhile, Table 6 (refer appendix) summarizes the summary of problem solving techniques, tools, models and frameworks proposed by the authors. Table 7 (refer appendix) organizes the attack models proposed by the researchers for penetrating-testing (pen-testing) purposes in order to test the robustness of the system.

The usage of a particular SNS in percentage is shown in a pie chart in Fig. 5.

TABLE V. Description of Attack/Issue

No.	Category of Attacks/issues	References
1	Direct attacks	[12], [21], [25], [27]-[29], [38], [42], [47], [50], [52], [54], [61], [64], [68], [72], [91]
2	Passive attacks	[12]-[14], [16]-[18], [23], [30]-[32], [41], [44], [46], [48], [51], [53], [57], [59], [60], [79], [81], [82], [85], [87]
3	Privacy issues	[7], [12], [15], [25], [36], [39], [42], [43], [45], [49], [55], [58], [62], [68], [73]-[78], [80], [84], [86], [88], [90], [92], [95]
4	Vulnerability	[61], [65], [94]

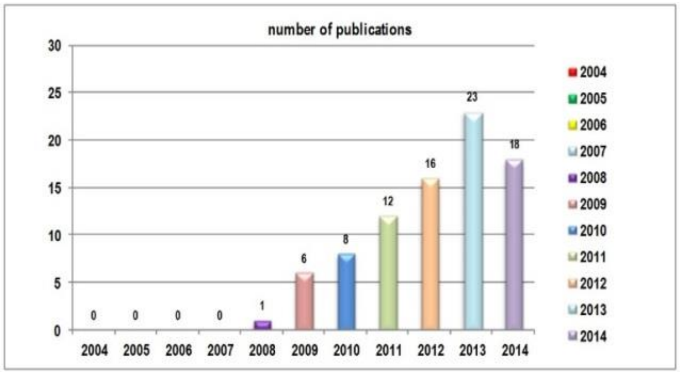

Fig. 3. Statistical data of number of publications in each year.

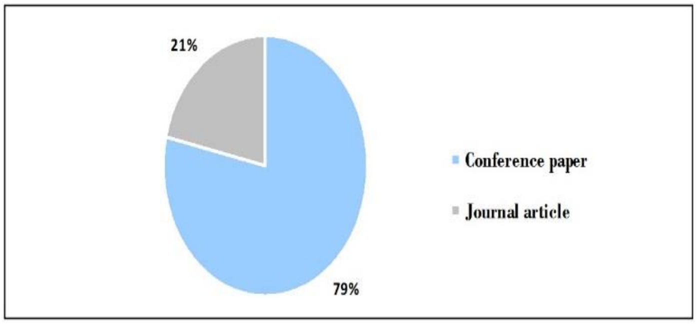

Fig. 4. Percentage of conference papers and journal articles published from 2004-2014.

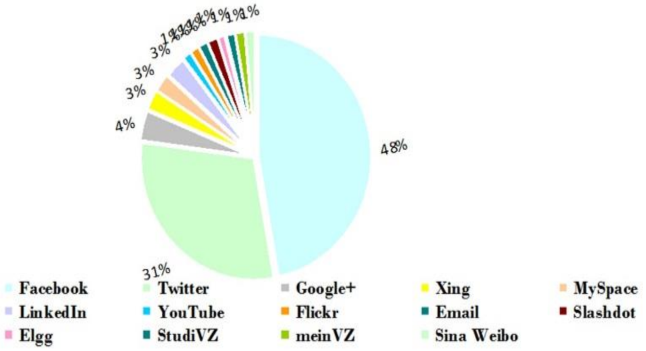

Fig. 5. Various SNSs and rate of usage by researchers.

IV. Discussion

A. In Which Year, Could the Researchers Could Determine the Most Security Problems on SNSs and Propose Techniques?

We obtained 84 relevant studies by applying the selection criteria and quality assessment described in Table 3 (refer appendix). Of these, we identified 17 journal papers and 67 conference papers.

According to the statistical data shown in Fig. 4, neither journal articles nor conference papers relevant to this domain were published from 2004 to 2007. In addition, there was only one publication in the field of SNS security problems and solutions in 2008. However, in 2009 the number of publications had by five times in comparison to 2008. From this information, we concluded that security problems on SNSs were not very common and only very slight attention had been paid to this domain until 2008.

In 2010, the rate of publication progressively increased compared with 2009. The number of publications rose almost 50% higher than in 2009. In the following years, from 2011 and 2012, the rate of publication was obviously high in contrast to the publication rate in the late 2000s. As the number of publications in 2012 rose to 16, it was exactly double that of 2010. The rate gradually increased and peaked in 2013 with a total of 23 publications. The number of publications slightly declined during 2014, as the publications decreased almost 20% in comparison 2013.

Referring to the increase in publication rate, we discovered two facts: the SNS usage has increased since 2009 and more security problems have arisen on SNSs along with its increasing use. As the rate of publication began decreasing in 2014, we can expect that security problems might lessen in the future.

We found a substantial difference in the numbers of journal publications and conference papers. As shown in Fig. 3, there is a dramatic difference between conference and journal article publication in the area of security problems and mechanisms for solving them. Though the numbers are different, we can see the eagerness of researchers in the area of SNS security.

B. What Significant Security Concerns and Threats on SNSs have Researchers Found, and What Remedies have they Proposed Since 2004?

We categorized our selected studies into three main groups: 1) studies that have only found security and privacy problems on SNSs; 2) studies that have yielded solutions to the existing security problems on SNSs; and 3) studies that have found both problems and their solutions. We identified 23 different attacks in our selected studies. We divided the attacks roughly into two types, human and technical-based attacks. The attacks/issues, their brief explanations and the consequences are listed in Table 4 (refer appendix).

We categorized the attacks and issues into specific groups: 1) direct attacks which are directly targeted; 2) privacy issues which are relate to personal information leaks; 3) vulnerabilities, which are flaws or loopholes of a system and which open the information security of a system to attack; and 4) passive attacks, which affect less cautious users as a result of their careless behaviors. The classification of attacks and issues and the studies that found those issues are listed in Table 5. Of these attacks, we select and briefly discuss the five most common attacks and threats on SNSs.

1) Spamming

Spamming is the misuse of an electronic messaging system to spread large numbers of unwanted messages, such as advertisements. Spammers apply various techniques to spread these messages leading users to click malicious links or redirect to malicious websites.

There are basically two types of spamming, broadcast and context-aware. In broadcast spamming, the spammers do not know exact email addresses; hence, they create possible addresses to send spams to. That kind of spamming is very dangerous because people tend to be skeptical. In context-aware the spammers learn about a user's personal details through SNSs or other similar sources and send spams mentioning part of the information they learned. These kinds of spams can be effective, because they say something that relates to the recipient and are therefore more likely to be opened [12].

Though spammers have been using email as a spam-spreading platform, SNSs have become a venue for sharing spam messages as a result of their availability. Twitter is the most attractive SNS for spammers owing to its microblogging feature [13]-[18].

Different methods have been proposed to detect spam accounts on SNSs. In [19] and [17], authors presented ways to detect spammers by creating honeypot profiles on SNSs. In [14], authors proposed an approach for detecting spam accounts in Twitter and Facebook by analyzing the features of spammers and applying data mining techniques.

2) Malware propagation

Malware is unwanted software and can take different forms, such as worms, spams or viruses. Malware writers propagate those malicious contents or links across SNSs by exploiting trust bonds among friends. Malware propagation on SNSs is effective because it can spread very swiftly in a short time owing to the nature of social networks.

According to [20] malware can be classified into three types, Trojan, cross-site scripting (XSS) and clickjacking.

Trojan malware cheats users on SNSs by sending messages with hot issues or attractive topics using social engineering techniques. After clicking a message, user is redirected to a malicious web page and it allowed user to download a Flash update. Downloading infects the machine, and then the infected profiles spread malicious links automatically to other friends of the victim. The most famous Trojan is Koobface, a takeoff on the word “Facebook” [21], [22]. It was first detected in 2008 and two major SNSs, Facebook and MySpace, suffered severely from.

An XSS worm on SNSs make infects the users who visited a particular profile owned by the worm propagator. The malicious code is automatically added to the profiles of those who visit that profile, spreading the worm around.

In clickjacking, also known as likejacking or user interface redressing, the propagator hides malicious code or images under a video file or other graphical trap to persuade users to click it. Clicking it infects the page or profile of the victim and friends of the victims who click or like the same malicious file.

3) Profile cloning attack

Since identity privacy is as important an issue as data privacy [23], profile cloning is a very harmful type of attack. Profile cloning, also known as identity cloning, is commonly seen on SNSs. As identity authenticity is difficult to detect on SNSs, attackers misuse this fact to their own advantage in social and business matters. As there is no strict rule on SNSs that names must be unique in a particular SNS, it is also possible that more than one person might have the same name [24], and it is easy for attackers to create cloned profiles of targeted victims. Attackers can create a cloned profile by copying someone's revealed personal information such as name, date of birth, photo, and schools, and then send friend requests to the victim's friends.

