Information Systems Security Practices in Social Software Applications: A Systematic Literature Review

Journal:	*Aslib Journal of Information Management*
Manuscript ID	AJIM-08-2016-0124.R2
Manuscript Type:	Research Paper
Keywords:	Information Systems Security practice, Social Software Applications, Systematic Literature Review, Availability, Confidentiality, Integrity

Information systems security practices in social software applications: A systematic literature review

[1]Azah Anir Norman, [2]Suraya Ika Tamrin and [3]Suraya Hamid
Faculty of Computer Science and Information Technology
University of Malaya, Kuala Lumpur, Malaysia
[1]azahnorman@um.edu.my, [2]surayaika@yahoo.com and [3]suraya_hamid@um.edu.my

Abstract:
Purpose – The paper aims to investigate the current Information Systems Security (ISS) practices of the Social Software Application (SSA) users via the Internet.
Design/methodology/approach – The paper opted for a systematic literature review (SLR) survey on ISS and its practices in SSAs between 2010 and 2015. The studiy includes a set of 39 papers from among 1,990 retrieved papers published in thirty-three high impact journals. The selected papers were filtered using the Publish or Perish (PoP) software by Harzing and Journal Citation Index (JCR) with an inclusion criterion of least 1 citation per article.
Findings – The practice of ISS is driven by the need to protect the confidentiality, integrity, and availability of the data from being tampered. It is coherent with the current practice as reported by many researchers in this study. Four important factors lead to the ISS practice in SSA: protection tools offered, ownership, user behavior and security policy.
Practical implications – The paper highlights the implication of successful ISS practices is having clear security purpose and security supported environment (user behavior and security protection tools) and governance (security policy and ownership) protection tools offered, ownership, user behavior and security policy towards ISS practice by the users.
Originality/value – This paper fulfills an identified need to study how to enable ISS practice.

Keywords Information systems security practices, Social software applications, Systematic literature review, confidentiality, integrity, availability
Paper Type Literature review

1. Introduction

Social network sites (SNSs), also known as social software applications (SSAs), are defined as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and navigate their list of connections and those made by others within the system (Boyd and Ellison, 2007). Through these SSAs, such as Facebook, Twitter, Instagram and LinkedIn, individuals are given the opportunity to share their valuable thoughts and information with a wider audience with different demographics. They also allow users to receive updates about upcoming events in their local societies or in the world. For these reasons, SSAs have become a very popular tool for interaction in today's society. Additionally, a summary of SSA literature review was found and all of them were published in the period between 2007 and 2012. Those are presented in Table I in chronological order to take the reader from the oldest to the most recent (ALTAMIMI, 2013).

The terms of social media, social networking application, and mobile messenger referring to applications such as WhatsApp and Messenger, have been widely used for a number of years. However, there are inconsistencies in the usage of these terms that may cause confusion. Sometimes, social media is treated as the general term for social networks sites such as Facebook, Twitter, blogs and YouTube (Leonardi *et al.*, 2013; Gao *et al.*, 2011). At other times, the term social networking application refers to mobile messaging applications such as WhatsApp, TweetBot, Hangouts and Vine within the context of smartphones. However, it is useful to simply apply the term social software application (SSA) to refer to the entire range of available social software, such as social networks, social news outlets, media sharing sites, mobile messengers, blogs and wikis, that can be accessed through all mediums of communication such as desktops, laptops and mobile devices. Therefore, in this paper, the term SSA refers to any social software, including social networks, which serve as social sites that provide services for connecting with other users (Grahl, 2014; Water *et al*., 2009), and mobile messengers, which provide instant messaging for smartphones.

In recent years, the number of SSA users has been rapidly expanding. As reported by ComScore, SSAs such as Facebook and Twitter are now used by 84 percent of the world's online population, and thus 1.3 billion users around the world (ComScore, 2015). Meanwhile, in 2011, eMarketer predicted that the number of SSA users around the world would rise from 1.47 billion in 2012 to 1.73 billion in 2013, an 18% increase (eMarketer, 2013). By 2017, the global SSA users' population will total 2.55 billion (eMarketer, 2013). Facebook, for instance, has more than 400 million active users and hosts more than 25 billion pieces of contents are shared each month (Li and Chen, 2010). This statistic shows that SSAs are widely accepted and used by today's society.

However, Information Systems Security (ISS) has become a critical strategic issue in SSAs and has been widely discussed (Hajli and Lin, 2014; Sanchez and Demazeau, 2014; Gritzalis *et al*., 2014). It encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets (Peltier, 2001). Many issues have been raised regarding the security on SSA, such as those related to viruses, trust, privacy, ownership and many other concerns (Hajli and Lin, 2014; Sanchez and Demazeau, 2014; Gritzalis *et al.*, 2014; Abdulhamid *et al.*, 2014). Hence, SSAs require ISS, which is essential for the safety of SSA users.

In this study, the researchers conducted a systematic literature review (SLR) to address the research questions. The SLR method helped guide the research in the identification, evaluation, and synthesis of the existing body of completed and recorded work produced by researchers, scholars, and practitioners (Okoli and Schabram, 2010). It is a systematic, explicit, comprehensive, and reproducible method of searching for credible and relevant articles to answer the research questions developed for this study. The researchers, then, present a comprehensive literature study based on a review of 39 empirical studies selected that have been drawn from high-impact journals with at least one citation, from the period between 2010 and 2014, as presented in Table II. The SLR was conducted following the guidelines provided by previous research. The objectives of this study were to demonstrate the increasing popularity of SSA usage incorporating the practice of ISS by users and to determine the success factors for ISS practices in SSAs. This paper presents the complete results of the findings from the SLR. The major contributions of the paper are as follows:

1) This SLR explores the relationship between ISS and SSAs, of which a comprehensive understanding is currently lacking in the available academic literature.
2) The study provides an analysis of the current trends of ISS in SSAs.
3) The study also presents an analysis of the motivations for SSA users to practice ISS.
4) Finally, the study identifies the factors that contribute to ISS practices in SSAs.

The purpose and benefits of a comprehensive study of ISS in SSA-related work are discussed in Section 2, and the research methodology and research questions are explained in Section 3. The detailed planning of the study to address all identified research questions is presented in Section 4. Section 5 discusses the main findings regarding the current trends and factors contributing to ISS practices in SSAs. The paper concludes with a discussion of the main findings based on the stated objectives, the limitations of this study and recommendations for future research.

2. Background and motivation

Okoli and Schabram (2010) stated that an SLR study may be conducted for a variety of purposes, such as providing a theoretical background for subsequent research, summarizing the breadth of research available on a topic of interest or answering practical questions by consulting existing research for insight on the matter. Thus, the purpose of conducting an SLR for this study is to seek a solid starting point for other researchers interested on the subject of ISS and SSA.

The advantage of this SLR study is that it reveals which areas have been covered and what tools have been proposed. It also provides guidelines to assist researchers in planning future work by analysing the existing evidence for various techniques and also by identifying research areas that require further attention in this field. Additionally, this SLR study provides an overall review for users with regard to security on SSA, thereby enhancing the knowledge of users on this subject and potentially increasing their level of concern.

3. Research Questions

The intent was to identify all empirical papers published with citations between 2010 and 2014 that investigated and evaluated ISS in SSAs. During the planning stage of this SLR, the researchers formulated the following questions based on the objectives with appended rationales:

RQ1: What is the purpose of ISS in SSA?

George (2006) stated that popular press coverage of SSAs has emphasized potential security concerns, primarily concerning the safety of younger users. Thus, this RQ was developed to identify the importance of implementing the security in SSA.

RQ2: What are current trends of ISS in SSA?

This RQ was developed to provide new input and expect the security impact towards SSA users. According to Smith and Eloff (1999), the current trends are needed for protecting the confidentiality and integrity in SSA, whilst at the same time ensuring its availability to authorized SSA providers.

RQ3: What factors motivate SSA users to practice security management?

Through the experience in the development and application of IT, SSA users learned the importance of ISS and the needs to practice security in SSA (Chang and Ho, 2006). Thus, this RQ was formulated in order to educate and enhance SSA users to implement security management in SSA.

RQ4: What are the factors that contribute to the implementation of ISS practices in SSA?

This RQ was developed to identify the importance to practice the ISS in SSA. Luo *et al*., (2009) asserted that both users and SNSs have an impact on the security of SSA. Hence, SNSs should provide users with enough security support and users should increase their security awareness to combat the growing number of attacks.

4. Systematic Literature Review Planning

This study adopted SLR method from Kitchenham *et al*., 2009 because it is well structured and indicates step-by-step procedure to find and select relevant papers on a particular topic. Additionally, the SLR method also determines that research questions should exist to help researchers to find the appropriate research context. The SLR method by Kitchenham *et al*., (2009) received 644 citations, hence proved that the method is robust enough to answer the research questions.

This study was conducted by three researchers, including a research assistant, the first researcher with expertise in the field of ISS research and second researcher with expertise in SSA studies. Any conflict with regard to any issue was discussed among the three researchers, and a decision was reached upon the agreement of all three. In this study, the three researchers have gone through the three main phases of SLR as proposed by Keele (2007). These consist of planning, execution, and reporting results. In conducting this SLR, the researchers developed a formal protocol during the planning phase. The protocol consisted of the details of paper search strategy, guided by the research questions formulation, filtration process, inclusion of keyword criteria, quality appraisal assessment, data extraction strategy, data synthesis and analysis guidelines and writing the review process. The protocol then was tested by the research assistant to evaluate the completeness of the review search string, and correctness of the keyword criteria, plus data extraction strategy. After the protocol was tested, all findings were discussed among the three researchers for the conclusion findings. Minor recommended amendment was required from both researchers related to the scope of SLR, and it was incorporated into the protocol. During the execution phase, the protocol was refined. Finally, the reporting result is followed after the execution phase.

In this section, the researchers discuss the following eight steps of the research method, as explained in Okoli and Schabram (2010) as follows.

4.1 Purpose of the literature

This first step requires the clear identification of the purpose and intended goals of this SLR study. This is necessary for the reader to clearly understand the study and its ramifications.

In this study, the specific goal was to identify, analyse, and synthesize the high-impact journal publications with at least one citation during the past 5 years in the field of ISS in SSAs, with an in-depth focus on the current trends in and motivations towards the practice of security management. Hence, this purpose for conducting this SLR was to answer the above-mentioned research questions.

4.2 Protocols and training

A protocol is defined as a plan that describes the manner in which a proposed SLR is conducted (Kitchenham and Charters, 2007). The research protocol of this study began with the determination of the research objectives, followed by the formulation of the research questions. Subsequently, the SLR technique was used as the method for performing the research, hence becoming the protocol of this study. Meanwhile, training refers to the process of evaluating the questions. The formulated questions were evaluated by two researchers with expertise in the fields of ISS and SSAs, respectively, to test the validity and reliability of the questions. These two experts participated in the research performed throughout this study.

4.3 Literature search

This step involves the planning and selection process for collecting publications from the literature. Traditionally, researchers have used books as their main sources of published studies. By virtue of recent advancements in technology, the researchers implemented a structured approach to selecting and narrowing the body of journals to be investigated through keyword searches. The researchers will briefly discuss the following aspects of the literature search:

- Journal Citation Reports
- Publish or Perish (PoP) software by Harzing

Journal Citations Report (JCR) is the recognized authority for evaluating journals (Reuters, 2014). It offers a systematic, objective means of critically evaluating the world's leading journals using quantifiable, statistical information based on citation data. By compiling the cited references to articles, JCR helps to measure these articles' research influence and impact at the journal and category levels and elucidates the relationship between citations and cited journals.

