2. LITERATURE REVIEW

Literature review is a critical and in-depth evaluation of previous research work done in the given field. The review of literature gives the clean picture of the problem to be solved as being a prerequisite to actual planning and conducting the study. The review of past investigation serves as a guideline to the researcher, as it avoids duplications in the field. In other words, literature review is a summary of a particular area of research, allowing anybody reading it to establish why you are pursuing this particular research work. A good literature review expands upon the reasons behind selecting a particular research question.

In short, it can be said that the literature review provides a background to the research work to be carried out and it considers one or more of the following aspects depending on the research question being posed:

- Critical evaluation with appropriate breadth and depth
- Theoretical background – past, present or future
- Methodology and/or research methods
- Previous findings
- Rationale and/or relevance of the current study
- Discovering important variables relevant to the topic;
- Identifying relationships between ideas and practice;
- Establishing the context of the topic or problem;
- Enhancing and acquiring the subject vocabulary;
- Understanding the structure of the subject;
- Relating ideas and theory to applications;
- Identifying methodologies and techniques that have been used;

For the research work undertaken by me I have done the literature review as given below:

**Ralph Gross, Alessandro Acquisti (2005)**

In this paper the authors study patterns of information revelation in online social networks and their privacy implications. They analyze the online behavior of more than 4,000 Carnegie Mellon University students who have joined a popular social networking site catered to colleges and evaluate the amount of information they disclose and study their usage of the site’s privacy settings. Authors highlight potential attacks on various aspects of privacy of these users, and shown that only a minimal percentage of users changes the highly permeable privacy preferences.

**Mohamad B., samer Ei-sawda, Hajjeh I. (2007)**

This paper put forwards that phishing is a form of online identity theft employing both social engineering and technical subterfuge to steal user credentials such as usernames and passwords. Targeted data sources include especially web pages, email spam, domain names. Mounting a phishing attacks may take several ways but the popular one takes the form of a phishing message arrives in the user mailbox pretending to be from a bank, directing the user to a web page and asking him to enter his credentials, but the web page is not one actually associated with the bank. The authors focus on the Web site phishing, in which available solutions are based either on providing early warning of suspicious activity and rapid response or on the use of TLS (Transport Layer Security).
**Adrienne Felt (2007)**

This paper focuses on the highly personal nature of Facebook data and the amplifying effects of the Online Social Network which make it crucial that the Facebook Platform does not enable third-party attacks. This paper further describes Facebook’s security mechanisms and presents a cross-site scripting vulnerability in Facebook Markup Language (FBML) that allows arbitrary JavaScript to be added to application users’ profiles. The profile in the code can then defeat their anti-request forging security measures and hijack the sessions of viewers.

**Paul Heymann, Hector Garcia (2007)**

According to this paper the success of Online Social Network has come with a growing influx of spam. If left unchecked, spam threatens to undermine resource sharing, interactivity, and openness of the Online Social Network. The paper surveys three categories of potential countermeasures - those based on detection, demotion, and prevention. Although many of these countermeasures have been proposed before for email and Web spam, the authors find that their applicability to social Web sites differs and also focused on how should we evaluate spam countermeasures for social websites, and what future challenges might we face?

**Danfens Y, Frikken K.B., Mikhail A., Roberto T (2008)**

This paper studies the notion of quantitative policies for trust management and gives protocols for realizing them in a disclosure-minimizing fashion. Here every user is having credential with certain points and requires a minimum total threshold of points before granting anybody else access to a resource. privacy-valuation of every credentials is kept private. The authors give protocols for computing such a subset of user's credentials without revealing any of
the two parties' above-mentioned private information. Furthermore, the authors develop a fingerprint method that allows the user to independently and easily recover the optimal knapsack solution. The fingerprint method is useful beyond the specific authorization problem studied, and can be applied to any integer knapsack dynamic programming in a private setting.

**Joshi Y., Saklikar S., Das D., Saha S. (2008)**

This paper presents phishing as act of identity theft aimed at acquiring sensitive information such as usernames, passwords, credit card details etc., by masquerading as a trustworthy entity in an electronic communication. Phishers use a number of different social engineering mechanism such as spoofed e-mail to try to trick their victims. Though there are many existing anti-phishing solutions, phishers continue to succeed to lure victims. In this paper authors proposed a novel algorithm which aims at identifying a forged website by submitting random credentials before the actual credentials in a login process of a website. We have also proposed a mechanism for analyzing the responses from the server against the submissions of all those credentials to determine if the website is original or phished one. Though the idea is generic and would work in any authentication technologies which are based on exchange of any credentials, the current prototype is developed for sites supporting HTTP Digest Authentication and accepting userID and password pair as credential.

**Weimin L., Jingbo L., Jing L., Chengyu F. (2009)**

This paper points out the threats to online social networks in recent years and analyze the targets, what the attackers want and the methods how attackers perform the attacks. Authors separate social networks into two part as user and social networking site and discuss in details
the countermeasures against the threats to social networks. They propose a security framework of social networks.