Profile cloning attacks can be classified into two types, same-site and cross-site profile cloning. In same-site profile cloning, an attacker creates cloned profiles in a particular SNS that mimic the victims' profile in the same SNS. In cross-site profile cloning, the victim's personal information is taken from one SNS and misused by an attacker in different SNSs in which he or she does not have accounts [12].

Attackers use this approach on SNSs for various purposes, but the most common purpose is for money [22]. This affects not only the victims but also their friends, as most legitimate users are not very attentive when accepting friend requests on SNSs [25].

4) Social engineering attack

Social engineering is the art of misrepresenting the credentials of a person or a company through the weakest link, people [26]. Such attacks were known originally as human-based attacks but attackers are now using automated social engineering in combination with other attacks and transforming them into technology-based attacks. The social engineering threat on SNSs is common and is partly related to factors of human behavior and lack of awareness of this type of threat [27].

This attack targets primarily to users on SNSs, because SNSs contain rich pools of information. Since most people are willing to expose their personal information on SNSs [28], people trust easily if the source seems to be reliable [29], and an SNS provides services, such as instant messenger or private chats which can be used as platforms to launch social engineering attacks [26].

A social engineering attack begins by sending a victim a message that contains a request, while hiding the sender's true identity. Attackers pretend to be someone interesting [27]. Then, they attempt to trick the victims into revealing their private information, such as passwords in an unnoticeable manner.

This threat is dangerous and is not easy to avoid this threat on SNSs, as it misuses the users' different trust levels, and there are no liable mechanisms for determining a person's trustworthiness. As social engineering is a kind of deception, it can be described roughly as a low-cost attack. However, some typical require spending large amounts of money and devoting substantial time [26].

5) Privacy leakage from third-party application

Third-party applications or apps are extended features offered by SNS providers to persuade users to remain with their SNSs. To use those apps, users must allow some of their personal information to be viewed by application developers, who then have full rights to control the user's personal information.

Facebook began including the third-party application feature in 2007, and most other SNSs allow to access to data in their social graphs. However, most users rely on the SNS providers to protect their personal data [30]. Actually, the personal data of users who access third-party applications are moved to a third party-server. In addition, service and app providers are mutually dependent on each other for their own advantages [26]. Thus, the safety of user's personal data is not protected well and can always be leaked.

In [31], authors discussed how SNSs can become a platform for malicious activities, especially by third-party applications. Three other studies [26], [30], [32] proposed frameworks that can help SNSs become privacy preserving social application platforms.

By carefully studying all of the selected 84 primary articles, we determined that researchers have been attempting to solve security problems on SNSs in the following manners: detecting attacks or attackers; implementing models, frameworks, and tools to take over those attacks or enhancing the existing techniques; pen-testing or penetrating the systems to determine the vulnerabilities of a particular SNS; presenting mechanisms to prevent attacks from being encountered or techniques to preserve privacy; and addressing new guidelines, policies, or for enhancing the privacy of users. The studies in each group are listed in Table 6 (refer appendix).

Although many studies have discussed the common attacks and problems, some researchers have conducted vulnerability testing or built new attack models to determine the strength of a system and to check for loopholes or weaknesses in the system. Table 7 (refer appendix) summarizes the possible attack models proposed by previous researchers.

In the selected literature, 64 studies addressed security problems on SNSs and proposed solutions using different methods, while 19 studies presented the means of testing system robustness. One study, [33] summarized the security problems and defense strategies for them and found that the problems and strategies do not match.

C. On Which SNS do the Researchers Conduct the Most Experiments?

Out of 84 studies, 54 have referred to the existing social networks in conducting their research. Conducting here includes revealing the security problems of a particular SNS (or SNSs), detecting attacks using the proposed frameworks, testing the effectiveness of their enhanced models, conducting pen-testing with the datasets from specific SNSs and inserting the proposed API into a particular SNS. Some researchers tested the effectiveness and robustness of the proposed techniques on two or three different SNSs, while most researchers tested on only one SNS.

Fig. 5 shows the statistical data regarding the SNSs used by researchers for their experiments. While most studies conduct testing on real datasets of specific SNSs, [34] proposed a framework for preventing a Sybil attack on an SNS by testing the mechanism on one news website, Slashdot, in an email system and on Facebook.

In [33], authors pointed out that most of the researches have focused only on Facebook. By reviewing the number of usage of different SNSs, we evaluated that the research works in this domain have done only upon the limited SNSs and the researchers should pay attention on the security issues of other SNSs which have potentiality to be attacked because of the rich professional information such as LinkedIn and Xing.

Hence, it led us to the consideration of the factors of choosing a certain SNS to be tested out. The most possible reasons for the researchers in choosing of SNSs to try out their experiments are: 1) popularity of SNSs and population of users; and 2) the possibility of prune to vulnerability of certain SNS or are facing various security problems.

D. Do the Proposed Security Mechanisms Achieve the Security Goals? If Not, Why do the Proposed Techniques Fail?

For a decade, there has been evidence that researchers were becoming involved in investigating security and privacy issues on SNSs, but the problem has not been a hot topic until now. Several remedies have been proposed in the hope of solving these security and privacy issues confronted in different SNSs, but the problem still remains and opens issue. In [33], authors emphasized that there is a discrepancy between the problems and solutions based on their observations of security problems of SNSs.

This leads us to the conclusion none of the proposed techniques or solutions have been proven to be capable of achieving the three main security goals fully. There are many possible factors from different perspectives that result in security and privacy still being open issues, since the proposed techniques have failed to resolve those issues. In Table 8 we describe the main security problems and attacks on SNSs, along with the affected security goals.

To the best of our knowledge, gained by reviewing all of the studies, we determined that there are two major causes maintaining security and privacy problems as ongoing issues, SNSs themselves and users.

TABLE VIII. MAJOR SECURITY PROBLEMS/ATTACKS AND THEIR IMPACT ON THE THREE SECURITY GOALS

Security attacks/problem	**Main security goals in web services**		
	Privacy	***Integrity***	***Availability***
Bonet	√	√	√
Content Sniffing XSS Attack	√	-	-
Clickjacking	√	-	-
Cross Domain Attack	√		
Fake Profile Building	-	√	-
Friend-in-the-middle Attack	√	√	√
Identity Cloning Attack	√	√	-
Identity Theft Attack	√	√	√
Malicious Crawlers	√	-	-
Malicious Web Content/Malicious Social Campaigns	√	√	-
Malware Propagation	√	-	√
Phishing	√	-	-
Privacy Conflicts	√	-	-
Session Hijacking	√	√	-
Social Engineering	√	√	-
Spamming	√	-	√
SQL Injection	√	√	-
Sybil Attack	√	√	√
Third Party Application	√	-	-

1) SNSs

Here we review factors governing SNS security and privacy breaches caused by SNSs themselves.

a) Original features of SNSs

In 2008**,** [36] pointed out that the centralized architectures of SNS are one of the characteristics that enable personal information leaks. On the other hand, centralized architecture has some positive features, such as accessibility, usability and controllability. In addition, SNSs are user-based social platforms, and they hold a substantial quantity of a user's personal data [36]. There are also user groups who the same social interests, bond with trust relationships and interact on a common ground. SNSs have the feature of platform openness, which can be exploited by attackers for malicious activities [31]. SNS providers do not follow the privacy-enhancing technologies (PETs) properly, because their priority is design, rather than privacy [7]. Similarly, privacy conflict becomes a traditional problem on SNSs as privacy control practices contradict the original design goals of SNSs, usability and sociability [29], [35], [37]. The usefulness of privacy controls on SNSs was lessened as a result of those conflicts.

b) Technical flaws of SNSs

Privacy leaks can occur as a result of negligent coding by the developers early in the development stage of SNS. The security goals of an SNS cannot be assured, if the system is sloppily written. In [38], authors pointed out that the major cause of vulnerabilities is the presence of deficiencies in source code, with improper input validations and decreased emphasis on security guidelines by the developers being factors as well. Additionally, a bad system design leaves users with weaknesses in the privacy and security of their data [39].

c) Inconsistency in privacy practices

It appears obvious that enhancing the setting of privacy preferences resolves most of the privacy issues on SNSs. However, privacy practices on SNSs can be contradictory. For instance, while SNSs are attempting to enhance privacy preferences to protect the users' personal data, they are also allowing third-party applications to access that private data. Furthermore, third-party app developers have full control of those private data as they retain them separately in their own servers, which are beyond the control of an SNS [26] and SNSs still do not have adequate mechanisms for checking the authenticity of users or accounts [40]. This leads SNSs to be a space convenient for adversaries to conduct malicious activities by creating fake accounts. Another factor is the lack of policies for permanently erasing of users' personal data, when their accounts are deleted from an SNS [33].

d) Lack of effective privacy policies

There are a number of weaknesses in the existing privacy policies of some SNSs. First, to have a profile in a particular SNS, users must provide basic information about themselves. Once they register, the personal data are in the possession of the SNS provider, but it is never returned even when the account is deleted. Most of the SNSs prefer that users provide accurate information but users' personal information is likely to be breached since SNS providers cannot provide full protection for them. Second, some users might not know of the privacy policy set by SNSs as a result of their understandability level and complexity and the instability of the policies set by the SNS providers [7].