The researchers utilized JCR to determine the journals of interest for this study in three steps as follows:

a) Chose the *JCR Science Edition* for the year of *2013*.

b) Viewed the group of journals in the *Subject Category* of "COMPUTER SCIENCES, INFORMATION SYSTEMS" – this category is the most closely related to the study field of ISS in SSAs.

c) Sorted the journal data by *Impact Factor* to obtain only the highest impact journals, consistent with the goals for this SLR study.

As a result, as of 17th December 2014, the researchers selected 33 publications in high-impact journals (Q1) from among the 135 total relevant journals as follows:

- ACM Transactions on Intelligent Systems and Technology (ACM)
- IEEE Wireless Communications (IEEEWC)
- IEEE Communications Surveys & Tutorials (IEEECST)
- MIS Quarterly (MISQ)
- Journal of Cheminformatics (JC)
- Journal of Chemical Information and Modelling (JCIM)
- Journal of the American Medical Informatics Association (JAMIA)
- Information Sciences (IS)
- Journal of Information Technology (JIT)
- IEEE Network (IEEEN)
- Journal of the ACM (JACM)
- IEEE Transactions on Mobile Computing (IEEETMC)
- International Journal of Medical Informatics (IJMI)
- IEEE Transactions on Information Theory (IEEETIT)
- Knowledge and Information Systems (KAIS)
- Journal of Strategic Information Systems (JSIS)
- Journal of the American Society for Information Science and Technology (JASIST)
- IEEE Pervasive Computing (IEEEPC)
- IEEE Transactions on Information Technology in Biomedicine (IEEETITB)
- Decision Support Systems (DSS)
- IEEE Transactions on Services Computing (IEEETSC)
- Ad Hoc Networks (AHN)
- Journal of Management Information Systems (JMIS)
- International Journal of Information Technology & Decision Making (IJITDM)
- IEEE Transactions on Knowledge and Data Engineering (IEEETKDE)
- Mobile Information Systems (MIS)
- Information & Management (IM)
- IEEE Transactions on Multimedia (IEEETM)
- IEEE Multimedia (IEEEM)
- IEEE Systems Journal (IEEESJ)
- Data Mining and Knowledge Discovery (DMKD)

- Annual Review of Information Science and Technology (ARIST)
- The VLDB Journal (VLDBJ)

Publish or Perish Software (PoP) program offers a swift and elegant tool for providing essential output features. It generates 18 bibliometric and scientometric indicators from the result set produced by Google Scholar (Jasco, 2009). PoP offers the capability of assigning items to their original ranked positions in the list of result Google Scholar. It also correctly sorts the results in order of decreasing citedness. Therefore, the researchers chose to adopt the PoP program because these features facilitate the determination of citation counts. The program also provides the option to select and deselect articles based on citation counts, hence simplifying the task of collecting related articles based on the selection criteria. As one of the inclusion criteria was that the articles must have been cited, PoP assisted the researchers in efficiently achieving this goal.

When implementing the PoP program, the first necessary task was to fulfil the entire required field in the *General Citations* options with the required information as follows:

• *Author(s)*	: Empty (the aim was not on the authors)
• *Publication*	: The name of each journal identified form JCR as listed above, one-by-one
• *All of the Words*	: INFORMATION SYSTEMS SECURITY AND SOCIAL NETWORK
• *Any of the Words*	: Empty (not useful for the study)
• *None of the Words*	: Empty (not useful for the study)
• *Phrase*	: Social Network (specified the focus on keyword)

As the most common and highly tagged term used on the Internet in SSA studies is the term *social network*, the researchers performed the keyword search using this term to ensure the collection of a broader variety of articles than would have been identified using the term *SSA* alone. The data source for this study was Google Scholar entries between the years of 2010 and 2014. The results of the search process were first obtained on November 3, 2014, and they were later updated through December 17, 2014.

4.4 Practical screening

This step involves the process of filtering a large number of initially identified studies to select only the studies that should be considered in the SLR. As stated by Sterne *et al.,* (2001), the reviewer must make several critical decisions regarding what types of work should be included or excluded. Thus, the researchers specified two selection criteria to finalize the number of journals to be reviewed as follows.

4.4.1 The year of publication. The papers must be published within the years of 2010 and 2014. Particularly, this 5-year period was chosen because the researchers tend to focus only on current issues and trends regarding the ISS and SSA. According to Petticrew and Roberts (2006), they suggest that the review considers the current evolutionary state of the field of research: a SLR is not very valuable early on when limited studies might be available, as the few existing studies might not represent the best knowledge that more time might give. Hence, 2010 to 2014 is considered the best time to practice this review.

4.4.2 Five inclusion criteria. To select the desired journals for this study, the researchers take into account five inclusion criteria as follows:

a) The publication name. One of the problems the researchers discovered when using the PoP software program is that it does not strictly identify the name of a publication exactly as it is typed. PoP will also list all publications with similar names. For instance, when the researchers entered the publication name "*Information & Management*", the program returned results for many publications with similar names containing the terms information and management, such as the "*International Journal of Information Management*", the "*Journal of Global Information Management*" and many others. The researchers had no interest in these unrelated journals, as the researchers wished to focus only on the high-impact journals identified by JCR. Thus, the researchers applied a filtration process to select only the specified journals.

b) Publications with at least one citation. Why did the researchers count the citation in the first place? A citation is a form of acknowledgment that one research paper gives to another and it is used as a measure of scientific influence and productivity (Smith, 1981). Additionally, Thompson (1991) stated that citation counts are used widely as an index of quality of research output. Thus, the researchers consider all the cited paper as relevant, replicated and quality to be counted in this research. PoP aided the researchers in this goal by providing citation counts and related information. The software also listed articles with zero citations; however, the researchers could simply uncheck the zero-citation articles and select only articles with one or more citations for inclusion in the SLR discussion.

c) Keyword – information systems security. As this study focuses on the field of ISS and SSAs, the third screening process was to select articles in the identified journals with the keyword '*information systems security*'.

d) Keyword – social network. Identical to the criterion described above, the researchers applied the fourth screening process to select journal articles with the keyword '*social network*'. As mentioned previously, the researchers chose to use the term social network in the keyword search to obtain a broader selection of articles compared with the scope of the articles that would have been identified using the term SSA, which is quite limited. The researchers needed a broad collection of articles to ensure that the researchers covered the most appropriate and targeted studies before proceeding with the subsequent quality appraisal and data extraction. The researchers performed the keyword searches separately instead of combining the two keywords because this approach allowed us to obtain more precise results. Only articles with these two keywords were selected for analysis.

e) *Abstract and conclusion.* The final procedure applied during practical screening to select only those articles related to the objective by reading the abstract and conclusion. The abstract provides an overall review of the article, and the conclusion helps to identify the outcome of the study and any specific circumstances that it addresses. The researchers performed this filtering to ensure that the study remained focused on the intended outcome and objective.

4.5 Quality appraisal

After performing practical screening, quality appraisal took place. This involves examining the selected articles in greater depth to assess their quality. As mentioned in Kitchenham and Charters (2007), quality instruments must be developed that incorporate both the subjective predispositions and the objective criteria set by the researchers. However, Leidner and Kayworth (2006) stated that the best quality is achieved when the articles are sorted based on methodology rather than placing an emphasis on numbers, even when exclusions must be made. Additionally, in reviews in which there is a minimum quality standard for acceptance, the quality appraisal becomes a second methodological screening process to eliminate articles that do not meet the standards established by the reviewer (Fink, 2005).

In this study, the quality of the selected studies was evaluated based on both the research method adopted as well as the quality of the reported results, as these are recognized as the only means of quality assessment available to us (Dyba et al., 2007). Overall, the researchers performed a three-stage quality appraisal as follows.

The quality of the publication outlet. For the purpose of evaluating the quality of the outlets through which the papers were published, the researchers utilized JCR, which is the recognized authority for evaluating journals. To ensure the quality of the included papers, the researchers selected only publications in high-impact journals.

The impact of the paper. To assess the impact of the published papers, the researchers checked their citations using the PoP software by Harzing (as discussed in Section 4.3).

The quality of the study. It was necessary to filter out studies that utilized poorly described research methods. One type of organizer that can be used for this purpose is called a Literature Review Matrix (LRM); such a matrix can be a useful tool for relating and organizing information and for managing sources for citation purposes (SGPPWritingCenter, 2009). In addition, an LRM is one method of developing a graphic organizer to illustrate how certain authors' ideas relate to other authors' ideas. Hence, the researchers developed an LRM to assist in evaluating the studies based on the effectiveness with which they reported the details of the design and execution of their empirical methods. One participating researcher applied this LRM to the selected articles. Then, feedback and discussion were provided by the other two researchers for the purpose of quality checking. The LRM was used not to score or rank the papers but rather to filter out low-quality papers before data extraction.

Moreover, according to Kitchenham *et al.,* (2009), basically, SLR steps have address validity and reliability issues. Such steps namely are:

a) Use of specific keywords for particular review

b) Use of reliable Online Databases and not just normal Google search

c) Use of reliable and ranked journal publications like ISI and A* ranked

d) Use of inclusion and exclusion criteria set earlier in the SLR process

e) Filtering the papers by removing articles not relevant in titles, abstract, and contents

f) Member checking of analysis by each team member

4.6 Data extraction

In this crucial stage of the SLR, the final list of selected articles constitutes the material used for the final SLR and provides the information to be used as the raw material in the synthesis stage. The data were extracted in the form of a list that consisted of the following components: (1) author and year; (2) title; (3) objectives and research questions; (4) research methodologies, design, and samples; (5) implications for practice or research theory or selected findings; (6) limitations; (7) results and conclusions or outcome variables; and (8) future research. Based on the matrix components listed above, the researchers identified the current trends in security practices in SSAs.

4.7 Synthesis of studies

This step involves aggregating, discussing, organizing and comparing the extracted data. Then, the outcome of the study is synthesized. Based on the data extracted in the previous step, the researchers summarized the current trends and patterns identified from all selected journal articles. Additionally, the researchers differentiated between *'information systems security'* and *'social networks'* for the following reasons:

a) The researchers recognize that issues related to ISS do not solely belong to the context of SSAs. Certain ISS techniques can be robustly implemented in a wide variety of environments, including SSAs. Hence, the researchers performed a broad keyword search on *'information systems security'*.

b) The researchers consider that treating the ISS and SSA concepts individually can yield broader results that nevertheless have implications for the SSA environment.

4.8 Writing the review

After the completion of all seven steps listed above, the entire process of a SLR must be summarized in a written report in sufficient detail that the results of the review can be independently reproduced (Okoli and Schabram, 2010).

5. Execution of the Systematic Literature Review

Through primary string searches, the researchers retrieved a total of 1,990 papers. The researchers then applied the five criteria discussed above to narrow the selection from this large number of retrieved papers to only higher quality papers, as shown in Figure 1. Irrelevant papers were eliminated after Step 1 of the study selection process. The remaining papers were then filtered in Step 2 using the inclusion/exclusion criteria, which reduced the selection to 565 relevant papers. The researchers then proceeded with the citation count check in Step 3, allowing further irrelevant papers (papers with no citations) to be eliminated and reducing the total to 445 papers. The *'information systems security'* keyword screening phase was performed in Step 4, after which 177 relevant papers remained. Of these 177 papers, 55 papers were excluded in Step 5 because they were irrelevant to the *'social network'* keyword.