Danesh I., Steve W., Li K., Calton Pu (2009)

In this paper the authors presented study of large online social footprints by collecting data on 13,990 active users. After parsing data from 10 of the 15 most popular social networking sites, it was found that a user with one social network reveals an average of 4.3 personal information fields. For users with over 8 social networks, this average increases to 8.25 fields. Further the authors also investigate the ease by which an attacker can reconstruct a person's social network profile. Over 40% of an individual's social footprint can be reconstructed by using a single pseudonym (assuming the attacker guesses the most popular pseudonym), and an attacker can reconstruct 10% to 35% of an individual's social footprint by using the person's name. the authors also perform an initial investigation of matching profiles using public information in a person's profile.

Tootoonchian A., Stefan S., Yashar G., Wolman A (2009)

This paper presents Lockr, a system that improves the privacy of centralized and decentralized online content sharing systems. Lockr offers three significant privacy benefits to OSN users. First, it separates social networking content from all other functionality that OSNs provide. This decoupling lets users control their own social information: they can decide which OSN provider should store it, which third parties should have access to it, or they can even choose to manage it themselves. Such flexibility better accommodates OSN user’s privacy needs and preferences. Second, Lockr ensures that digitally signed social relationships needed to access
social data cannot be re-used by the OSN for unintended purposes. This feature drastically reduces the value to others of social content that users entrust to OSN providers. Finally, Lockr enables message encryption using a social relationship key. This key lets two strangers with a common friend verify their relationship without exposing it to others, a common privacy threat when sharing data in a decentralized scenario.

**Jan Nagy, Peter Pecho** (2009)

This paper analyses possibilities of misusing social network sites due to irresponsible behaviour of users. Social engineering can be misused by attackers concerning on social network with the purpose of gaining sensitive information. The authors found out users’ behaviour which leads to insufficient protection of published information. This sensitive information is suitable for all kinds of phishing and other similar attacks.

**Chuan Yue, Haining Wang**  (2010)

The authors claim that many anti-phishing mechanisms currently focus on helping users verify whether a Web site is genuine. However, usability studies have demonstrated that prevention-based approaches alone fail to effectively suppress phishing attacks and protect Internet users from revealing their credentials to phishing sites. In this paper, instead of preventing human users from “biting the bait,” the authors propose a new approach to protect against phishing attacks with “bogus bites.” The authors develop BogusBiter, a unique client-side anti-phishing tool, which transparently feeds a relatively large number of bogus credentials into a suspected phishing site. BogusBiter conceals a victim’s real credential among bogus credentials, and moreover, it enables a legitimate Web site to identify stolen credentials in a timely manner.
Leveraging the power of client-side automatic phishing detection techniques, BogusBiter is complementary to existing preventive anti-phishing approaches.


This paper put forwards the design issues for the security and privacy of Online Social Networks. There are some inherent design conflicts between these and the traditional design goals of Online Social Networks such as usability and sociability. The authors present the unique security and privacy design challenges brought by the core functionalities of Online Social Networks and highlight some opportunities of utilizing social network theory to mitigate these design conflicts.


According to this paper a side-effect of tremendous growth of Online Social Network is that possible exploits can turn Online Social Network into platforms for malicious and illegal activities, like DDoS attacks, privacy violations, disk compromise, and malware propagation. In this paper it is shown that social networking web sites have the ideal properties to become attack platforms. The authors introduce a new term, antisocial networks that refers to distributed systems based on social networking web sites which can be exploited to carry out network attacks. An adversary can take control of a visitor's session by remotely manipulating their browsers through legitimate web control functionality such as image-loading HTML tags, JavaScript instructions, and Java applets.

Justin Zhan (2010)
According to the authors a social network is the mapping and measuring of relationships and flows between individuals, groups, organizations, computers, websites, and other information/knowledge processing entities. Privacy-preserving social networks have not been well explored. So in this paper, authors tried to address how to build up a social network involving multiple parties. Data collection is a necessary step in the social-network-construction process. Due to privacy reasons, collecting data from different parties becomes difficult and these concerns may prevent the parties from directly sharing the data. How multiple parties collaboratively construct a social network without breaching data privacy presents a challenge. This paper has tried to provide a solution for privacy-preserving collaborative social-network problem.

Dimitrios M., Ioannis M. (2010)

This paper presents a survey on online social network’s privacy leaks and the potential hazards for users, especially teenagers. In particular, the profiles of two teenagers, one male and one female, with fake names were created. Using a suitable software tool, friend requests were sent massively. As a result, two networks of friends were created and access was granted to a significant amount of users’ personal information. Both profiles received requests for friendship and personal chat by adults aged up to 53 years old. In general the survey leads to results that reveal several hazards for children and critical issues about privacy of social network users.