2) Users

a) User behaviors

Kevin Mitnick, a security consultant who was once a hacker, has been quoted as having said, based on his experience, that "people" are the weakest link in accessing prohibited data. In [27], authors pointed out that social engineering attacks are still occurring on SNSs partly to the complexity of human behaviors. As curiosity is natural for in human beings, people are willing to click malicious URLs without thinking twice [41].

Another important factor is that users are highly reliant on the privacy controls of the SNSs [42]. Most users believe that their sensitive information will be fully protected by the SNS providers, but that fact is really not true in practice. That is why most users pay no attention to the security of their posted and shared information.

We can introduce many technical protective solutions to block the loopholes in security of SNSs to prevent direct attacks, but the security problems caused by users, such as clicking malicious links or video files are entirely up to the user's behaviors. The interview with a journalist of a recently hacked French television station, TV5Monde, is the best example to show that careless behavior of people invites the security breaches, as it was filmed with the written passwords of Twitter and Instagram visibly pasted on the background screen [43].

b) Users' stand on SNSs

Therefore, user's behavior plays an important role in security and privacy problems of SNSs. Most people tend to disclose their personal information on SNSs, because they prefer to have popularity and sociability without careful considering of privacy and security issues. Another factor is people's trust in their friends [41], [29]. Sometimes, a friend himself can be a malware propagator without his knowledge. Furthermore, people tend to click when they see a video link or new apps link, if the source is a known person. Attackers know this very well and hence can win people's trust easily for cheating.

c) User's ability to understand the privacy policies

25% of world's population, from different cultures and communities with different levels of education, interact on various social networks. As a result, their knowledge levels regarding the understanding of privacy controls on SNSs must differ [19]. User awareness programs and user-friendly privacy enhancements are critically needed. Furthermore, rigid security preserving policies on SNSs must be designed and enacted.

V. Limitation of the Study

Although we endeavored to conduct our SLR systematically by following the rules set by [10], we might have deviated from the path in some respects. Especially in selecting the literature, we might be missing some important articles owing to the limited selection criteria. As our scope includes only SNSs, some security attacks and their solutions affecting other web services might not be included in our SLR.

VI. Conclusion

Despite the fact that the advancement of the relevant technology enables attackers to develop more harmful security violations on SNSs, people themselves are the main factor in security and privacy issues. Our SLR confirmed this little-known fact by reviewing previous studies.

By examining 84 selected pieces of literature systematically, we discovered that security problems and issues became a common concern in 2010, and that researchers began paying attention to these issues the most in 2013. It is worth noting that 23 common security attacks and vulnerabilities were found in the ten years from 2004 to 2014. Though there are various SNSs, were surprised to find that most of the researchers referred to two SNSs, Facebook and Twitter, in highlighting security problems. Furthermore, most of the practical attacks and security frameworks were tested on the offline or online datasets of those two SNSs.

Our findings showed that different types of solutions have been proposed to address the security issues of SNSs. Even though a particular SNS has used security strictly in every layer of the system since the creation, lack of awareness and ethics and careless behaviors of users will definitely destroy the security shields for the users themselves. On the other hand, SNS providers must find ways to design privacy-enhanced but sociable SNSs and must set more user-friendly privacy policies protecting users' personal data and shared contents.

We believe that information extracted collectively from our SRL will provide future researchers and practitioners with a proper and concise idea of the reasons why security and privacy issues are still an ongoing problem, as well as different directions for solving those problems on SNSs. Hence, it will be useful for their efforts to find better means of eliminating this ongoing problem.

ACKNOWLEDGMENT

The authors would like to thank and acknowledge the support provided by New UMRG Program 2013 at University Malaya, under research grant reference number: RP004E-13HNE, entitled "Information System Security Management for the Holy Quran: An Approach Towards Reliability of the Holy Quran Application" that has been led by Prof Dato' Dr.Mohd Yakub @ Zulkifli Hj.Mohd Yusoff.

REFERENCES

[1] Anderson, P. (2012). What is Web 2.0? Ideas, technologies and implications for education. JISC Technology and Standards Watch.

[2] Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), pp. 210-230.

[3] Bennett, S. (2014). Facebook, Twitter, Instagram, Pinterest, Vine, Snapchat – Social Media Stats 2014 [INFOGRAPHIC]. Available at: http://www.adweek.com/socialtimes/social-media-statistics-2014/499230.

[4] Global Digital Statistics. (2014). Available at: http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20&%20Mobile%20Statistics,%20Jan%202014.pdf

[5] Microsoft. (2015). Chapter 1: Security Fundamentals for Web Services. Available at: https://msdn.microsoft.com/en-us/library/ff648318.aspx

[6] Chia, T. (2012). Confidentiality, Integrity, Availability: The three components of the CIA Triad. IT Security Community Blog. Available at: http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

[7] Aimeur, E., Gambs, S., & Ho, A. (2010). Towards a Privacy-Enhanced Social Networking Site. International Conference on Availability, Reliability and Security. pp. 172-179.

[8] Labs, V. (2014). Majority of Global 2000 Organizations Have Not Remediated Heartbleed, Remain Vulnerable to Cyber Attacks. Venafi Labs Q3 Heartbleed Threat Research Analysis.

[9] Walker, D. (2014). Experts take inventory of Sony Pictures data leak, potential costs. Available at: http://www.scmagazine.com/experts-take-inventory-of-sony-pictures-data-leak-potential-costs/article/386991/

[10] Kitchenham, B. (2004). Procedures for performing systematic reviews. Joint Technical Report, 33(2004), pp. 1-26.

[11] Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS)–A systematic literature review. Information and Software Technology, 58, pp. 170-186.

[12] Devmane, M., & Rana, N. (2013). Security Issues of Online Social Networks. Advances in Computing, Communication, and Control, Springer. pp. 740-746.

[13] Ahmed, F., & Abulaish M. (2012). An MCL-Based Approach for Spam Profile Detection in Online Social Networks. IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 602-608.

[14] Ahmed, F., & Abulaish, M. (2013). A generic statistical approach for spam detection in Online Social Networks. Computer Communications. Vol. 36 (10–11), pp. 1120–1129.

[15] Beck, K. (2011). Analyzing tweets to identify malicious messages. IEEE International Conference on Electro/Information Technology (EIT). pp. 1-5.

[16] Hua, W., & Zhang, Y. (2013). Threshold and Associative Based Classification for Social Spam Profile Detection on Twitter. International Conference on Semantics, Knowledge and Grids (SKG), IEEE. pp. 113-120.

[17] Yang, C., Harkreader, R., & Gu, G. (2013). Empirical evaluation and new design for fighting evolving Twitter spammers. IEEE Transactions on Information Forensics and Security, vol. 8(8), pp. 1280-1293.

[18] Yang, C., Zhang, J., & Gu, G. (2014). A taste of tweets: reverse engineering Twitter spammers. Proceedings of the 30th Annual Computer Security Applications Conference, ACM. pp. 86-95.

[19] Stringhini, G., Kruegel, C., & Vigna, G. (2010). Detecting spammers on social networks. Proceedings of the 26th Annual Computer Security Applications Conference, ACM. pp. 1-9.

[20] Faghani, M. R., Matrawy, A., & Lung, C.-H. (2012). A study of trojan propagation in online social networks. International Conference on New Technologies, Mobility and Security (NTMS), IEEE. pp. 1-5.

[21] Cashion, J., & Bassiouni, M. (2011). Protocol for mitigating the risk of hijacking social networking sites. International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). pp. 324-331.

[22] Kiruthiga, S., & Kannan, A. (2014). Detecting cloning attack in Social Networks using classification and clustering techniques. International Conference on Recent Trends in Information Technology (ICRTIT), IEEE. pp. 1-6.

[23] Zhao, X., Li, L., & Xue, G. (2012). Keeping identity secret in online social networks. Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ACM. pp. 55-56.

[24] Jin, L., Takabi, H., & Joshi, J. B. (2011). Towards active detection of identity clone attacks on online social networks. Proceedings of the first ACM conference on Data and application security and privacy, ACM. pp. 27-38.

[25] Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. Proceedings of the 18th international conference on World wide web, ACM. pp. 551-560.

[26] Huber, M., Mulazzani, M., Schrittwieser, S., & Weippl, E. (2013). Appinspect: large-scale evaluation of social networking apps. Proceedings of the first ACM conference on Online social networks, ACM. pp. 143-154.

[27] Algarni, A., Yue, X., & Chan, T. (2014). Social Engineering in Social Networking Sites: The Art of Impersonation. IEEE International Conference on Services Computing (SCC). pp. 797-804.

[28] Algarni, A., Yue, X., Taizan, C., & Yu-Chu, T. (2013). Social engineering in social networking sites: Affect-based model. International Conference for Internet Technology and Secured Transactions (ICITST). pp. 508-515.

[29] He, B.-Z., Chen, C.-M., Su, Y.-P., & Sun, H.-M. (2014). A defence scheme against Identity Theft Attack based on multiple social networks. Expert Systems with Applications, 41(5), pp. 2345-2352.