Finally, after considering the abstracts and conclusions of the papers remaining after Step 5 (the final inclusion study), the researchers agreed to review 39 relevant papers in this SLR study.

6. Results

In this section, the researchers elaborate on four different categories of characteristics of the 39 selected studies as follows.

6.1 Quality attributes

The number of times a paper is cited is considered to be a good indicator of the impact of that paper (Wikipedia, 2015). Thus, the quality attributes depend strongly on the number of citations of the selected articles. The results (as shown in Figure 2) showed that of the papers selected using the applied exclusion and inclusion criteria, three papers had 9 citations, which was the highest number of citations among the selected studies, and there were ten papers each with 1 or 2 citations. Table 3 provides the complete reference for each of the top 5 most highly cited studies considered in this paper.

6.2 Temporal attributes

Of the 39 selected papers from the five years between 2010 and 2014, six articles were published in 2010, seven articles were published in 2011, six more articles were published in the year 2012, thirteen articles were published in 2013 and the remaining seven articles were published in the year 2014. Figure 3 presents the overall chronological distribution of the studies.

6.3 Research methodologies

Of the 39 selected studies, 21 were experiments, 7 were surveys, 7 were field studies, 2 were grounded theories, one was action research and one was a case study, as shown in Figure 4. The corresponding usage percentages of the various research methods in the reviewed studies are as follows: 54% experiments, 18% surveys, 18% field studies, 5% grounded theories, and 3% for both action research and case studies. The majority of the studies used experimental research methods, and only one each used action research methods or the case study approach.

6.4 Data sources

The journal with high impact factor is referring to the average number of times articles from the journal published in the past two years have been cited in the JCR year. An impact factor of 1.0 indicates that, on average, the articles published one or two year ago has been cited one time (Reuters, 2012).

As discussed above, all 33 high-impact journal publications were used for the initial article selection. However, after the filtration process, only 16 journals discussed ISS and 39 studies were drawn from them. It is important to note that all selected studies were published in journals that have retained high impact factors for years. In this study, all the paper selected is from impact factor within the range of 9.390 and 1.701, as shown in Table 4. This clearly indicates the rigor and quality of the data sources from which the researchers obtained the collection of studies to review.

7. Findings

Based on the data extracted from our set of 39 selected studies and the analysis thereof, the researchers now present the findings to answer each of the research questions.

RQ1: What is the purpose of ISS in SSA?

With regard to ISS, there is no guarantee that the available security tools will fully protect a SSA from any uninvited attacks. As stated in PandaLabs (2013), anyone who works in the ISS field knows that nothing is 100% secure. Thus, from the researchers' point of view, the purpose of ISS in SSA is to protect the confidentiality, integrity and availability of the data being attacked from any unwanted malicious action that may harm the SSA system to the greatest degree possible.

SSAs have always been a favourite target of attacks. On Facebook, for instance, there was a security incident in January 2002 in which a worm was discovered that had allowed over 45,000 Facebook login credentials to be stolen (PandaLabs, 2012). More recently, Paganini (2015) reported a large increase in phishing attacks, up 19% during the second half of 2011. The total losses incurred by various organizations due to such attacks over the last 18 months amounts to $2.1 billion. These statistics illustrate that ISS is an important component that requires expert security implementation in every aspect of the security pillars of a SSA environment, which include confidentiality, integrity, and availability. There is no doubt that appropriate security measures should be considered by developers to gain users' trust in their online SSA. Additionally, SSA can be valuable and the best place to communicate with each other as long as the security concern is applied.

The main purpose of ISS in SSA is to protect end-users' privacy. This clearly shown in Table 5, where 26 out of 39 papers reviewed, emphasized on the privacy issues. Privacy addresses problems of information protection from third parties and hence increases end-users' confidentiality when communicating in the SSA.

RQ2: What are the current trends of ISS in SSA?

The most popular current topic of discussion trend being widely discussed in the field of ISS is privacy, as shown in Table 5. According to Gross and Acquisti (2005), in one of the first academic studies of privacy and SSAs, the researchers who conducted the study analysed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information included on the site by the students, such as the potential for determining users' Social Security numbers using information often found in profiles, such as hometown and date of birth.

By contrast, survey data offer a more optimistic perspective on the issue, suggesting that teens are aware of potential privacy threats online and that many are proactive about taking steps to minimize certain potential risks. Pew Research found that 55% of teens who are active online have profiles, 66% of whom report that their profile is not visible to all Internet users (Lenhart and Madden, 2007). This finding indicates that SSA users are very concerned about the privacy and confidentiality of information shared in SSAs.

Of the 39 papers for review, 26 of the papers discussed privacy, 5 papers discussed trustworthiness, 3 discussed attack threats, 2 discussed access control, and the topics of the remaining 3 papers were network conflict, accuracy, and authorization.

Throughout the five years, the selected research papers indicate that the majority of the papers have discussed similar ISS issues which are privacy. However, other ISS issues such as threats attack, trustworthiness, network conflict, accuracy, access control and authorization were discussed inconsistently. Figure 5 shows the frequency of current trends over five years of reviewed papers. Additionally, it also represents the similarities and differences of current trends identified using the keyword search identified earlier.

RQ3: What factors motivate SSA users to practice security management?

As security becomes a more visible and pressing issue, the users of SSAs are becoming very concerned about following good security practices in SSA. This motivation of SSA users to practice security management is reflected by the current trends discussed in regard to RQ2 above. As particular ISS trends become more popular, this popularity will lend them greater impact towards influencing security practices in SSA. According to the literature analysis, as shown in Figure 6, the CIA (confidentiality, integrity, and availability) triad may influence users to practice security management as Figure 6.

1) *Confidentiality.* Defined in ISO/IEC (2005) as the ability to ensure that information is accessible only to those with access authorization. It is also a means to ensure that information is not made available or disclosed to unauthorized entities. In this paper, confidentiality is found to be the major factor driving SSA users to practice security management. Figure 6 shows that 26 papers out of 39 selected for review papers discussed the importance of confidentiality on SSA. The security trend that addresses the issue of confidentiality is privacy. According to Cleveland (2008), privacy is the primary concern related to confidentiality, and Haughn and Gibilisco (2014) stated that confidentiality is approximately equivalent to privacy. Additionally, Arapinis *et al.*, (2016) stated that confidentiality is the most obvious privacy-related property. Thus, as shown in Table 6, the researchers categorize privacy under the heading of confidentiality. Table 7 summarizes the discussions of privacy presented in the 26 papers related to this issue.

2) *Integrity.* Integrity is defined as the quality that defines assets that can only be modified by authorized parties (Fleeger and Charles, 1989). It also refers to the protection of the accuracy and completeness of information (ISO/IEC, 2014). As shown in Figure 6, of the 39 reviewed papers, 9 discussed the issue of integrity; this indicates that integrity also plays a role in SSA users to practice security management. As stated in Haughn and Gibilisco (2014), integrity involves maintaining the consistency, accuracy, and trustworthiness of data over their entire life cycle. It also includes issues related to file permissions, user access controls, and authorization. However, there is a little argument regarding access control and integrity.

Access control is defined as the security features that control how users and systems communicate and interact with other systems and resources. Yet, access controls also give the organization the ability to control, restrict, monitor, and protect resource integrity (Harris, 2007). For instance, the access to one resource is only limited to those who have been given permission or to only entities who are trusted not to mess up its integrity. This is indeed one of the primary motivations for access control. Hence, access control can be considered to fall under integrity in security. In this study, however, as shown in Table 6, the researchers consider only four security trends related to integrity: accuracy, trustworthiness, access control, and authorization. Table 8 summarizes the discussions of accuracy, trustworthiness, access control and authorization found in the 9 papers that addressed issues of integrity.

3) *Availability.* The quality that describes whether the information is accessible and usable at need when an authorized entity demands access (ISO/IEC, 2014). In addition, HillAssociates (2007) stated that the availability is the fundamental purpose and nature of networking. In other words, any event or phenomenon related to a network that may harm the system can be considered to affect its availability, for instance, a software conflict, a network conflict, a threat of attack, or a network bottleneck, among others. This paper suggests that availability concerns are less influential in motivating SSA users to practice security management, as indicated by the fact that of the 39 reviewed papers, only 4 discussed issues of availability, as shown in Figure 6. This finding implies that SSA users are not strongly concerned about this factor compared with confidentiality and integrity. Nevertheless, two security trends related to availability are considered in this study, namely, attack threats and network conflict, as shown in Table 6. Meanwhile, Table 9 summarizes the discussions of attack threats and network conflict presented in the related studies.

According to Gross and Acquisti (2005), information security is defined as the process of protecting and preserving the confidentiality, integrity, and availability of information, whether in storage or during processing or transmission. In the context of this study, the relevant issues of confidentiality are focused on (a) data confidentiality, namely, the attempt to ensure that data are available only to authorized parties, whereas integrity refers to (b) data integrity, namely, methods of preventing data from being tampered with or modified, and finally, the availability issues of interest are specifically related to (c) data availability, namely, the ability to guarantee that data will continue to be available at least at the minimal operational level in situations ranging from normal to disastrous. Hence, the triple concern of confidentiality, integrity, and availability, also known as the CIA triad, is the fundamental concept driving the development and usage of security measures in SSAs.

RQ4: What are the factors that contribute to ISS practices in SSA?

Based on the analysis of the selected literature that presented in Table 10, the researchers conclude that proper management of the CIA triad is achievable through the factors listed below. As such, the researchers deem these 4 factors to be the factors contributing to ISS in SSAs as follows:

1) *Protection tools (software/protocols/prototypes/systems)* refer to the implementation of a concept for addressing a particular security problem with the intent of protecting a SSA system from any unwanted attack that may harm it. A protection tool for security purposes could be a software program, a protocol, a prototype or a system. Such a measure can be considered to be a tool as long as it is the implementation of an idea for preventing the SSA from attacks. 13 of the 39 reviewed papers discussed the implementation of protection tools to protect SSA systems. For instance, P9, Tseng *et al.,* (2011) discussed the implementation of a Cosdes system (a Collaborative Spam Detection System) that consists of an efficient near-duplicate matching scheme and a progressive updating scheme that enables the system to maintain the most up-to-date information for near-duplicate detection.
2) *Ownership* concerns one's right to access one's own information without interference from any unauthorized party (Squicciarini *et al.,* 2011). Only one of the 39 papers discussed the issue of ownership. This paper, P2, Squicciarini *et al.,* (2010), stated that ownership in a SSA refers to the set of users who are owners of a piece of data, regardless of where (i.e., in which user's profile) this piece of data was originally posted. The profile owner is expected to take responsibility for managing access to the posted data content. In other words, data owners must play a role in determining the privacy status of every piece of posted content included in their own information. Ownership dictates that no other user or entity may repudiate or deny the uploading of posts, information or data by the person or user who owns them. It also implies that no other party may claim credit for posts, information or data from their rightful owners. Hence, ownership as a whole addresses the issue of intellectual property breach and non-repudiation. As stated in Constantinos *et al*., (2014), the term 'ownership' should not be considered in terms of property or copyright; rather, it refers to the fundamental right to privacy. Users expect that when they submit their personal photos to an SSA, they will be free to set their own privacy policies, allowing access only to users they choose.
3) *User behaviour* is the attitude required of SSA users to ensure that security in a SSA system is well protected (Li and Chen, 2010; Caverlee *et al*., 2010). Of the 39 selected papers, 10 papers discussed issues related to user behavior. These papers state that individual attitudes may lead to either success or failure in the implementation of security systems. As stated in paper P26 by Vastardis and Yang (2013), user behavior plays a major role in determining the effectiveness and efficiency of security protocols in a SSA. Thus, the importance of user behavior in achieving desired security objectives in a SSA cannot be denied. Moreover, according to P29 by Chen (2013), within the context of an SSA, individual privacy values may affect site members in terms of their attitudes (behavior) towards the networking site. It is clear that user behavior is a crucial element in the success of security implementations.