Alkesandra korolova (2010)

In this paper the authors propose a new class of attacks that exploit advertising systems offering micro targeting capabilities in order to breach user privacy. The authors studied the
advertising system offered by the world's largest online social network - Facebook, and the risks that the design of the system poses to the privacy of its users. This paper further propose, describe and provide experimental evidence of several novel approaches to exploiting the advertising system in order to obtain private user information. The authors communicated their findings to Facebook on July 13, 2010, and received a prompt response. On July 20, 2010, Facebook launched a change to their advertising system that made the kind of attacks described by the authors more difficult but not impossible to implement.


In this paper the authors pointed out that the Online Social Networking web sites have the ideal properties to become attack platforms. The authors introduce a new term, antisocial networks that refers to distributed systems based on social networking web sites which can be exploited to carry out network attacks. An adversary can take control of a visitor's session by remotely manipulating their browsers through legitimate web control functionality such as image-loading HTML tags, JavaScript instructions, and Java applets.

Gail-Joon A., Mohamed S., Anna S. (2011)

According to this paper one of the most important issues we must immediately address is the security and privacy of sensitive information, which is generally any data an adversary, could use to cause significant harm to users. Unfortunately, current trends in Online Social Networks indirectly require users to become system and policy administrators to protect their own online contents. Further complicating this issue is social networks’ rapid growth as well as their continual adoption of new services.
Danesh I., Steve W., Calton Pu, kang li (2011)

This paper performs modeling of unintended personal-information leakage from multiple Online Social Network account of the same person. As these networks offer various levels of privacy protection, the weakest privacy policies in the social network ecosystem determine how much personal information is disclosed online. A new information leakage measure quantifies the information available about a given user. Using this measure makes it possible to evaluate the vulnerability of a user’s social footprint to two known Attacks like physical identification and password recovery.

Na Li, Nan Z., Sajal Das (2011)

This paper depicts about systematic look at existing privacy-preservation techniques and highlights the vulnerabilities of users even in networks that completely anonymize identities. Through a taxonomy that categorizes techniques according to the degree of user identity exposure, the authors examine the ways that existing approaches compromise relation privacy and offer more secure alternatives.

Paul M. Schwartz (2011)

According to this paper when using the analytics process, Online Social Networking companies should consider the risks it poses to individual’s information privacy as well as develop responsible measures to accompany its use. This set of ethical standards calls on companies to adopt accountable approaches that reflect the specific risks in a given use of the analytics process.
Saeed A., Thomas C., Omar A. (2011)

A large-scale study of more than half a million Facebook posts suggests that members of online social networks can expect a significant chance of encountering spam posts and a much lower but not negligible chance of coming across malicious links.

Khan N., Duck T. (2011)

This paper focuses on the analysis of activities of user in the faceboook. Facebook has been the largest, most influential and fastest growing social network on internet to the date. As facebook’s userbase is extremely diverse, spreading across different countries, races, ages, professions and interests to name a few, this network is a good model to study. This paper presents an analysis of regional facebook dataset, with attention given to the correlation among user connectivity, activity and similarity.

Sora, Shin, Yumi, KO, Jihwa, Jang (2011)

This paper focuses on whether the personal needs of privacy and the one of self-disclosure have a one-dimensional relationship with each other or are independent from each other. Authors reviewed research articles both on information privacy and on self-disclosure. This research also focuses on the dynamic relations between the needs for self-disclosure and privacy attitudes among SNS users.

This paper focuses on the profile cloning where the attackers may duplicate a user's online presence in the same or across different social networks and, therefore, fool other users into forming trusting social relations with the fake profile. By abusing that implicit trust transferred from the concept of relations in the physical world, they can launch phishing attacks, harvest sensitive user information, or cause unfavorable repercussions to the legitimate profile's owner. This paper further proposes a methodology for detecting social network profile cloning. The authors present the architectural design and implementation details of a prototype system that can be employed by users to investigate whether they have fallen victims to such an attack. The experimental results from the use of this prototype system prove its efficiency and also demonstrate its simplicity in terms of deployment by everyday users.

Markus H., Martin M., Gerhad k., sigrun G., Edgar w. (2010)

This paper focuses on Friend-in-the-middle attacks on social networking sites which can be used to harvest social data in an automated fashion. Attackers can then exploit this data for large-scale attacks using context-aware spam and social phishing. The authors prove the feasibility of such an attack and simulate the impact on Facebook. Alarmingly, all major social networking sites are vulnerable to this attack because they fail to appropriately secure the network layer.


This paper surveys the current state of security issues pertaining to popular Online Social Networks. Some issues related to privacy, viral marketing, structural attacks and malware attacks discussed with a focus on the privacy concerns. This paper presents an in depth discussion of
each category of attacks and the defense mechanisms as well as analyze connections among different security issues.