[30] Reynaert, T., De Groef, W., Devriese, D., Desmet, L., & Piessens, F. (2012). PESAP: A Privacy Enhanced Social Application Platform. International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Confernece on Social Computing (SocialCom). pp. 827-833.

[31] Makridakis, A., Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S., & Markatos, E. P. (2010). Understanding the behavior of malicious applications in social networks. Network, IEEE, vol. 24(5), pp. 14-19.

[32] Cheng, Y., Park, J., & Sandhu, R. (2013). Preserving user privacy from third-party applications in online social networks. Proceedings of the 22nd international conference on World Wide Web companion, International World Wide Web Conferences Steering Committee. pp. 723-728.

[33] Huber, M., Mulazzani, M., & Weippl, E. (2010). Social Networking Sites Security: Quo Vadis. IEEE Second International Conference on Social Computing (SocialCom). pp. 1117-1122.

[34] Gong, N., & Wang, D. (2014). On the security of trustee-based social authentications. IEEE Transactions on Information Forensics and Security. Vol. 9 (8).

[35] Li, Y., Li, Y., Yan, Q., & Deng, R. H. (2014). Privacy leakage analysis in online social networks. Computers & Security, vol. 49, pp. 239–254.

[36] Lucas, M. M., & Borisov, N. (2008). Flybynight: mitigating the privacy risks of social networking. Proceedings of the 7th ACM workshop on Privacy in the electronic society, ACM. pp. 1 - 8.

[37] Sureshkumar, A., Palanisamy, S., & Sowdeshwari Sowmiya, R. (2013). Data isolation and protection in online social networks. International Conference on Information Communication and Embedded Systems (ICICES), IEEE. pp. 150-155.

[38] Gupta, M. K., Govil, M. C., & Singh, G. (2014). An approach to minimize false positive in SQLI vulnerabilities detection techniques through data mining. International Conference on Signal Propagation and Computer Technology (ICSPCT), IEEE. pp. 407-410

[39] Mahmood, S. (2012). New privacy threats for Facebook and Twitter users. International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE. pp. 164-169.

[40] Noor, U., Anwar, Z., Mehmood, Y., & Aslam, W. (2013). TrustBook: Web of Trust Based Relationship Establishment in Online Social Networks. International Conference on Frontiers of Information Technology (FIT). pp. 223-228.

[41] Chen, C.-M., Guan, D. J., & Su, Q.-K. (2014). Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. Information Sciences, 289(0), pp. 133-147.

[42] Atrey, P. K. (2011). A secret sharing based privacy enforcement mechanism for untrusted social networking operators. Proceedings of the 3rd international ACM workshop on Multimedia in forensics and intelligence, ACM. pp. 13-18.

[43] Aggarwal, A., Rajadesingan, A., & Kumaraguru, P. (2012). PhishAri: Automatic realtime phishing detection on twitter. eCrime Researchers Summit (eCrime).

[44] Ahmadinejad, S. H., & Fong, P. W. L. (2014). Unintended disclosure of information: Inference attacks by third-party extensions to Social Network Systems. Computers & Security, 44(0), 75-91.

[45] Aiello, L. M., & Ruffo, G. (2012). LotusNet: Tunable privacy for distributed online social network services. Computer Communications. Vol. 35 (1), pp.75–88.

[46] Al-Qasem, I., Al-Qasem, S. & Al-Hammouri, A.T. (2013). Leveraging online social networks for a real-time malware alerting system. IEEE Conference on Local Computer Networks (LCN). pp. 272-275.

[47] Alsaleh, M., Alarifi, A., Al-Salman, A. M., Alfayez, M., & Almuhaysin, A. (2014). TSD: Detecting Sybil Accounts in Twitter. International Conference on Machine Learning and Applications (ICMLA), IEEE. pp. 463-469.

[48] Amleshwaram, A. A., Reddy, N., Yadav, S., Gu, G., & Yang, C. (2013). CATS: Characterizing automation of Twitter spammers. International Conference on Communication Systems and Networks (COMSNETS), IEEE. pp. 1-10.

[49] Bachpalle, S. D., & Desai, M. (2014). Data security approach for online social network. 2nd International Conference on Current Trends in Engineering and Technology (ICCTET), IEEE. pp. 262-267.

[50] Beato, F., Conti, M., & Preneel, B. (2013). Friend in the middle (fim): Tackling de-anonymization in social networks. IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE. pp. 279-284.

[51] Bernard, C., Debar, H., & Benayoune, S. (2012). Cross-domain vulnerabilities over social networks. International Conference on Computational Aspects of Social Networks (CASoN). pp. 8-13.

[52] Bhumiratana, B. (2011). A Model for Automating Persistent Identity Clone in Online Social Network. IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 681-686.

[53] Chaitanya, T. K., Ponnapalli, H., Herts, D. & Pablo, J. (2012). Analysis and Detection of Modern Spam Techniques on Social Networking Sites. International Conference on Services in Emerging Markets (ICSEM). pp. 147-152.

[54] Conti, M., Poovendran, R., & Secchiero, M. (2012). FakeBook: Detecting Fake Profiles in On-Line Social Networks. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 1071-1078.

[55] Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, IEEE, 47(12), pp. 94-101.

[56] Devmane, M., & Rana, N. (2014). Detection and prevention of Profile Cloning in Online Social Networks. Recent Advances and Innovations in Engineering (ICRAIE), IEEE. pp. 1-5.

[57] Egele, M., Moser, A., Kruegel, C., & Kirda, E. (2012). PoX: Protecting users from malicious Facebook applications. Computer Communications, 35(12), pp. 1507-1515.

[58] Faisal, A. A., Nisa, B. S., & Ibrahim, J. (2013). Mitigating privacy issues on Facebook by implementing information security awareness with islamic perspectives. International Conference on Information and Communication Technology for the Muslim World (ICT4M). pp. 1-5.

[59] Fan, W., Yeung, K. H., & Wong, K. Y. (2013). Assembly effect of groups in online social networks. Physica A: Statistical Mechanics and its Applications, 392(5), pp. 1090-1099.

[60] Gebre, M. T., Lhee, K.-S., & Hong, M. (2010). A robust defense against content-sniffing xss attacks. International Conference on Digital Content, Multimedia Technology and its Applications (IDC). pp. 315-320.

[61] Gong, N. Z., Frank, M., & Mittal, P. (2014). SybilBelief: A semi-supervised learning approach for structure-based sybil detection. IEEE Transactions on Information Forensics and Security, 9(6), pp. 976-987.

[62] Hu, H., Ahn, G.-J., & Jorgensen, J. (2011). Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. Proceedings of the 27th Annual Computer Security Applications Conference, ACM. pp. 103-112.

[63] Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. International Conference on Computational Science and Engineering. pp. 117-124.

[64] Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. Internet Computing, IEEE, 15(3), pp. 28-34.

[65] Javed, A., Bletgen, D., Kohlar, F., Durmuth, M., & Schwenk, J. (2014). Secure Fallback Authentication and the Trusted Friend Attack. International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE. pp. 22-28.

[66] Jin, L., Joshi, J. B. D., & Anwar, M. (2013). Mutual-friend based attacks in social network systems. Computers & Security, 37(0), pp. 15-30.

[67] Kai, C., Yi, Z., Li, S., & Xiaokang, Y. (2011). Building Artificial Identities in Social Network Using Semantic Information. International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 565-566.

[68] Keister, J. W., Fujinoki, H., Bandy, C. W., & Lickenbrock, S. R. (2011). SoKey: New security architecture for zero-possibility private information leak in social networking applications. IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR). pp. 1-6.

[69] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report.

[70] Lee, S., & Kim, J. (2014). Early filtering of ephemeral malicious accounts on Twitter. Computer Communications, 54(0), pp. 48-57.

[71] Li, L., Zhao, X., & Xue, G. (2012). An identity authentication protocol in online social networks. Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. pp. 28-29.

[72] Luo, W., Liu, J., Liu, J., & Fan, C. (2009). An analysis of security in social networks. IEEE International Conference on Dependable, Autonomic and Secure Computing. pp. 648-651.

[73] Luo, W., Xie, Q., & Hengartner, U. (2009). Facecloak: An architecture for user privacy on social networking sites. International Conference on Computational Science and Engineering. pp. 26-33.

[74] Malik, S., & Sardana, A. (2011). Secure vault: A privacy preserving reliable architecture for secure social networking. International Conference on Information Assurance and Security (IAS), IEEE. pp. 116-121.

[75] Marés, J., & Torra, V. (2013). On the protection of social networks user's information. Knowledge-Based Systems, vol. 49(0), pp. 134-144.

[76] Marques, J., & Serrão, C. (2013). Improving Content Privacy on Social Networks Using Open Digital Rights Management Solutions. Procedia Technology, vol. 9(0), pp. 405-410.

[77] Moonam, K., Touati, H., & Shehab, M. (2011). Enabling Cross-Site Content Sharing between Social Networks. IEEE Third Inernational Conference on Social Computing (SocialCom) and IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT). pp. 493-496.

[78] Nepali, R. K., & Yong, W. (2013). SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking. IEEE 33rd International Conference on Distributed Computing Systems Workshops (ICDCSW). pp. 162-166.

