Sub-Sahara African Academic Research Publications
March, 2022, Editions

JASOR
Journal of Advanced Science and Optimization Research
Vol. 23, No.9, ISSN 2418-9325

AN EFFECT OF SECURITY AND PRIVACY IN SOCIAL NETWORKING

EDINO KENNEDY O.; OKORODUDU JOSEPH
Computer Science Department, Delta State Polytechnic Otefe-Oghara

ABSTRACT
In the era of Internet technologies, social networking websites has witnessed thriving popularity. Computer mediated communication has changed the rules of social interaction and communication. Most social networking sites like Orkut, Facebook, Googlet, Twitter etc. facilitates users with the features like online interaction, sharing of information, knowledge and developing new relationships etc. Online interaction and sharing of personal information in social networking sites has raised new privacy concerns. So, it requires an exploratory insight into users behavioural intention to share information. The task resource manager is to identify better method to provide effective protection to improve security. This research paper analyses security and privacy issues in social networking sites. The main aim is to enhance the user security and privacy which is the most important for the social network services. This paper is a survey which is more specific to exposes the social networks service models and issues in network environment with respect to enhancement of security.

***Keywords**: Enhancement, Social Networking, Online Interaction, Exploratory, Users Behavioural*

INTRODUCTION
In the recent years, user's participation in the Social networking sites has moved from its niche phenomenon to its highest level of mass adoption. The rapid growth of social networking sites under web 2.0 such as Facebook, Orkut, Google+, Twitter etc. felicitates millions of individuals to build a public or

semi-public profile within a bounded system. Facebook has become most accessed website in the cyberspace today. Facebook statistics shows that it has one billion active users as of October 2012 with 552 million daily active users in average in June 2012 (Bilge, et al., 2019).

The active participation in social networking sites have changed the way people build their online personal network for computer mediated communication. The primary objective of social networking users is to make connections, communication and maintain relationships. But latest trends shows social networking sites like Facebook is reshaping the way people communicate. The Internet's wide adoption has contributed to online social networking sites' thriving popularity, which is evident in the attention such sites received from both the media and academia.

One of the most important issues we must immediately address in this context is the security and privacy of sensitive information, which is generally any data an adversary could use to cause significant harm to users. Such data might include financial information, which an attacker could use to perpetrate identity theft, or medical information, such as health conditions, diagnoses, or treatment histories. Unfortunately, current trends in social networks indirectly require users to become system and policy administrators to protect their online contents.

Social networks have seen a dramatic growth during the past decade. For users, the benefits provided by the services outweighed any risks to privacy imposed by usage of these services. The privacy concerns and awareness did not stop users from revealing large amounts of personal information. In fact, in 2005, the majority of users opted to use default privacy settings, which were quite loose (Zheleva & Getoor, 2019). This combined with security was existing in these services created a favorable environment for collecting of private data not only by the service provider, but also by various third parties.

Gradually, the awareness of privacy risks among users increased. According to, in 2009 the majority of surveyed Facebook users were already using much stricter access policies. Furthermore, users started actively defending their privacy. Changes, introduced by the social network provider, which users considered as a potential threat to their privacy were met with protests.

While security patches and additional privacy mechanisms developed by social network providers gave users the impression that they were in control of their

data, in reality it has always been a social network service provider (SNP) that has had full control. For example, Facebook's Terms of Services (TOS) up till November 2013 stated that it gets "perpetual non-exclusive, transferable, fully paid, and worldwide" license to any content user posts and that it can use it for commercial or advertising purposes. Google's TOS up till March 2012 stated that the company had perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to user content and that it could make this content available to other companies, organizations or individuals for the provision of syndicated services. Other services like Twitter, Instagram, and Linkedin have TOS that gives them similar rights to the user content. While Google's current TOS are much more modest and state that "The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones.", Facebook according to its current TOS still retains: "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post" (Von, et al., 2015).