4) *Security policy* is important to ISS, as they provide the blueprints for the overall security program and create a platform for the implementation of secure practices in an organization (Von Solms and Von Solms, 2004). According to Bulgurcu *et al.* (2010), a security policy is defined as a statement of the roles and responsibilities of employees in safeguarding the information and technology resources of their organization. This factor was the most commonly discussed among those considered in this paper. Of the 39 selected papers, 15 discussed security policy. This finding indicates that security policy is the most important issue to discuss in regards to SSAs. As stated in paper P22 by Hu *et al.,* (2013), for the protection of user data, current online SSAs indirectly require users to be system and policy administrators for the regulation of their own data, as users can restrict their data sharing to a specific set of trusted users. In other words, security policies help SSA users to protect their information in an appropriate and more secure manner.

8. Discussion

Overall, the results of this review present four factors contributing to ISS practices in SSA. Based on the findings, in this study, the results present the relationship between factors contributing to practice ISS in SSA as shown in Table 10. As discussed in Section 7, there are 4 factors that contribute to the implementation of ISS practices in SSA: (1) protection tools, (2) ownership, (3) user behaviour, and (4) security policy. In addition, the researchers found that the factor contributing to SSA that was most widely discussed in the articles considered in this study was the security policy, followed by protection tools, user behaviour and, finally, ownership.

Security policy refers to a set of rules that defines the specific security requirements that must be followed to protect an online SSA system from attack. These rules must be developed before the security system itself is implemented. Without a proper security policy plan, it is impossible to achieve appropriate security to secure a SSA against attack. Once the security policy has been developed, protection tools are then implemented. Thus, these two critical factors are connected. In essence, a protection tool is a practical manifestation of a security policy and requires certain skills and knowledge to be implemented. A protection tool is a critical security factor because it acts as a medium through which to control the system or protect it from harm.

User behaviour refers to users' attitudes or actions towards a system. This factor is critical because the users themselves must take some responsibility for ensuring that their ISS is always as high as possible. Users are also responsible for preventing other parties from accessing their information without permission. Finally, in the use of SSAs, it is clear that human intervention cannot be avoided. Thus, ownership becomes a crucial element, as it further enhances user privacy, thereby allowing users to feel secure in their ability to access their own data in the system.

9. Conclusion

ISS has been shown to play an important role in protecting SSA users from unwanted threats. In this paper, the researchers presented the first SLR of papers published in high-impact journals between 2010 and 2014 in the field of ISS and SSA. The initial search retrieved 1,990 cited papers, of which 39 were ultimately included in this study after passing through five different levels of practical screening. Based on the stated objective, the researchers formulated four RQs; then, data and evidence were systematically extracted from the chosen studies and were finally synthesized to answer the formulated RQs.

The results indicated that ISS in SSAs is an active area of research with an increasing number of publications. Furthermore, this SLR also reveals the ISS and SSAs are areas that still require further attention. Many aspects of ISSs have been covered, and many tools and techniques have been proposed, such as those mentioned in Section 7. This study provides guidelines for assisting researchers in planning future work by analysing the existing evidence for various techniques and also by identifying research areas that need more attention in this field.

In addition, this study can help other researchers to gain an overview of the existing state of ISS in SSA approaches, tools, and empirical evidence and to subsequently identify areas that require further attention from the research community. This paper also offers additional information for security professionals regarding the most common and most sought-after ISS issues and the ways in which they are addressed, specifically for the development of future SSAs.

In future research, more in-depth studies should be conducted to ensure the effectiveness of ISS measures in SSA. It is also good to increase the SLR searching in other search engines, mainly in security and SSA area with new keywords like “cyber security”, “authentication” and “privacy”.

Acknowledgement

The authors would like to acknowledge the support provided by UMRG Programme 2013, University of Malaya (RP004E – 13HNE).

References

Abdulhamid, S.M., Ahmad, S., Waziri, V.O. and Jibril, F.N. (2014), "Privacy and National Security Issues in Social Networks: The Challenges", *International Journal of the Computer, the Internet and Management,* Vol 19 No. 3, pp. 14-20.

Adams, S.A. (2010), "Revisiting the Online Health Information Reliability Debate in the Wake of 'Web 2.0': An Interdisciplinary Literature and Website Review", *International Journal of Medical Informatics,* Vol. 79 No. 6, pp. 391-400.

ALTAMIMI, L. (2013), "A Lexical Analysis of Social Software Literature", *Informatica Economica,* Vol. 17 No. 1, pp. 14-26.

Arapinis, M., Mancini, L.I., Ritter, E. and Ryan, M.D. (2016), "Analysis of Privacy in Mobile Telephony Systems", *International Journal of Information Security,* pp. 1-33.

Asuncion, A.U. and Goodrich, M.T. (2013), "Nonadaptive Mastermind Algorithms for String and Vector Databases, with Case Studies", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 No. 1, pp. 131-144.

Berendt, B. (2012), "More than Modelling and Hiding: Towards a Comprehensive View of Web Mining and Privacy", *Data Mining and Knowledge Discovery,* Vol. 24, pp. 697-737.

Bishop, M. (2004), *Introduction to Computer Security.* 1st ed. Boston: Addison-Wesley Professional.

Bonchi, F., Gionis, A. and Tassa, T. (2014), "Identify Obfuscation in Graphs through the Information Theoretic Lens", *Information Sciences,* Vol. 275, pp. 232-256.

Boyd, D.M.and Ellison, N.B. (2007), "Social Network Sites: Definition, History and Scholarship", *Journal of Computer-Mediated Communications,* Vol. 13 No. 1, pp. 210-230.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information Security Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly,* Vol. 34 No. 3, pp. 523-548.

Carullo, M., Carminati, B., Ferrari, E., Binaghi, E. and Vanetti, M. (2013), "A System to Filter Unwanted Messages from OSN User Walls", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 No. 2, pp. 285-297.

Caverlee, J., Liu, L. and Webb, S. (2010), "The SocialTrust Framework for Trusted Social Information Management: Architecture and Algorithms", *Information Sciences,* Vol. 180, pp. 95-112.

Chakraborty, R., Vishik, C. and Rao, H.R. (2013), "Privacy Preserving Actions of Older Adults on Social Media: Exploring the Behavior of Opting Out of Information Sharing", *Decision Support Systems,* Vol. 55, pp. 948-956.

Chang, S.E. and Ho, C.B. (2006), "Organizational Factors to the Effectiveness of Implementing Information Security Management", *Industrial Management & Data Systems,* Vol. 106 No. 3, pp. 345-361.

Chard, K., Bubendorfer, K., Caton, S. and Rana, O.F. (2012), "Social Cloud Computing: A Vision for Socially Motivated Resource Sharing", *IEEE Transactions on Service Computing,* Vol. 5 No. 4, pp. 551-563.

Chen, R. (2013), "Living a Private Life in Public Social Networks: An Exploration of Member Self-Disclosure. *Decision Support Systems,* Vol. 55, pp. 661-668.

Cho, J.-H., Swami, A. and Chen, I.-R. (2011), "A Survey on Trust Management for Mobile Ad Hoc Networks", *IEEE Communications Surveys & Tutorials,* Vol. 13 No. 4, pp. 562-583.

Cleveland, F.M. (2008), "Cyber Security Issues for Advanced Metering Infrastructure (AMI)", *IEEE PES Power System Communications Committee,* pp. 1-5.

ComScore, 2015. *ComScore.* [Online] Available at: http://www.comscoredatamine.com/ [Accessed 2 February 2015].

Constantinos, P., Athanasios, Z., Achilleas, P. and Edgar, G.-L. (2014), "Distributing Privacy Policies Over Multimedia Content Across Multiple Online Social Networks", *Computer Networks,* Vol. 75(B), pp. 531-543.

Dogan, S., Betin-Can, A. and Garousi, V. (2014), "Web Application Testing: A Systematic Literature Review", *The Journal of Systems and Software,* Vol. 91, pp. 174-201.

Dwivedi, M., Shibu, T.P. and Venkatesh, U. (2007), "Social Software Practices on the Internet: Implications for the Hotel Industry", *International Journal of Contemporary Hospitality Management,* Vol. 19 No. 5, pp. 415-426.

Dyba, T., Dingsoyr, T. and Hanssen, G.K. (2007), *Applying Systematic Reviews in Software Engineering,* s.l.: EBSE Technical Report.

eMarketer, 2013. *eMarketer.* [Online] Available at: http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976 [Accessed 12 December 2015].

Fink, A. (2005), *Conducting Research Literature Reviews: From the Internet to Paper.* 2nd ed. California: Sage Publications.

Fleeger, P. and Charles, P. (1989), *Security in Computing.* s.l.:Prentice-Hall.

Fung, B.C.M., Trojer, T., Hung, P.C.K.., Al-Hussaeni, K. and Dssouli, R. (2012), "Service-oriented Architecture for High-Dimensional Private Data Mashup", *IEEE Transactions on Service Computing,* Vol. 5 No. 3, pp. 373-386.

Gao, H., Barbier, G. and Goolsby, R. (2011), "Harnessing the Crowdsourcing Power of Social Media for Disaster Relief", *IEEE Intelligent Systems,* Vol. 26 No. 3, pp. 10-14.

George, A., 2006. *New Scientist.* [Online] Available at: https://www.newscientist.com/article/mg19125691.700-living-online-the-end-of-privacy/ [Accessed 1 December 2014].

Grahl, J. (2014), "The Professors and the Banks: US Views on the Subprime Crisis", *International Review of Applied Economics, Taylor & Francis Journals,* Vol. 28 No. 3, pp. 383-400.

Gritzalis, D., Kandias, M., Stavrou, V. and Mitrou, L. (2014), *History of Information: The Case of Privacy and Security in Social Media.* s.l., In. Proc. of the History of Information Conference.

Gross, R. and Acquisti, A. (2005), *Information Revelation and Privacy in Online Social Networks.* Alexandria, Virginia, USA, ACM Workshop on Privacy in the Electronic Society (WPES), pp. 71-80.

Hajli, N. and Lin, X. (2014), "Exploring the security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information", *Journal of Business Ethics,* Vol. 133, No. 1, pp. 1-13.

Harris, S., 2007. *CISSP: All-in-one Exam Guide.* s.l.:McGraw-Hill Osborne Media.

Haughn, M. & Gibilisco, S., 2014. *WhatIs.com.* [Online] Available at: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed 28 December 2014].

Hay, M., Miklau, G., Jensen, D., Towsley, D. and Li, C. (2010), "Resisting Structural Re-Identification in Anonymized Social Networks", *The VLDB Journal,* Vol. 19, pp. 797-823.

Heatherly, R., Kantarcioglu, M. and Thuraisingham, B. (2013), "Preventing Private Information Inference Attacks on Social Networks", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 No. 8, pp. 1849-1862.