[79] Perez, C., Birregah, B., Layton, R., Lemercier, M., & Watters, P. (2013). REPLOT: Retrieving profile links on Twitter for suspicious networks detection. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 1307-1314.

[80] Raji, F., Miri, A., & Jazi, M. D. (2013). CP2: Cryptographic privacy protection framework for online social networks. Computers & Electrical Engineering, vol. 39(7), pp. 2282-2298.

[81] Robertson, M., Pan, Y., & Yuan, B. (2010). A social approach to security: Using social networks to help detect malicious web content. International Conference on Intelligent Systems and Knowledge Engineering (ISKE), IEEE. pp. 436-441.

[82] Sanzgiri, A., Hughes, A., & Upadhyaya, S. (2013). Analysis of Malware Propagation in Twitter. International Symposium on Reliable Distributed Systems (SRDS), IEEE. pp. 195-204

[83] Sanzgiri, A., Joyce, J., & Upadhyaya, S. (2012). The Early (tweet-ing) Bird Spreads the Worm: An Assessment of Twitter for Malware Propagation. Procedia Computer Science, vol. 10(0), pp. 705-712.

[84] Saritha, S. K., & Dharavath, K. (2012). Link Encryption to Counteract with Rouge Social Network Crawlers. International Conference on Information Technology: New Generations (ITNG). pp. 883-884.

[85] Sebastian, S., & Ayyappan, S. (2014). Framework for design of Graybot in social network. International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE. pp. 2331-2336.

[86] Sharma, R., Jain, A., & Rastogi, R. (2013). A new face to photo security of Facebook. International Conference on Contemporary Computing (IC3), IEEE. pp. 415-420.

[87] Shehab, M., Squicciarini, A., Ahn, G.-J., & Kokkinou, I. (2012). Access control for online social networks third party applications. Computers & Security, vol. 31(8), pp. 897-911.

[88] Shin, D., Lopes, R., Claycomb, W., & Ahn, G.-J. (2009). A Framework for Enabling User-controlled Persona in Online Social Networks. IEEE International Computer Software and Applications Conference. Vol 1, pp. 292-297.

[89] Sinha, R., Uppal, D., Singh, D., & Rathi, R. (2014). Clickjacking: Existing defenses and some novel approaches. International Conference on Signal Propagation and Computer Technology (ICSPCT), IEEE. pp. 396-401.

[90] Van den Berg, B., & Leenes, R. (2010). Audience Segregation in Social Network Sites. IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust. pp. 1111-1116.

[91] Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010, 16-19 May 2010). A Practical Attack to De-anonymize Social Network Users. IEEE Symposium on Security and Privacy. pp. 223-238.

[92] Xu, S., Li, X., Parker, T. P., & Wang, X. (2011). Exploiting trust-based social networks for distributed protection of sensitive data. IEEE Transactions on Information Forensics and Security, vol. 6(1), pp. 39-52.

[93] Yang, F., & Manoharan, S. (2013). A security analysis of the OAuth protocol. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), IEEE. pp. 271-276.

[94] Yi, C., Bao, Y., Jiang, J., Xue, Y., & Dong, Y. (2014). Cascading failures of social networks under attacks. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), IEEE. pp. 679-686.

[95] Youna, J., Minsoo, K., & Joshi, J. B. D. (2012). Towards secure cooperation in online social networks. International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). pp. 80-88.

APPENDIX

TABLE III. QUALITY CHECKLIST OF EACH SELECTED STUDY

No.	Title	QA1	QA2	QA3	Total Score
#01	Flybynight: Mitigating the Privacy Risks of Social Networking	1	1	1	3
#02	A Framework for Enabling Use-controlled Persona in Online Social Networks	1	1	1	3
#03	All of Your Contents are Belong to Us: Automated Identity Theft Attacks on Social Networks	1	1	1	3
#04	An Analysis of Security in Social Network	1	1	0.5	2.5
#05	Facecloak: An Architecture for User Privacy on Social Networking Sites	1	1	1	3
#06	SafeBook: A Privacy-preserving Online Social Network Leveraging on Real-life Trust	1	1	1	3
#07	Towards Automating Social Engineering Using Social Networking Sites	1	1	1	3
#08	Audience Segregation in Social Network Sites	0.5	1	1	2.5
#09	A practical Attack to De-Anonymize Social Network Users	1	1	1	3
#10	A Robust Defense Against Content-Sniffing XSS Attacks	1	1	1	3
#11	A Social Approach to Security: Using Social Networks to Help Detect Malicious Web Content	1	1	1	3
#12	Detecting Spammers on Social Network	1	1	1	3
#13	Social Networking Sites Security: Quo Vadis	1	1	0.5	2.5
#14	Towards a Privacy-Enhanced Social Networking Site	1	1	1	3
#15	Understanding the Behavior of Malicious Applications in Social Networks	0.5	1	1	2.5
#16	A Model for Automating Persistent Identity Clone in Online Social Network	1	1	1	3
#17	A Secret Sharing Based Privacy Enforcement Mechanism for Untrusted Social Networking Operators	1	1	1	3
#18	Analyzing Tweets to Identify Malicious Messages	1	1	1	3
#19	Building Artificial Identities in Social Network Using Semantic Information	1	1	1	3
#20	Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks	1	1	1	3
#21	Enabling Cross-Site Content Sharing between Social Networks	1	1	1	3
#22	Exploiting Trust-Based Social Networks for Distributed Protection of Sensitive Data	1	1	1	3
#23	Friend-in-the Middle Attacks Exploiting Social Networking Sites for Spam	1	1	1	3

#24	Protocol for Mitigating the Risk of Hijacking Social Networking Sites	1	1	1	3
#25	Secure Vault: A Privacy Preserving Reliable Architecture for Secure Social Networking	1	1	1	3
#26	SoKey: New Security Architecture for Zero-Possibility Private Information Leak in Social Networking Applications	1	1	1	3
#27	Towards Active Detection of Identity Clone Attacks on Online Social Networks	1	1	1	3
#28	A Study of Trojan Propagation in Online Social Networks	1	1	0.5	2.5
#29	Access Control for Online Social Networks Third Party Applications	1	1	1	3
#30	An Identity Authentication Protocol in Online Social Networks	1	1	1	3
#31	An MCL-based Approach for Spam Profile Detection in Online Social Networks	1	1	1	3
#32	Analysis and Detection of Modern Spam Techniques on Social Networking Sites	1	1	1	3
#33	Cross-domain Vulnerabilities over Social Networks	1	0.5	1	2.5
#34	FakeBook: Detecting Fake Profiles in Online Social Networks	1	1	1	3
#35	Keeping Identity Secret in Online Social Networks	1	1	1	3
#36	Link Encryption to Counteract with Rouge Social Network Crawlers	1	1	1	3
#37	LotusNet: Tunable Privacy for Distributed Online Social Networks	1	1	1	3
#38	New Privacy Threats for Facebook and Twitter Users	1	1	1	2.5
#39	PESAP: a Privacy Enhanced Social Application Platform	1	1	1	3
#40	PhishAri: Automatic Realtime Phishing Detection on Twitter	1	1	1	3
#41	PoX: Protecting Users from Malicious Facebook Applications	1	1	1	3
#42	The Early (tweet-ing) Bird Spreads the Worm: An Assessment of Twitter for Malware Propagation	1	1	1	3
#43	Towards Secure Cooperation in Online Social Networks	1	1	1	3
#44	A Security Analysis of the OAuth Protocol	1	0.5	0.5	2
#45	A Generic Statistical Approach for Spam Detection in Online Social Networks	1	0.5	0.5	2
#46	A New Face to Photo Security of Facebook	1	1	0.5	2.5
#47	Analysis of Malware Propagation in Twitter	1	1	1	3
#48	AppInspect: Large-scale Evaluation of Social Networking Apps	1	1	0.5	3
#49	Assembly Effect of Groups in Online Social Networks	1	1	1	3
#50	CATS: Characterizing Automation of Twitter Spammers	1	1	0.5	2.5
#51	CP2: Cryptographic Privacy Protection Framework for Online Social Networks	1	1	1	3
#52	Data Isolation and Protection Online Social Networks	1	1	0.5	2.5
#53	Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers	1	1	1	3
#54	Friend in the Middle (FiM): Tackling De-Anonymization in Social Networks	1	1	1	3
#55	Improving Content Privacy on Social Networks Using Open Digital Rights Management Solutions	1	1	0.5	2.5
#56	Leveraging Online Social Networks for a Real-time Malware Alerting System	1	1	0.5	2.5
#57	Mitigating Privacy Issues on Facebook by Implementing Information Security Awareness with Islamic Perspectives	0.5	1	0.5	2
#58	Mutual Friend Based Attacks in Social Networks	1	1	1	3
#59	On the Protection of Social Networks User's Information	1	1	1	3
#60	Preserving User Privacy from Third -party Applications in Online Social Networks	1	1	1	3
#61	REPLOT: REtrieving Profile Links On Twitter for Suspicious Networks Detection	1	1	1	3
#62	Security Issues of Online Social Networks	1	1	0.5	2.5
#63	Social Engineering in Social Networking Sites: Affect-Based Model	1	1	1	3
#64	SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking	1	1	0.5	2.5
#65	Threshold and Associative Based Classification for Social Spam Profile Detection on Twitter	1	1	1	3
#66	TrustBook: Web of Trust Based Relationship Establishment in Online Social Networks	1	1	1	3
#67	A Defence Scheme Against Identity Theft Attack based on Multiple Social Networks	1	1	1	3
#68	A Taste of Tweets: Reverse Engineering Twitter Spammers	1	1	1	3
#69	An Approach to Minimize False Positive in SQLI Vulnerabilities Detection Techniques through Data Mining	0.5	0.5	1	2
#70	Cascading Failures of Social Networks under Attacks	0.5	1	1	2.5
#71	Clickjacking: Existing Defenses and Some Novel Approaches	1	1	0.5	2.5
#72	Data Security Approach for Online Social Network	1	1	1	3
#73	Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques	1	1	1	3
#74	Detection and Prevention of Profile Cloning in Online Social Networks	1	1	1	3
#75	Early Filtering of Ephemeral Malicious Accounts on Twitter	1	1	1	3
#76	Framework for Design of Graybot in Social Network	1	1	1	3
#77	On the Security of Trustee-Based Social Authentications	1	1	1	3
#78	Privacy Leakage Analysis in Online Social Networks	1	1	1	3
#79	Secure Fallback Authentication and the Trusted Friend Attack	1	1	1	3
#80	Social Engineering in Social Networking Sites: The Art of Impersonation	1	1	0.5	2.5
#81	SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection	1	1	1	3
#82	TSD: Detecting Sybil Accounts in Twitter	1	1	1	3
#83	Unintended Disclosure of Information: Inference Attacks by Third-Party Extension to Social Network Systems	1	1	1	3
#84	Feature Set Identification for Detecting Suspicious URLs using Bayesian Classification in Social Networks	1	1	1	3

TABLE IV. DESCRIPTION ON CLASSIFIED SECURITY ATTACKS/VULNERABILITIES

No.	**Name of the Attack/Vulnerability/ Issues**	**Category**	**Type**	**Definition**	**Brief description of their effect**	**Reference**
1	Attack of Facebook's Trusted Friends	Vulnerability	Human-based	This is a type of vulnerability in Facebook and it can be occurred when an attacker exploit the Facebook's account recovery feature, 'Trusted Friends'. Generally, an attacker creates fake accounts and send friend requests to the victim and make a plot and steal his/her personal information by exploiting the 'Trusted Friends' feature of Facebook.	Once this attack has successfully launched, the other linked accounts will be affected and make 'chained trusted friend attack' as the attacker will use the compromised account to launch more attacks.	[65]
2	Bonet	Passive Attack	Human-based	Bonet is a set of compromised computers in a network under the command and control of attacker called botmaster. To start a botnet in SNS, a malicious application is shared on a person's profile and persuades him/her to click that application. Once he/she click, the malicious application will be automatically sent to other computers.	Botnets are applied to do further severe attacks such as Denial-of-Service attack, identity theft and spamming.	[12], [85]
3	Fake profile Building	Direct attack	Human-based	Fake profile building is the type of impersonation by which an attacker creates a fake profile of a real person who does not have any social account in a certain SNS.	By exploiting fake profiles, first the attacker builds friendship with the friends of the victim and later will steal the personal information of his/her and misuse in other cybercrimes.	[54]
4	Forest Fire Attack	Vulnerability	Human-based	It is a kind of vulnerability attack based on trustee-based social authentications. It is named as forest fire because attacks to a certain victim can be spread very quickly as forest fire and damage the large amount of victims in a short time.	According to nature of the attack, this attack can spread easily to many SNSs.	[34]
5	Friend-in-the-Middle (FITM)	Direct attack	Tech-based	Friend-in-the-Middle is a common eavesdropping attack in web services especially in SNSs. This attack can be started by exploiting the missing protection link between a user and SNS provider.	With this attack, the social data of the users can be accessed automatically and will be used in other attacks such as spamming and social phishing.	[12], [50], [64]
6	Identity Cloning Attack	Direct attack	Tech-based/ Human-based	Identity cloning attack tries to mimic as someone else by cloning his/her identities on online social network. Attackers cheat the belief of victim's friends of their authenticity and collect the private information of the victim which are not revealed in SNSs.	Basically, this attack will effect equally to the victims as well as to their friends in the network. Based on the attackers, the effects include defaming and disrupting a person's image by committing crime-related manners such as fraud. It also effect on the trust relationship among friends.	[12], [25], 52], [68]
	Cascading Failures	Vulnerability	Human-based	A cascading failure is a procedure in which the	This can lead to complete failure of a social network.	[94]

7				failure of one part of a system can trigger the successive failures of many other parts of the system.		
8	Clickjacking/User interface Redness Attack	Passive Attack	Tech-based	Clickjacking is a type of attack from which user's clicks were led to the different route rather than the page he/she targeted to.	The one who click the malicious link become the source of malware and spread to his/her friends. So this type of attack can spread very fast.	[12], [53]
9	Content Sniffing XSS Attack	Passive Attack	Tech-based	This is an attack in which an attacker uploads a file which contains malicious HTML script embedding into a non-HTML file to a website. By this way, the attacker let the user to run that malicious code in his browser.	It is a very dangerous attack as the embedded malicious code will surely run on the certain SNS according to the JavaScript's original policy.	[60]
10	Cross Domain Attack	Passive Attack	Tech-based	Cross domain attack is occurred due to the software vulnerability of a system. By exploiting the cross-domain requests from different websites, the attacker compromises those sites with embedded flash objects.	When Software vulnerabilities on video sharing platforms combine with the malicious exploiting of the cross domain requests, it leads to session hijacking attack.	[51]
11	Identity Theft	Direct Attack	Human-based	Identity theft is a form of stealing someone's personal information without the knowledge of that person. Pretending to be that person to commit crimes such as fraud or theft.	By using those personal information, other harmful cyber-attacks and physical attacks such as impersonation, financial fraud, scamming can be committed.	[25]; [29], [72] [91]
12	Inference Attack	Passive Attack	Tech-based	This attack is an information leakage process in which a malicious extension tries to infer the uncovered information via legitimately accessible information.	Although this attack is type of privacy violation, it could lead to other harmful attacks such as identity theft and phishing attacks.	[44]
13	Malicious Crawlers	Privacy Issue	Tech-based	Malicious crawlers are type of threats to user's personal data on SNSs. Crawlers are automated software which have the ability to access and download large amount of users' data on Web in a very fast and effective manner.	Large amount of personal data can be leaked and misused.	[84]
14	Malicious Web Content propagation	Passive Attack	Human-based	Malicious web content propagation means spreading of the content which include malicious links on SNSs. A large amount of malicious profiles or users who perform that malicious web content propagation massively together can be defined as malicious social campaign.	From this, the other attacks such as phishing, spamming can occur and can lead to identity theft.	[79], [81]
15	Malware Propagation	Passive Attack	Tech-based/ Human-based	Malware propagation in SNS can be defined as spreading malicious software to the SNS users which let them download specific software (malware) and propagate that malware to others.	As malware are mostly propagated by the pay-per-install (PPI) institutions, the victims will suffer from financial loss.	[41], [46], [59], [82]
	Phishing	Privacy	Human-	Phishing is a form of	With phishing, the secret and confidential	[12], [15], [25],

16		Issue	based	electronic deception in which the attacker creates a replica of a certain web page and trick the user to disclose his/her personal and credentials. [from reference folder]	information such as bank account number, other financial information and passwords can be leaked.	[43]
17	Personal Information Leak/Privacy Conflict	Privacy Issue	Tech-based/ Human-based	This is very common problem in SNSs and almost every user has been facing. Personal information leak means a certain user's covered information is disclosed to unwanted people without that user's consent.	Adversaries can misuse those leaked personal information to do other dangerous attacks such as profile cloning, identity theft, phishing etc.	[7], [12], [42], [45], [49], [55], [58], [62], [68], [35], [36], [39], [72], [74]-[78], [80], [86], [88], [90], [95]
18	Session Hijacking Attack	Direct Attack	Tech-based	It is a form of phishing attack in which a malicious browser component monitor the user's log in activities and steal the networking session by impersonating as the real users.	Once the attackers hijack the network section of the user, they can do anything they wish such as view the photos, share the messages and view the users' web history etc.	[12], [21]
19	Social Engineering	Direct Attack	Human-based/Tech-based	Social engineering is a type of threat which is an art of cheating someone's personal information with the ways the victims never notice that their information is cheated or attracting them to do an action to be beneficial to the attacker.	With social engineering, the attacker will make the victims to accept the other different threats and make them involve in cybercrimes such as phishing, sexual abuse, financial abuse, identity theft and even in physical crimes.	[27], [28]
20	Spamming	Passive Attack	Human-based	Spamming is process of misusing the electronic messaging system by sending many unwanted messages such as advertising the products, giving some alert messages. Via these messages, the users are sent to different websites and make them reveal their personal information or spreading malwares.	By misusing the trust of the network, they do promoting blogs or advertising the products or scamming. By exploiting URL shortening feature, harmful spams which contains links to scam advertisements and adult contents.	[12], [13], [16]-[19], [48], [53]
21	SQL Injection	Direct Attack	Tech-based	SQL injection is a type of attack in which an attacker inserts a malicious SQL query into the web application by change the original targeted SQL logic.	It affects the integrity and confidentiality of the system.	[38]
22	Sybil Attack	Direct Attack	Human-based	Sybil attack is caused by Sybil attackers. Sybil attackers are the software-controlled SNS accounts or fake profiles who pretend as real human users. The attackers can be social bot or spammer.	By use of Sybil accounts, various malicious activities such as identity stealing, phishing, spamming or malware propagation.	[47], [61]
23	Third Party Application	Passive Attack	Tech-based	Some SNSs allow the third party application developers to access their social graph which contains the user's information. Third party applications or apps are designed for entertaining the SNS users which includes games, quizzes and horoscopes etc.	As apps developers move the users' data on their servers which are beyond the control of actual SNS, there is possibility to personal information leakage.	[13], [23], [30]-[32], [44], [57], [87]