HillAssociates, 2007. *Hill Associates.* [Online] Available at: http://www.hill2dot0.com/wiki/index.php?title=CIA_triad [Accessed 15 November 2014].

Hu, H., Ahn, G.-J. and Jorgensen, J. (2013), "Multiparty Access Control for Online Social Networks: Model and Mechanisms", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 No. 7, pp. 1614-1627.

Inagaki, T., Nakahashi, Y., Yabuuchi, T. and Tanaka, H. (2012), "Consideration of Competencies of the Future Learners from a Review of 'Web 2.0' Literature", *International Journal,* Vol. 6 No.1, pp. 61-68.

ISO/IEC. (2005), *Information Technology - Security Techniques: Code of Practise for Information Security Management.* [Online] Available at: http://www.iso.org/iso/en/ prods services/popstds/informationsecurity.html [Accessed 18 November 2014].

ISO/IEC. (2014), *Information Security: Terms and Definition.* s.l.:Praxiom Research Group Limited.

Jasco, P. (2009), "Calculating the H-Index and Other Bibliometric and Scientometric Indicators from Google Scholars with the Publish or Perish Software. *Emerald Insight,* Vol. 33 No. 6, pp. 1189-1200.

Keele, S. (2007), *Guidelines for Performing Systematic Literature Review in Software Engineering,* UK: EBSE Technical Report.

Khan, W.Z., Xiang, Y., Aalsalem, M. and Arshad, Q. (2013), "Mobile Phone Sensing Systems: A Survey", *IEEE Communications Surveys & Tutorials,* Vol. 15 No. 1, pp. 402-427.

Kitchenham, B. Brereton, O.P., Budgen, D., Turner, M., Bailey, J. and Linkman, S. (2009), "Systematic Literature Review in Software Engineering – A systematic literature review." *Information and Software Technology,* Vol. 51 No. 1, pp. 7-15.

Kitchenham, B. and Charters, S. (2007), "Guidelines for Performing Systematic Literature Reviews in Software Engineering", *Evidence-Based Software Engineering.*

Ku, Y.-C., Chen, R. and Zhang, H. (2013), "Why Do Users Continue Using Social Networking Sites? An Exploratory Study of Members in the United States and Taiwan", *Information & Management,* Vol. 50, pp. 571-581.

Lee, B., Fan, W., Squicciarini, A.C., Ge, S. and Huang, Y. (2014), "The Relativity of Privacy Preservation Based on Social Tagging", *Information Sciences,* Vol. 288, pp. 87-107.

Leidner, D.E. and Kayworth, T. (2006), "A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict", *MIS Quarterly,* Vol. 30 No. 2, pp. 357-399.

Lenhart, A. and Madden, M. (2007), *PewResearch Center.* [Online] Available at: http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/ [Accessed 25 January 2015].

Leonardi, P.M., Huysman, M. and Steinfiled, C. (2013), "Enterprise Social Media: Definition, History, and Prospects for the Study of Social Technologies in Organizations", *Journal of Computer-Mediated Communication,* Vol. 19 No. 1, pp. 1-19.

Liang, X., Zhang, K., Shen, X. and Lin, X. (2014), "Security and Privacy in Mobile Social Networks: Challenges and Solutions", *IEEE Wireless Communications,* Vol. 21 No. 1, pp. 33-41.

Li, N. and Chen, G. (2010), "Sharing Locations in Online Social Networks", *IEEE Network,* Vol. 24 No. 5, pp. 20-25.

Liu, G., Wang, Y., Orgun, M.A. and Lim, E.-P. (2013), "Finding the Optimal Social Trust Path for the Selection of Trustworthy Service Providers in Complex Social Networks", *IEEE Transactions on Service Computing,* Vol. 6 No. 2, pp. 152-167.

Luo, W., Liu, J., Liu, J. and Fan, C. (2009), "An Analysis of Security in Social Networks", *IEEE International Conference on Dependable, Autonomic and Secure Computing,* pp. 648 - 651.

Makridakis, A. Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S. and Markatos, E.P. (2010), "Understanding the Behaviour of Malicious Applications in Social Networks", *IEEE Network,* Vol. 24 No. 5, pp. 14-19.

Mascetti, S., Freni, D., Bettini, C., Wang, X.S. and Jajodia, S. (2011), "Privacy in Geo-Social Networks: Proximity Nortification with Untrusted Service Providers and Curious Buddies", *The VLDB Journal,* Vol. 20, pp. 541-566.

Okoli, C. and Schabram, K. (2010), "A Guide to Conducting a Systematic Literature Review of Information Systems Research", *Association of Information Systems.*

Paganini, P. (2015), *Infosec Institute.* [Online] Available at: http://resources.infosecinstitute.com/phishing-dangerous-cyber-threat/ [Accessed 5 January 2015].

PandaLabs. (2012), *2012 Annual Report PandaLabs.* [Online] Available at: http://press.pandasecurity.com/wp-content/uploads/2013/02/PandaLabs-Annual-Report-2012.pdf. [Accessed 23 December 2014].

PandaLabs. (2013), *PandaLabs Quarterly Report January - March 2013.* [Online] Available at: http://press.pandasecurity.com/wp content/uploads/2010/05/PandaLabsQuaterly-Report. Pdf [Accessed 23 December 2014].

Park, H.-S., Huh, S.-Y., Oh, W. and Han, S.P. (2012), "A Social Network-Based Inference Model for Validating Customer Profile Data", *MIS Quarterly,* Vol. 36 No. 4, pp. 1217-1237.

Parris, I., Ben, A.F. and Henderson, T. (2014), "Facebook or Fakebook? The Effects of Simulated Mobile Applications on Simulated Mobile Networks", *Ad Hoc Networks,* Vol. 12, pp. 35-49.

Peltier, T. (2001), Information Security Risk Analysis. In: USA: Auerbach Publications, pp. 308 - 313.

Petticrew, M. and Roberts, H. (2006), *Systematic Reviews in the Social Sciences: A Practical Guide.* s.l.:Blackwell Publications.

Poor, H.V. (2012), "Information and Inference in the Wireless Physical Layer", *IEEE Wireless Communications,* Vol. 19 No. 1, pp. 40-47.

Puttaswamy, K..P.N., Wang, S., Steinbauer, T., Agrawal, D., El-Abbadi, A., Kruegel, C. and Zhao, B.Y. (2014), "Preserving Location Privacy in Geosocial Applications", *IEEE Transactions on Mobile Computing,* Vol. 13 No. 1, pp. 159-173.

Reuters, T., 2012. *Web of Knowledge.* [Online] Available at: http://admin-apps.webofknowledge.com/JCR/help/h_impfact.htm [Accessed 7 March 2015].

Reuters, T., 2014. *Thomson Reuters.* [Online] Available at: http://thomsonreuters.com/en/products-services/scholarly-scientific-research/research-management-and-evaluation/journal-citation-reports.html [Accessed 15 1 2015].

Sanchez, A.J. and Demazeau, Y. (2014), "The Age of Confidentiality: A Review of the Security in Social Networks and Internet Distributed Computing and Artificial Intelligence", *11th International Conference Advances in Intelligent Systems and Computing,* Vol. 290, pp. 407-415.

Schall, D., Skopik, F. and Dustdar, S. (2012), "Expert Discovery and Interactions in Mixed Service-Oriented Systems", *IEEE Transactions on Service Computing,* Vol. 5 No. 2, pp. 233-245.

Secker, J. (2008), *Social Software, Libraries and Distance Learners: Literature Review.* [Online] Available at: http://eprints.lse.ac.uk/4058/1/LASSIE_lit_review%28LSERO%29.pdf

SGPPWritingCenter. (2009), *Literature Reviews: Using a Matrix to Organize Research.* [Online] Available at: http://www2.smumn.edu/deptpages/tcwritingcenter/forms_of_writing/litrevmatrix_tc.pdf [Accessed 5 October 2014].

Shailey, M. (2009), "Role of Social Software Tools in Education: A Literature Review", *Education + Training,* Vol. 51 No. 5/6, pp. 353-369.

Smith, E. and Eloff, J.H.P. (1999), "Security in Health-care Information Systems - Current Trends", *International Journal of Medical Informatics,* Vol. 54 No. 1, pp. 39-54.

Smith, L. (1981), "Citation Analysis", *Library Trends,* Vol. 30, pp. 83-106.

Squicciarini, A.C., Shehab, M. and Wede, J. (2010), "Privacy Policies for Shared Content in Social Network Sites. *The VLDB Journal,* Vol. 19, pp. 777-796.

Squicciarini, A.C., Xu, H. and Zhang, X. (2011), "CoPE: Enabling Collaborative Privacy Management in Online Social Networks. *Journal of the American Society for Information Science and Technology,* Vol. 62 No. 3, pp. 52 -534.

Sterne, J.A. C., Egger, M. and Smith, G.D. (2001), "Investigating and Dealing with Publications and Other Biases in Meta-analysis", *British Medical Association,* Vol. 323 No. 7324, pp. 101-105.

Tai, C.-H., Yu, P.S., Yang, D.-N. and Chen, M.-S. (2014), "Structural Diversity for Resisting Community Identification in Published Social Networks", *IEEE Transaction on Knowledge and Data Engineering,* Vol. 26 No. 1, pp. 235-252.

Tassa, T. and Cohen, D.J. (2013), "Anonymization of Centralized and Distributed Social Networks by Sequential Clustering", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 25 No. 2, pp. 311-324.

Thompson, D.F. (1991), "Citation analysis of selected clinical pharmacology journals", *Hospital Pharmacy,* Vol. 26, pp. 437-439.

Tseng, C.-Y., Sung, P.-C. and Chen, M.S. (2011), "Cosedes: A Collaborative Spam Detection System with a Novel E-mail Abstraction Scheme.", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 23 No. 5, pp. 669-682.

Vastardis, N. and Yang, K. (2013), "Mobile Social Networks: Architectures, Social Properties, and Key Research Challenges", *IEEE Communications Surveys & Tutorials,* Vol. 15 No. 3, pp. 1355-1371.

Von Solms, R. and Von Solms, B. (2004), "From Policies to Culture", *Computer & Security,* Vol. 23, pp. 275-279.

Wang, Y., Xie, L., Zheng, B. and Lee, K.C.K (2014), "High Utility K-Anonymization for Social Network Publishing", *Knowledge and Information Systems,* Vol. 41, pp. 697-725.

Water, R.D., Burnett, E., Lamm, A. and Lucas, J. (2009), "Engaging Stakeholders through Social Networking: How Nonprofit Organizations are Using Facebook", *Public Relations Review,* Vol. 35, pp. 102-106.

Wikipedia, 2015. *Wikipedia, the Free Encyclopedia.* [Online] Available at: https://en.wikipedia.org/wiki/Citation_analysis [Accessed 17 March 2015].

Wilson, D.W., Lin, X., Longstreet, P. and Sarker, S. (2011), *Web 2.0: A Definition, Literature Review, and Directions for Future Research.* s.l., AMCIS 2011 Proceedings Paper 368.

Wyatt, D., Choudhury, T., Bilmes, J. and Kitts, J.A. (2011), "Inferring Colocation and Conversation Networks from Privacy-Sensitive Audio with Implications for Computational Social Science", *ACM Transactions on Intelligent Systems and Technology,* Vol. 2, No. 1, pp. 1-41.

Ying, X. and Wu, X. (2011), "On Link Privacy in Randomizing Social Networks", *Knowledge and Information Systems,* Vol. 28, pp. 645-663.