TABLE VI. SUMMARY OF PROPOSED SOLUTION AND TYPES

No	Prototype Name	Brief Description of Solution	Addressing type	Area of Focus	Reference
1.	FlyByNight	A prototype to be applied in Facebook which encrypt the sensitive data of FB users by use of client-side JavaScript.	Implementation	Protecting of user's privacy	[36]
2.	U-Control	A user-centric framework that enable the users to be controllable upon their personal sensitive data.	Implementation	Protecting of user's privacy	[88]
3.	FaceCloak	Architecture for preserving users' privacy from the SNS as well as from unwanted users to be misused.	Implementation	Protecting of user's privacy	[72]
4.	SafeBook	A decentralized and privacy preserving online social network application which is based on two design principles decentralization and real-life trust.	Implementation	Protecting of user's privacy	[55]
5.	Clique	A prototype of social networking site which include a mechanism called audience segregation that means the partitioning of different audiences and the compartmentalization of social spheres	Implementation	Protecting of user's privacy	[90]
6.	Not Mentioned	A filter which examines the user uploaded files whether they are potentially dangerous HTML elements or not, in order to protect the vulnerable browsers from being mistreated to Non-HTML files.	Implementation	Protecting of browser's vulnerability	[60]
7.	Not Mentioned	A Facebook application which automatically evaluate and detect the malicious link content by use of a method of combining traditional security heuristics with social networking data.	Implementation	Detecting malicious links	[81]
8.	Not Mentioned	A tool for detecting spammers based on the preliminary investigations of the features of spammers by creating honeynet accounts.	Implementation	Detecting attackers	[19]
9.	Privacy Watch	A prototype of social networking site which preserved privacy designed to meet some attributes: privacy awareness and customization, data minimization and data sovereignty.	Implementation/Setting policies	Protecting of user's privacy	[7]
10.	Not Mentioned	A system which encrypts the users' private data and protect not to disclose the encryption key.	Implementation	Protecting of user's privacy	[42]
11.	Not Mentioned	This work includes doing experiments to show that spams can spread in Twitter without using specific keywords, proving that using Logical Regression is better than using Support Vector Machine approach, and proving that considering follower/followee ratio in detecting spam is a wrong option.	Proving/ Enhancing	Detecting attackers	[15]
12.	Retinue	A prototype of Facebook application which applies the mechanism of identifying and resolving privacy conflict for collaborative data sharing in SNSs.	Implementation	Protecting of user's privacy	[62]
13.	x-mngr	A framework which help users in their cross-site sharing by allowing them to set the preferred policies.	Implementation	Protecting of user's privacy	[77]
14.	Self-Configuring Repeatable Hash Chain (SCRHC)	A security authentication protocol in order to prevent the session hijacking problem in SNSs by used of modified hash chain approach.	Setting policies	Preventing from attack	[21]
15.	Secure Vault	Architecture for a particular SNS which will yield the fake information of users' personal data to unauthorized users by encrypting the data.	Implementation	Protecting of user's privacy	[74]
16.	SoKey	Security architecture which protects users' personal information not to be leaked from SNS servers.	Implementation	Protecting of user's privacy	[68]
17.	Not Mentioned	A framework to detect the fake accounts in SNSs based on two detection schemes, attribute similarity and similarity of friend network.	Implementation	Detecting potential attacks	[24]
18.	Not Mentioned	This solution includes investigating the attacking vector of Trojan type malware and suggesting some adjustments to the current models in protecting malware in SNSs: to consider the effect of clustering coefficient and user's behaviors.	Enhancing	Preventing from attack	[20]
19.	Not Mentioned	An access control framework for third party application developers which let the user set the specified privacy preferences and let the developers to create customized design based on users' preferences.	Implementation	Protecting of user's privacy	[87]
20.	Not Mentioned	An authenticated key exchange protocol which provides identity authentication and key exchange without sharing the personal information ahead.	Setting Policies	Preventing from attack	[71]
21.	Not Mentioned	An approach to detect spam accounts in SNSs by applying Markov Clustering (MCL) method.	Implementation	Detecting attackers	[12]
22.	Not Mentioned	Based on the evaluation gained after analyzing two attacks, the enhancements which fill the gap of current solution to	Enhancing/ Setting Policies	Detecting attacks	[53]

		clickjacking attack and a security policy is proposed to prevent malicious browser extension attacks			
23.	Not Mentioned	An approach to detect the malicious behaviors in sharing videos focus on cross-domain requests authorized by the Flash platform by applying flow network analysis.	Implementing	Detecting attacks	[51]
24.	FakeBook	An approach to serve as a prior detector of potential fake profiles in a certain SNS in which a real user never sign up and make alert the SNS providers to do further investigations by use of friend network graph.	Implementing	Detecting attackers	[54]
25.	Not Mentioned	A system which hides users' identity when they visit to unreliable web sites by defining a fine-grained access control policy for revealing authentication by a data owner.	Implementing/ Setting Policies	Protecting of user's privacy	[23]
26.	Not Mentioned	A framework which defends the malicious crawlers from crawling users' private data, based on the mechanism of URL time out.	Implementing	Protecting of user's privacy	[84]
27.	LotusNet	A framework which supports strong authentication and lets the users to adjust privacy settings through fine-grained access control system. This scheme is based on single peer-to-peer network and distributed hash table method.	Implementing	Protecting of user's privacy	[45]
28.	PESAP	A framework which protects users' private information when interacting with third party applications, based on anonymizing of social graph and making secure of the information flow inside the browser.	Implementing	Protecting of user's privacy	[30]
29.	PhishAri	A tool which automatically detects the phishing attacks in Twitter by checking the posted tweets with URLs by use of special feature of Twitter and URL features.	Implementing	Detecting attacks	[43]
30.	PoX	A browser plug-in which serve as fine-grained access control on user's private data prior to the transmission them to third party applications.	Implementing	Protecting of user's privacy	[57]
31.	CRiBAC (Community-centric Role Interaction Based Access Control)/SeCON	A model which extends the existing model and which makes SNSs to support cooperation among users in order to control unauthorized access to the properties of the users, communities and online social networks.	Implementing/ Enhancing	Protecting of user's privacy	[95]
32.	Not Mentioned	An approach which identifies the spam campaigns in SNSs based on 7 identified features by use of clustering-based approach, Markov clustering.	Implementing	Detecting attacks	[13]
33.	Anti-copy	An approach which prevents copying other's personal information especially photos by introducing new features for Facebook.	Setting Policies	Protecting of user's privacy	[86]
34.	AppInspect	A framework which automatically detects the malicious behaviors of third party applications in SNSs.	Implementing	Protecting of user's privacy	[13]
35.	CATS	A tool which detects the spammers in Twitter by applying analyzed new features and generated models.	Enhancing	Detecting attackers	[48]
36.	CP2	A framework which designed to protect users' private information when they interact with third parties, by applying public-key broadcast encryption scheme.	Implementing	Protecting of user's privacy	[80]
37.	Not Mentioned	This work contains analyzing the weakness in system design of Facebook and Twitter and suggesting putting new module in commonly used DPIS algorithm in detection of phishing attack.	Enhancing	Preventing from attack	[37]
38.	Not Mentioned	This work first analyzes the features of Twitter spammers in depth and design a new feature set to detect the spammers based on those new features.	Enhancing	Detecting attackers	[17]
39.	Friend in the Middel (FiM)	An approach to countermeasure friend in the middle attack in SNSs by making the attackers to face with difficulty when they re-identify an anonymized user in SNSs.	Implementing	Preventing from attack	[50]
40.	Not Mentioned	Architecture which let users control of their own privacy rather than SNSs based on a generic rights management platform called OpenSDRM.	Implementing	Protecting of user's privacy	[76]
41.	Not Mentioned	A mechanism which make SNS as an alarm to give real-time alerts for new type of malware and attacks in Twitter by automatically mining the posts in Twitter.	Implementing	Preventing from attack	[46]
42.	Not Mentioned	This work discusses information security awareness from the Islamic point of view.	Addressing security awareness	Preventing from security breaches	[58]
43.	Not Mentioned	An approach which preserves user's privacy without affecting to the utility of the information by protecting social graph extracted from Twitter by used of k-anonymity protection method.	Implementing	Protecting of user's privacy	[75]
44.	Not Mentioned	A framework which allows third party applications to utilize some of users' private without actually transferred to those applications and let users have controls upon their data.	Implementing	Protecting of user's privacy	[32]