Yuan, M., Chen, L., Yu, P.S. and Yu, T. (2013), "Protecting Sensitive Labels in Social Network Data Anonymization." *IEEE Transaction on Knowledge and Data Engineering,* Vol. 25 No. 3, pp. 633-647.

Zhang, C., Sun, J., Zhu, X. and Fang, Y. (2010), "Privacy and Security for Online Social Networks: Challenges and Opportunities", *IEEE Network,* Vol. 24 No. 4, pp. 13-18.

Zhou, B. and Pei, J. (2011), "The K-Anonymity and I-Diversity Approaches for Privacy Preservation in Social Networks against Neighbourhood Attacks", *Knowledge and Information Systems,* Vol. 28, pp. 47-77.

Zhou, J., Cao, Z., Dong, X., Lin, X. and Vasilakos, A.V. (2013), "Securing M-Healthcare Social Networks: Challenges, Countermeasures and Future Directions", *IEEE Wireless Communications,* Vol. 20 No. 4, pp. 12-21.

Zyl, A.S. v. (2009), "The Impact of Social Networking 2.0 on Organisations", *The Electronic Library,* Vol. 27 No. 6, pp. 906-918.

Figures

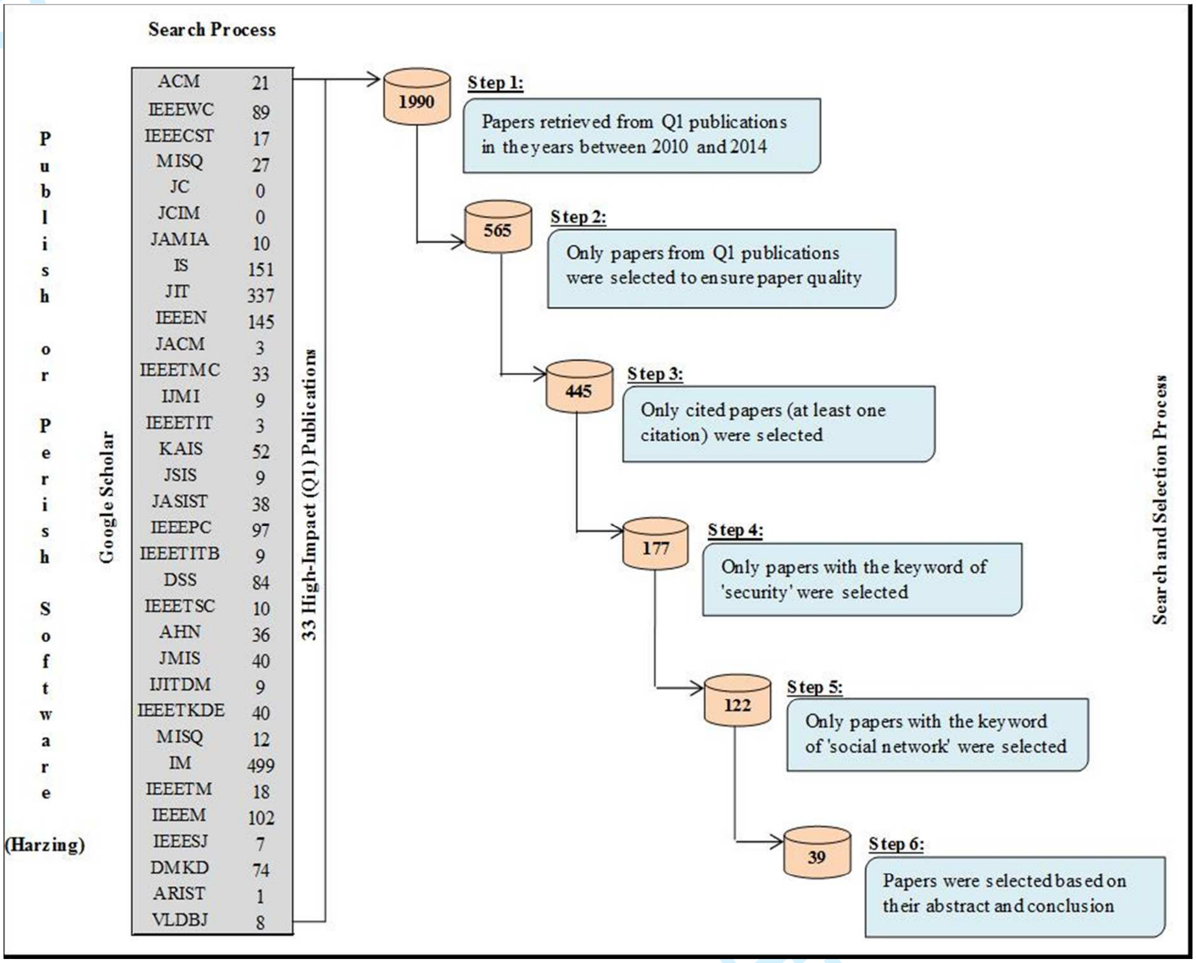
Search Process
Publish or Perish Software (Harzing)
Google Scholar
ACM 21
IEEEWC 89
IEEECST 17
MISQ 27
JC 0
JCIM 0
JAMIA 10
IS 151
JIT 337
IEEEN 145
JACM 3
IEEETMC 33
IJMI 9
IEEETIT 3
KAIS 52
JSIS 9
JASIST 38
IEEEPC 97
IEEETITB 9
DSS 84
IEEETSC 10
AHN 36
JMIS 40
IJITDM 9
IEEETKDE 40
MISQ 12
IM 499
IEEETM 18
IEEEM 102
IEEESJ 7
DMKD 74
ARIST 1
VLDBJ 8
33 High-Impact (Q1) Publications
1990
Step 1:
Papers retrieved from Q1 publications in the years between 2010 and 2014
565
Step 2:
Only papers from Q1 publications were selected to ensure paper quality
445
Step 3:
Only cited papers (at least one citation) were selected
177
Step 4:
Only papers with the keyword of 'security' were selected
122
Step 5:
Only papers with the keyword of 'social network' were selected
39
Step 6:
Papers were selected based on their abstract and conclusion
Search and Selection Process

Figure I. Systematic Literature Review (SLR) Execution Process

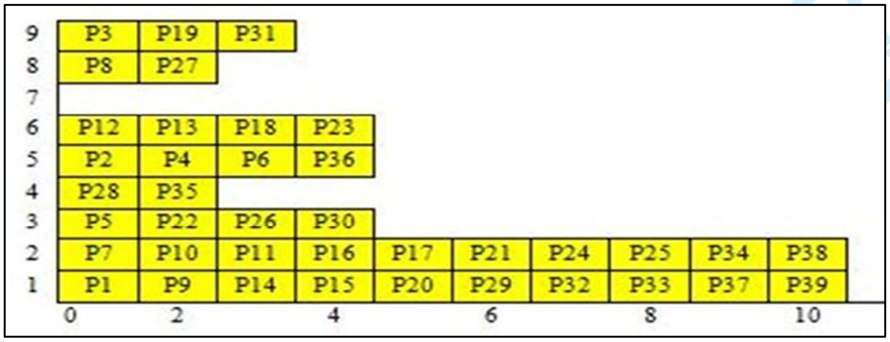

Figure II. Citation counts for the studies retrieved and selected from Google Scholar (as of 17th December 2014)