45.	REPLOT	An approach which detect and characterize the malicious social campaigns in Twitter by combining of authorship attribution techniques and behavioral analysis.	Implementing	Detecting attacks	[79]
46.	Not Mentioned	This work includes organizing different types of common attacks on SNSs and give some facts of how to protecting them.	Addressing the attacks, Providing suggestions	Protecting of user's privacy/ Preventing from attacks	[12]
47.	Not Mentioned	This work builds social engineering knowledge base by identifying the different entities and sub-entities that affects the social-engineering related attacks in SNSs.	Implementing	Preventing from attack	[28]
48.	SONET	A social network model which monitor and rank the privacy and can be calculated the privacy risk in real time with the proposed privacy risk indicator, PDIX.	Implementing	Protecting of user's privacy	[78]
49.	Not Mentioned	An approach which detects the social spam profiles in Twitters based on four categories of data: content, behavior, interaction and graph.	Implementing	Detecting attackers	[16]
50.	TrustBook	A trust-based approach which verifies the legitimacy of a user by applying OpenPGP digital certificates or web of trust public key system.	Implementing	Verifying legitimate users	[40]
51.	Not Mentioned	A scheme which protects the users from identity theft attack without affecting the nature of social networks. This scheme consists of three approaches and is based on multiple social networks.	Implementing	Protecting of user's privacy	[29]
52.	Not Mentioned	This work includes providing more effective guidelines to build honey profiles in Twitter and designing two samplers which crawls more likely spammer accounts.	Setting guidelines/ Implementing	Detecting attackers	[18]
53.	SQLDetector	A prototype tool which applies the methodology of reducing the false positive in the detection of SQL injection vulnerability by use of data mining techniques.	Implementing	Detecting attacks	[38]
54.	Not Mentioned	This work includes the summarizing the previous tools and techniques in solving clickjacking attack, testing out and providing ways to improve defenses in client side and during development.	Enhancing	Preventing from attack	[89]
55.	Not Mentioned	In this work, a set of security policies are proposed to enhance the current privacy policies of Facebook.	Setting policies/Enhancing	Protecting of user's privacy	[49]
56.	Detecting Cloning Attack (DCA)	An enhanced system which detects cloning attack by differentiating between cloned and real account, based on user action time period and user's click pattern.	Enhancing	Detecting attacks	[22]
57.	Not Mentioned	This work includes designing mechanisms to detect cloned profiles and fake profiles in cross-site or same site of SNSs and setting guidelines for SNS users and providers in order to reduce cloning attacks.	Implementing/ Setting guidelines	Detecting attacks/ Preventing from attack	[12]
58.	Not Mentioned	A scheme which filters the potential malicious accounts in Twitter based on account names and the creation time by employing data mining algorithms.	Implementing	Detecting attackers	[70]
59.	Not Mentioned	This work contains investigating the impact of source characteristics on naivety of the users in facing of social engineering attack in Facebook and developing a model which explains what and how source characteristics overwhelmed upon Facebook users to decide the attacker as credible.	Implementing	Preventing from attack	[27]
60.	SybilBelief	A framework which detects the Sybil nodes in SNSs and performs Sybil classification and ranking.	Implementing	Detecting attack	[61]
61.	Twitter Sybil Detector (TSD)	A browser plug-in which utilizes the classifier that is built based on the identified Sybil detection features and notifies the users of the Sybil accounts.	Implementing	Detecting attackers	[47]
62.	Not Mentioned	A system which identifies suspicious URLs in SNSs by applying Bayesian Classification algorithm.	Implementing	Detecting attacks	[41]
63.	Not Mentioned	A complex system which takes advantages on real-life social trust among average users in order to protect the users' sensitive data as well as the cryptographic keys.	Implementing	Protecting of user's privacy	[92]
64.	Not Mentioned	This work includes investigations of security attacks on SNSs in recent years, analysis of why and how attackers perform attacks and countermeasures for both SNSs and users to avoid from those attacks.	Addressing attacks, Providing suggestions	Protecting of user's privacy/ Preventing from attacks	[72]

TABLE VII. PROPOSED ATTACK MODEL, DESCRIPTION AND SOLUTION

No.	Attack Model	Year	Brief Description of Attack	Solution to Attack	Reference
1.	iCloner	2009	With their attack scenario, users' personal information are automatically crawled, profiles are cloned and sent friend requests to the victim's friends in the SNSs in which the victims have never registered.	No Solution is mentioned.	[25]
2.	Automated Social Engineering Bot	2009	This attack cycle describes the ways how SNSs can be misused for social engineering attacks by setting the attack to be automated for time-reducing purpose.	No solution is mentioned.	[63]
3.	De-anonymization Attack	2010	This attack learns the identity of the users by misusing the group membership information in a certain SNS applied stealing web browser history stealing attacks.	No solution is mentioned.	[91]
4.	Antisocial Networks	2010	This work presents how the original features of SNSs makes itself be a platform for attackers to do DDoS attacks, malicious objects embedding and personal information leak.	No solution is mentioned.	[31]
5.	Not Mentioned	2011	An identity cloning attack model which collects more personal information of the users by exploiting the trust model of SNSs and maintaining the eligibility of fake accounts.	No solution is mentioned.	[52]
6.	Not Mentioned	2011	An attack model which shows that how an attacker could build the artificial identities seems to be real.	No solution is mentioned.	[67]
7.	Friend-in-the-Middle (FITM)	2011	An attack which develops to overcome the various access-protection measures of SNSs by doing session hijacking activities on the network layer.	All of the communication should be done over HTTPS platform.	[64]
8.	Not Mentioned	2012	According to the scenario, one Twitter account which is compromised by an adversary and is led to the malicious site. The victim tweet the malicious short URL to his/her followers, and it repeatedly spread followers by followers.	Only general suggestion is given. They point out Twitter new feature, short URL provider and crowd sourcing anti-virus software.	[83]
9.	Not Mentioned	2013	Three attack scenarios are presented: *A simple attack* which is compromising one Twitter account and let it spread malicious URL to his/her followers. *An Advanced self-propagating scenario* which retweets malicious URL whenever user clicks the link by using clickjacking techniques. *A complex attack scenario* which makes the Twitter user be victimized when he/she visit blogs or other news websites by inserting malicious URL in comments or in the conversations.	No solution is mentioned.	[82]
10.	Cascading Failures	2014	This work introduces a cause named cascading failures and shows how super users can make the complete failure of a social network.	No solution is mentioned.	[94]
11.	Graybot	2014	A botmaster uses fake accounts and tweets the post which contains commands that are correctly interpreted by infected bots. The botclients received those commands and launch the attack in victimized machines by using Diffie Hellman Key Exchange.	No solution is mentioned.	[85]
12.	Forest Fire Attacks	2014	This attack points out the weakness of trustee-based authentication systems of SNSs and shows how an adversary can misuse that feature.	Three aspects of solutions, to hide trustee networks from attackers, to mitigate spoofing attacks, to make right decision in selection of trustee, are proposed.	[61]
13.	Trusted Friend Attack	2014	This attack scenario exploits the loophole of Facebook's trusted friend feature and sets the plan by learning one of the identities of the victim, making friend with them and cheating the accounts.	No solution is mentioned.	[65]
14.	Inference Attack	2014	This attack is newly proposed attack and it can be happened when an information leakage process occurred in which a malicious extension tries to infer the uncovered information via legitimately accessible information. The ways how inference attack could happen via third party applications are discussed.	No solution is mentioned.	[44]
15.	Mutual Friend Based Attack	2013	This attack scenario shows that how an attacker can launch privacy attacks by misusing one of the features of SNSs, mutual friend.	No solution is mentioned.	[24]
16.	Extended Susceptible-Infected-Susceptible (SIS) Model	2013	A virus propagation model which shows that how fast is the virus propagation in a group network than in a network without group.	No solution is mentioned.	[59]
17.	Social Network Relay Attacks and other vulnerabilities	2012	Possibilities of six privacy threats on Facebook and Twitter have introduced based on the loopholes of Facebook's account recovery service, Facebook's timeline feature and ways of how an attacker reconstruct a victim's friend list, how an attacker can manipulate a victim's account once it has taken over, how social plug in breaches user's privacy, introduction of network relay attacks.	New policies for Facebook SNS providers are introduced in order to solve those problems.	[39]
18.	Not Mentioned	2013	An attacker model which contains four attack modules, monitoring	No solution is mentioned.	[93]

			attack module, replay attack module, phishing attack module, and impersonation attack module, in order to test the robustness of OAuth 2.0 protocol.		
19.	Not Mentioned	2014	Seven attacks scenarios for three SNSs (Facebook, Twitter, Google+) were introduced in order to show that privacy leak could still occur though the users set the privacy settings properly.	They provide necessary conditions to be aware and suggestions for the users to mitigate those privacy problems.	[35]