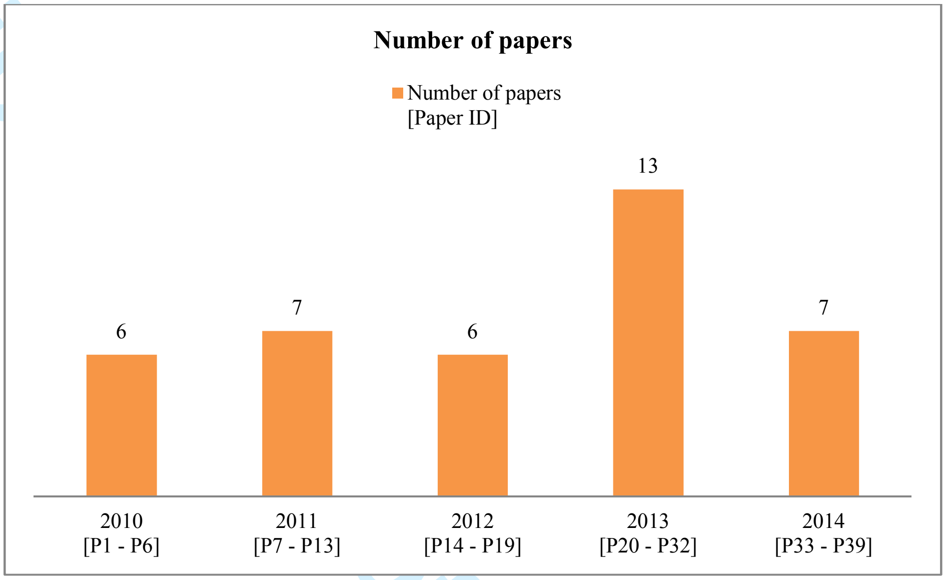

Figure III. Summary of the chronological characteristics of the reviewed studies

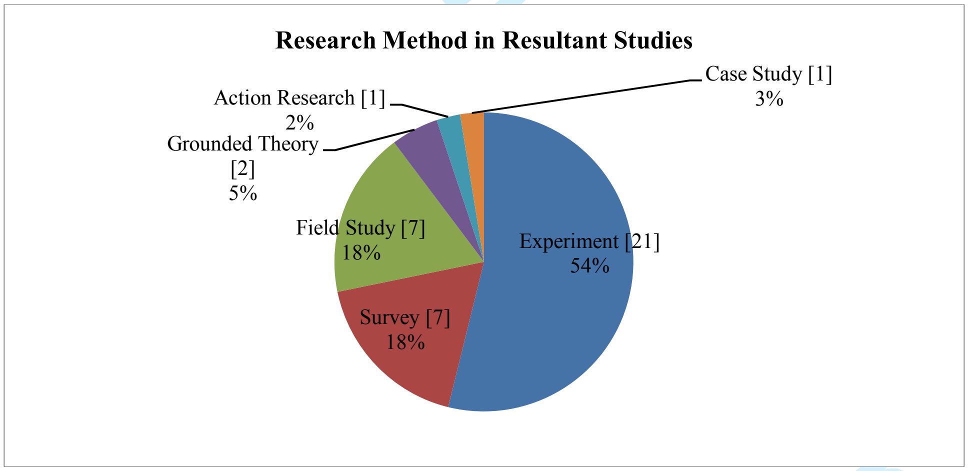

Figure IV. Research methods used in the reviewed studies

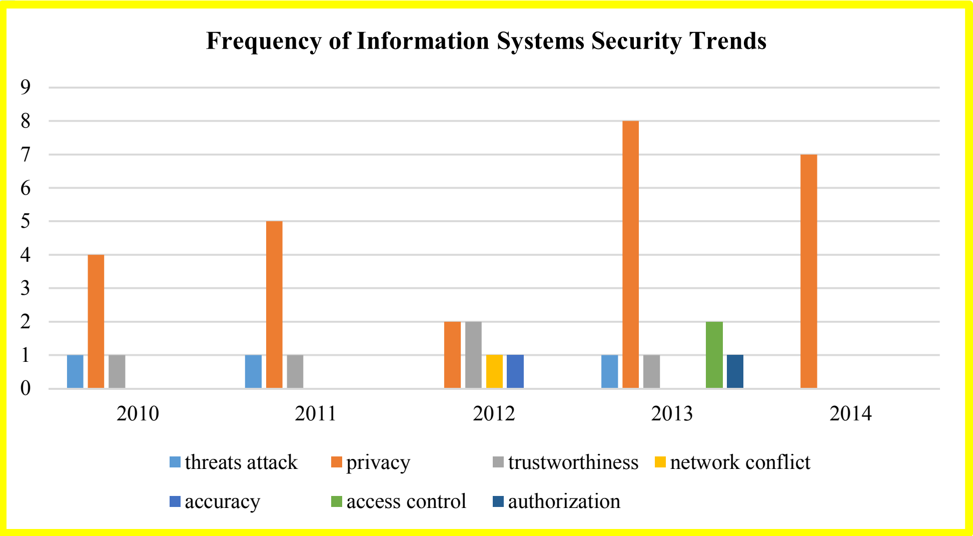

Figure V. Frequency of Information Systems Security Trends

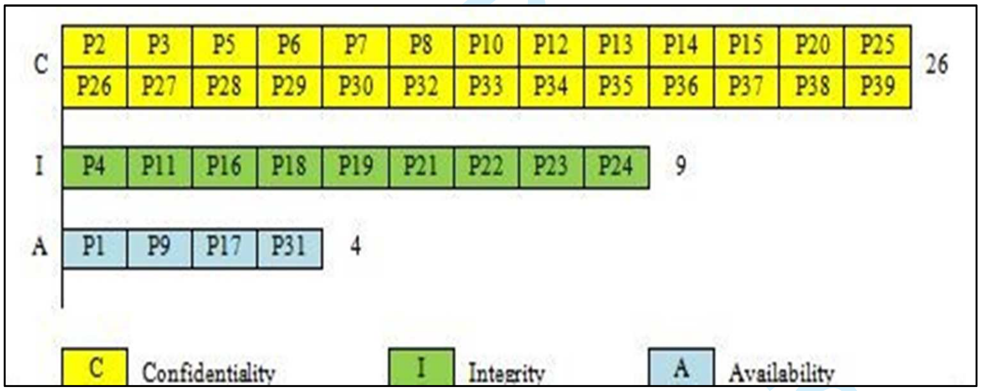

Figure VI. The motivations for social network users to practice security management

Tables

Reference	Period	No. of articles	Type of sources	Databases	Keywords	Focus area
(Dwivedi, et al., 2007)	N/A	N/A	Journals, Periodicals, Blogs, Message-Boards & Consumer Review Sites.	N/A	N/A	Hotel industry
(Secker, 2008)	Up until 2007	N/A	N/A	LISA, LISTA & ERIC	N/A	Library Community
(Shailey, 2009)	Up until 2009	N/A	N/A	N/A	N/A	Education
(Zyl, 2009)	N/A	N/A	Journal Articles, White Papers, Popular Media & Books	N/A	N/A	Electronic Social Networking in Organizations
(Adams, 2010)	2006-2008	56 + 6 Blogs + 1 Wiki	Journals, Conference Proceedings, Trade Publications & Book Series + Blogs + Wiki	Scopus, Elsevier PubMed & Google Scholar	"Web 2.0," "Web Log," "Weblog" "Blog" Singularly & In Combination With Patient, Health & Medicine. "Second Generation Web," "Wiki" "Health 2.0," "Medicine 2.0"	Online Health
(Wilson, et al., 2011)	N/A	114 Articles	Academic, Crossover (Outlets at Intersection between Academia & Practice), & Practitioner	EBSCO Business Source Complete And ABI/INFORM Proquest	Variants of "Blog" Or "Wiki", "Social Bookmarking" or "Social Computing" , "Facebook" or "YouTube"	Information Systems (IS)
(Inagaki, et al., 2012)	2006-2010	181 Articles	International Journals	EBSCO, Pro Quest & Google Scholar	Web 2.0, Learning And E-Learning	Education
(Zyl, 2009)	N/A	N/A	Journal Articles, White Papers, Popular Media & Books	N/A	N/A	Electronic Social Networking in Organizations

Table I. Summary of Social Software Literature Reviews (ALTAMIMI, 2013)

P1 Makridakis, A., Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S., Markatos, E.P.: Understanding the Behavior of Malicious Applications in Social Networks. IEEE Network. Pp. 14 – 19 (2010)

P2 Squicciarini, A.C., Shehab, M., Wede, J.: Privacy Policies for Shared Content in Social Network Sites. The VLDB Journal. 19: 777 – 796 (2010)

P3 Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and Security for Online Social Networks: Challenges and Opportunities. IEEE Network. Pp. 13 – 18 (2010)

P4 Caverlee, J., Liu, L., Webb, S.: The SocialTrust Framework for Trusted Social Information Management: Architecture and Algorithms. Information Sciences. 180: 95 – 112 (2010)

P5 Hay, M., Miklau, G., Jensen, D., Towsley, D., Li, C.: Resisting Structural Re-Identification in Anonymized Social Networks. The VLDB Journal. 19: 797 – 823 (2010)

P6 Li, N., Chen, G.: Sharing Location in Online Social Networks. IEEE Network. Pop 20 – 25 (2010)

P7 Squicciarini, A.C., Xu, H., Zhang, X. (L.): CoPE: Enabling Collaborative Privacy Management in Online Social Networks. Journal of the American Society for Information Science and Technology. Vol. 62, No. 3, pp. 521 – 534 (2011)

P8 Zhou, B., Pei, J.: The K-Anonymity and I-Diversity Approaches for Privacy Preservation in Social Networks against Neighborhood Attacks. Knowledge and Information Systems. 28: 47 – 77 (2011)

P9 Tseng, C.-Y., Sung, P.-C., Chen, M.-S.: Cosdes: A Collaborative Spam Detection System with a Novel E-mail Abstraction Scheme. IEEE Transactions on Knowledge and Data Engineering. Vol. 23, No. 5, pp. 669 – 682 (2011)

P10 Wyatt, D., Choudhury, T., Bilmes, J., Kitts, J. A.: Inferring Colocation and Conversation Networks from Privacy-Sensitive Audio with Implications for Computational Social Science. ACM Transactions on Intelligent Systems and Technology. Vol. 2, No. 1 (2011)

P11 Cho, J.-H., Swami, A., Chen, I.-R.: A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE Communications Surveys & Tutorials. Vol. 13, No. 4, pp. 562 – 583 (2011)

P12 Mascetti, S., Freni, D., Bettini, C., Wang, X.S., Jajodia, S.: Privacy in Geo-Social Networks: Proximity Notification with Untrusted Service Providers and Curious Buddies. The VLDB Journal. 20: 541 – 566 (2011)

P13 Ying, X., Wu, X.: On Link Privacy in Randomizing Social Networks. Knowledge and Information Systems. 28: 645 – 663 (2011)

P14 Fung, B.C.M., Trojer, T., Hung, P.C.K., Xiong, L., Al-Hussaeni, K., Dssouli, R.: Service-Oriented Architecture for High-Dimensional Private Data Mashup. IEEE Transactions on Services Computing. Vol. 5, No. 3, pp. 373 – 386 (2012)

P15 Berendt, B.: More than Modelling and Hiding: Towards a Comprehensive View of Web Mining and Privacy. Data Mining and Knowledge Discovery. 24: 697 – 737 (2012)

P16 Schall, D., Skopik, F., Dustdar, S.: Expert Discovery and Interactions in Mixed Service-Oriented Systems. IEEE Transactions on Services Computing. Vol., 5, No. 2, pp. 233 – 245 (2012)

P17 Poor, H. V.: Information and Inference in the Wireless Physical Layer. IEEE Wireless Communications. Pp. 40 – 47 (2012)

P18 Chard, K., Bubendorfer, K., Caton, S., Rana, O.F.: Social Cloud Computing: A Vision for Socially Motivated Resource Sharing. IEEE Transactions on Services Computing. Vol., 5, No. 4, pp. 551 – 563 (2012)

P19 Park, H.-S., Huh, S.-Y., Oh, W., Han, S.P.: A Social Network-Based Inference Model for Validating Customer Profile Data[1]. MIS Quarterly. Vol., 36, No. 4, pp. 1217 – 1237 (2012)

P20 Asuncion, A.U., Goodrich, M.T.: Nonadaptive Mastermind Algorithms for String and Vector Databases, with Case Studies. IEEE Transactions on Knowledge and Data Engineering. Vol., 25, No. 1. Pp 131 – 144 (2013)

P21 Liu, G., Wang, Y., Orgun, M.A., Lim, E.-P.: Finding the Optimal Social Trust Path for the Selection of Trustworthy Service Providers in Complex Social Networks. IEEE Transactions on Services Computing. Vol., 6, No. 2. Pp. 152 – 167 (2013)

P22 Hu, H., Ahn, G.-J., Jorgensen, J.: Multiparty Access Control for Online Social Networks: Model and Mechanisms. IEEE Transactions on Knowledge and Data Engineering. Vol., 25, No. 7. Pp. 1614 – 1627 (2013)

P23 Zhou, J., Cao, Z., Dong, X., Lin, X., Vasilakos, A.V.: Securing M-Healthcare Social Networks: Challenges, Countermeasures, and Future Directions. IEEE Wireless Communications. Pp. 12 – 21 (2013)

P24 Vanetti, M., Binaghi, E., Ferrari, E., Carminati, B., Carullo, M.: A System to Filter Unwanted Messages from OSN User Walls. IEEE Transactions on Knowledge and Data Engineering. Vol., 25, No. 2. Pp. 285 – 297 (2013)

P25 Yuan, M., Chen, L., Yu, P.S., Yu, T.: Protecting Sensitive Labels in Social Network Data Anonymization. IEEE Transactions on Knowledge and Data Engineering. Vol., 25, No. 3. Pp. 633 – 647 (2013)

P26 Vastardis, N., Yang, K.: Mobile Social Networks: Architectures, Social Properties, and Key Research Challenges. IEEE Communications Surveys &Tutorials. Vol., 15, No. 3. Pp. 1355 – 1371 (2013)

P27 Chakraborty, R., Vishik, C., Rao, H.R.: Privacy Preserving Actions of Older Adults on Social Media: Exploring the Behavior of Opting Out of Information Sharing. Decision Support Systems. 55: 948 – 956 (2013)

P28	Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Preventing Private Information Inference Attacks on Social Networks. Vol., 25, No. 8. Pp. 1849 – 1862 (2013)
P29	Chen, R.: Living a Private Life in Public Social Networks: An Exploration of Member Self-disclosure. Decision Support Systems. 55: 661 – 668 (2013)
P30	Tassa, T., Cohen, D.J.: Anonymization of Centralized and Distributed Social Networks by Sequential Clustering. IEEE Transactions on Knowledge and Data Engineering. Vol., 25, No, 2. Pp. 311 – 324 (2013)
P31	Khan, W.Z., Xiang, Y., Aalsalem, M., Arshad, Q.: Mobile Phone Sensing Systems: A Survey. IEEE Communications Surveys & Tutorials. Vol. 15, No. 1, pp. 402 – 427 (2013)
P32	Ku, Y.-C., Chen, R., Zhang, H.: Why Do Users Continue Using Social Networking Sites? An Exploratory Study of Members in the United States and Taiwan. Information & Management. 50: 571 – 581 (2013)
P33	Lee, B., Fan, W, Squicciarini, A.C., Ge, S., Huang, Y.: The Relativity of Privacy Preservation Based on Social Tagging. Information Sciences. 288: 87 – 107 (2014)
P34	Tai, C.-H., Yu, P.S., Yang, D.-N., Chen, M.-S.: Structural Diversity for Resisting Community Identification in Published Social Networks. IEEE Transactions on Knowledge and Data Engineering. Vol. 26, No. 1. Pp. 235 – 252 (2014)
P35	Bonchi, F., Gionis, A., Tassa, T.: Identify Obfuscation in Graphs through the Information Theoretic Lens. Information Sciences. 275: 232 – 256 (2014)
P36	Parris, I., Ben Abdesslem, F., Henderson, T.: Facebook or Fakebook? The Effects of Simulated Mobile Applications on Simulated Mobile Networks. Ad Hoc Networks. 12: 35 – 49 (2014)
P37	Puttaswamy, K.P.N., Wang, S., Steinbauer, T., Agrawal, D., El Abbadi, A., Kruegel, C., Zhao B.Y.: Preserving Location Privacy in Geosocial Applications. IEEE Transactions on Mobile Computing. Vol. 13. No. 1. Pp. 159 – 173 (2014)
P38	Liang, X., Zhang, K., Shen, X., Lin, X.: Security and Privacy in Mobile Social Networks: Challenges and Solutions. IEEE Wireless Communications. Pp. 33 – 41 (2014)
P39	Wang, Y., Xie, L., Zheng, B., Lee, K.C.K.: High Utility K-Anonymization for Social Network Publishing. Knowledge and Information Systems. 41: 697 – 725 (2014)

Table II. Selected empirical studies

ID	Complete reference	Citation count
P3	Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and Security for Online Social Networks: Challenges and Opportunities. IEEE Network. Pp. 13 – 18 (2010)	9
P19	Park, H.-S., Huh, S.-Y., Oh, W., Han, S.P.: A Social Network-Based Inference Model for Validating Customer Profile Data1. MIS Quarterly. Vol., 36, No. 4, pp. 1217 – 1237 (2012)	9
P31	Khan, W.Z., Xiang, Y., Aalsalem, M., Arshad, Q.: Mobile Phone Sensing Systems: A Survey. IEEE Communications Surveys & Tutorials. Vol. 15, No. 1, pp. 402 – 427 (2013)	9
P8	Zhou, B., Pei, J.: The K-Anonymity and I-Diversity Approaches for Privacy Preservation in Social Networks against Neighborhood Attacks. Knowledge and Information Systems. 28: 47 – 77 (2011)	8
P27	Chakraborty, R., Vishik, C., Rao, H.R.: Privacy Preserving Actions of Older Adults on Social Media: Exploring the Behavior of Opting Out of Information Sharing. Decision Support Systems. 55: 948 – 956 (2013)	8

Table III. Top 5 most highly cited studies among the results, with 8 and 9 citations on Google Scholar (as of 17th December 2014)

No	Name of Journal	Paper	Impact factor	Citation counter
1	ACM Transactions on Intelligent Systems and Technology	P10	9.390	1028
2	IEEE Wireless Communications	P17, P23, P38	6.524	2910
3	IEEE Communications Surveys and Tutorials	P11, P26, P31	6.490	2002
4	MIS Quarterly	P19	5.405	8705
5	Information Sciences	P4, P33, P35	3.893	12028
6	IEEE Network	P1, P3, P6	3.720	1500
7	IEEE Transactions on Mobile Computing	P37	2.912	3801
8	Knowledge and Information Systems	P8, P13, P39	2.639	1436
9	Journal of the American Society for Information Science and Technology	P7	2.230	5125
10	Decision Support Systems	P27, P29	2.036	4196
11	IEEE Transactions on Services Computing	P14, P16, P18, P21	1.985	337
12	Ad Hoc Networks	P36	1.943	1812
13	IEEE Transactions on Knowledge and Data Engineering	P9, P20, P22, P24, P25, P28, P30, P34	1.815	4642
14	Information & Management	P32	1.788	3384
15	Data Mining and Knowledge Discovery	P15	1.743	1717
16	VLDB Journal	P2, P5, P12	1.701	1513

Table IV. The publications represented by the articles selected for the SLR

Current trend	Description	Studies from which the trend was extracted	Freq. (N = 39)
Threat of attack	Social network users regard attack threats as representing the potential for a harmful event that may destroy or damage a social network system	P1, P9, P31	3
Privacy	Social network users regard privacy as a very important issue in a social network security system to ensure that their confidential information is protected from third-party access	P2, P3, P5, P6, P7, P8, P10, P12, P13, P14, P15, P20, P25, P26, P27, P28, P29, P30, P32, P33, P34, P35, P36, P37, P38, P39	26
Trustworthiness	Social network users regard trustworthiness as a measure of their confidence in the dependability and reliability of a platform for accessing a social network	P4, P11, P16, P18, P21	5
Network conflict	Social network users regard network conflict as a source of difficulties that may lead to problems on a social network	P17	1
Accuracy	Social network users conceptualize accuracy as the quality of being correct or precise on a social network	P19	1
Access control	Social network users regard to access control as a suite of security features that limit who can access information on a social network	P22, P24	2
Authorization	Social network users regard authorization as a permission system for access to a social network	P23	1

Table V. The current trends in information security in social networking.

Confidentiality (C)	Integrity (I)	Availability (A)
Privacy (26)	Accuracy (1)	Threat of attack (3)
	Trustworthiness (5)	Network conflict (1)
	Access control (2)	
	Authorization (1)	

Table VI. Security trends as categorized into the CIA triad

Paper ID	Discussion
P2	People are concerned about privacy.
P3	Confidentiality or privacy is of paramount importance in online social networks (OSNs) because the illegal disclosure and improper use of users' private information can cause undesirable or damaging consequences.
P5	Maintaining privacy when publishing a network dataset is uniquely challenging because an individual's network context can be used to identify that individual even if other identifying information is removed.
P6	Sharing user information in SSAs (the original article referred to OSNs) naturally raises privacy concerns.
P7	In the context of social networking, privacy control is a concern for users whose presence is widely distributed over a large social network and who may have complicated and heterogeneous social relationships.
P8	Preserving privacy in the publishing of social network data is an important concern.
P10	When collecting situated conversation data, it is necessary to protect the privacy of not just those who willingly consent to wear a recording device but also those who may come within range of the microphones.
P12	Although proximity services are very attractive for many social network users, the repeated release of information concerning a user's location at any given time raises severe privacy concerns.
P13	The privacy concerns associated with data analysis over social networks have motivated several recent research studies.
P14	Many agencies and companies believe that privacy protection means simply removing explicit identifying information from released data, such as names, Social Security numbers, addresses, and telephone numbers.
P15	Over the last decade, privacy has been widely recognized as one of the major problems regarding data collection, particularly on the Web and in social networking
P20	Privacy concerns also exist regarding online social networks and other databases that store user preferences in vector form.
P25	Privacy is one of the major concerns involved in the publication or sharing of social network data for social science research and business analysis.
P26	The heuristic approach raises privacy concerns because users' personal contact information is required to be uploaded to service providers.
P27	In addition to fraud, privacy breaches and leaks also pose major issues for social media websites.
P28	The privacy concerns of individuals in a social network can be classified into two categories: privacy after data release and the leakage of private information.
P29	Privacy values play a role in deterring site members from revealing their identities.
P30	It is necessary to anonymize the data prior to their publication to address the need to respect the privacy of the individuals whose sensitive information is included in these data.
P32	Gratifications and privacy concerns are cultivated by members' initial use experiences.
P33	Privacy preservation has gained importance with the development of tools for personal information retrieval and social information sharing in Web 2.0 environments.
P34	Serious privacy concerns exist for individuals whose personal information is contained in social networking data.
P35	The sharing of social network datasets is often constrained by privacy considerations.
P36	Privacy preferences can have a large impact on mobile ad hoc network protocol performance.
P37	Without adequate privacy protection, geosocial applications can be easily misused, for example, to track users or target them for home invasion.
P38	It is critically important to study the specified security and privacy requirements and their relations to the unique MSN characteristics before developing any specific scheme design.
P39	The question of how to publish social network data without compromising user privacy is a real concern.

Table VII. Discussions found in the reviewed literature about the issue of privacy

Paper ID	Discussion
	Trustworthiness
P4	From a user's perspective, the benefits of reputation-based trust include the ability to rate neighbours, a mechanism for reaching out to the rest of the community, and assurances regarding the trustworthiness of unknown users in the community.
P11	Trust management finds diverse applicability in many decision-making situations, including intrusion detection, authentication, access control, key management, the isolation of misbehaving nodes for effective routing, and other purposes.
P16	The competencies of individuals evolve over time, thereby requiring methods for the automated management of actor skills, reputation, and trust.
P18	Users are more likely to trust information received from a “friend” if the digital relationship between the two is based on a real-world relationship (friend, family, and colleague) rather than a purely online relationship.
P21	Trust is one of the most important factors in decision-making by a service consumer, which requires the evaluation of the trustworthiness of a service provider along the social trust paths from the service consumer to the service provider.
	Accuracy
P19	The accuracy of the relational inference framework presented in this study was firmly validated in its ability to assess the quality of self-reported user profile data.
	Access Control
P22	To protect user data, access control has become a central feature of OSNs.
P24	Content filtering can be regarded as an extension of access control because it can be used to protect both objects from unauthorized subjects and subjects from inappropriate objects.
	Authorization
P23	As an efficient alternative to ISS, an authorized private keyword search over encrypted PHI content can be exploited to satisfy privacy requirements by implicitly representing the PHI content with well-protected indices instead of directly using content names.

Table VIII. Discussion found in the reviewed literature about the issues of trustworthiness, accuracy, access control and authorization

Paper ID	Discussion
	Attack threats
P1	A side effect of this growth of attack threats is that possible exploits can turn OSNs into platforms for malicious and illegal activities, such as DDoS attacks, privacy violations, disk compromise, and malware propagation.
P9	The primary difficulty in near-duplicate spam detection is to withstand malicious attacks by spammers.
P31	Some of the security threats to mobile or cell phones include loss, theft or disposal, unauthorized access, malware, spam, electronic eavesdropping, electronic tracking, cloning and server resident data.
	Network conflict
P17	Wireless networking applications continue to pose challenging problems in the fields of information theory, signal processing, and social networking.

Table IX. Discussion found in the reviewed literature about attack threats and network conflict

CIA triad (%)	Contributing factors	Description	Studies from which the factor was extracted	Freq. (N = 39)
C, I, A (33%)	Protection tools (software / protocols / prototypes / systems)	Users utilize protection tools as implementations of concepts for protecting and securing social network systems from unwanted malicious actions or unauthorized parties.	P1, P5, P9, P15, P16, P18, P19, P20, P21, P30, P31, P34, P37	13
C (3%)	Ownership	Users find ownership to be useful because it allows them the right to access their own information on a social network without interference from unauthorized parties	P2	1
C, I (26%)	User behaviour	Users regard behavior as the attitude required to ensure security in an online social network system	P4, P6, P10, P11, P12, P26, P27, P29, P32, P36	10
C, I, A (38%)	Security policy	Users regard security policies as a set of rules that defines specific security requirements for the protection of an online social network system	P3, P7, P8, P13, P14, P17, P22, P23, P24, P25, P28, P33, P35, P38, P39	15

Table X. Factors contributing to information security practices in SSA