LITERATURE REVIEW

In related social networking site research, some prior studies examined the impact of privacy concerns on usage behaviour and information revelation. Park & Sandhu, (2017) defined information privacy as ‘the claim of individuals, groups, or institutions to determine of themselves when, how, and to what extent information about them is communicated to others’. Privacy can be defined as ‘control over the flow of one’s personal information, including the transfer and exchange of that information’. Security is defined as ‘the extent to which a user believes that using a social networking application will be risk-free’

Von, et al., 2015 defined privacy as a process of anonymity preservation and is strongly connected to control over information about the self. In online environments, people who perceive higher threats to privacy are less disposed to disclose information about the self because they perceive themselves as less able to control information and also protect themselves. In contrast, when people perceive lower privacy risks and higher control, such as when privacy policies are clearly exposed, they disclose more personal information. Research in information security and marketing has argued that information privacy and consumer concerns thereof are one of the most important issues in today’s technology-based environment. The concept of privacy is in itself not new and

it has generally been defined as an individual's ability to control the terms by which their personal information is acquired and used (Park & Sandhu, 2017).
Security corresponds to concerns about the protection of personal information with three specific goals: integrity that ensures information is not altered during transit and storage; authentication that addresses the verification of a user's identity and eligibility for data access; and confidentiality that requires that data use be confined to authorized purposes by authorized people.
The use of personal information in social networks raises new privacy concerns and requires insights into security problems. Online social networks have recently emerged as a challenging research area with a vast reach and application space. Several studies and recent news reports have highlighted the increased risk to personal data processed by online social networking applications, as well as the user population's lack of awareness. In general, the privacy issue in social networking is coupled with the identifiability and linkability of the information available in this social setting, its possible recipients, and its potential uses (Von, et al., 2015).

CONCEPT OF SECURITY AND PRIVACY IN SOCIAL NETWORK

Social networks' security and privacy requirements still aren't well understood or fully defined. Nevertheless, it's clear that they'll be quite different from classic security and privacy requirements because social networks involve user-centric concerns and allow multiple users to specify security policies on shared data. So, we must bring a depth of security experience from multiple security domains and technologies to this field, as well as a breadth of knowledge about social networks (Park & Sandhu, 2017).
In the larger context of data mining, a considerable measure of productive analyzing so as to learn can be found advanced records of human conduct in interpersonal organizations without breaching the users' privacy. Thus, information ought to be made accessible in a manner that privacy should be safeguarded and protection is extremely scrutinized.
According to Lin & Lu, (2011), who had proposed that any sort of examination about the number of inhabitants in clients who express inclinations, therefore defusing protection dangers as well as vital investigation. The proposition is still to keep connection ready to the interpersonal organization profiles of their users, however to permit clients to partner some guaranteed property

estimations with their credentials, by picking each time they express credits that need to uncover. In the sideline perspective of the privacy domain (Correa, et al., 2010), the subject of privacy has been under scrutiny and ensuring the basic importance given by the particular academic group has deemed to be vigilant. To ensure privacy of clients by recognizing characteristics, not by vulnerability based anonymization.

Maintaining privacy of the register users is the central role of the authorities and any deviation of policy given would totally wreck the organizational policy governance which in turn leads to serious havoc to the fundamental rights of society. In social media, some of the private data are shared by the user unknowingly or voluntarily. Sometimes, private details other than that are intentionally shared by the users are extracted from them extrinsically by offering them some benefits. Through the Location-Based Social Network Services (LBSNS) like FireEagle, Google Latitude, Nearby etc., you are able to identify the location of a person. Even you are able to identify the location of his/her friends.

SECURITY AND PRIVACY SETTING

Many social networking sites provide configurable security and privacy setting to empower the client to shield their personal information from undesirable access by outsiders or applications. For instance, the Facebook client can modify their security setting and select the audience (like friends, friends of friends, and everybody) in the network who can see their details, pictures, posts, and other sensitive information. Moreover, Facebook additionally permits its users to either acknowledge or reject the access of third-party applications to their personal information. Many social networking sites are equipped with security measures that are internal to the system. They ensure users of the network against spams, counterfeit profiles, spammers, and different risks (Jagatic, et al., 2017).

ISSUES IN SOCIAL NETWORKS

Social Networks has lot issues to discuss in the network environment. But this paper concentrate the unsolved issues like security, trust and privacy. The new mechanism will solve the issues. This study describes the Social Network

Models and also security which is one of the key attribute for resource provisioning.

1. **Security issues:** Network security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also emphasizes about the delivery of services through service models. Network security comprises a broad range of security constraints from an end-user and provider's perspective, where the end-user will always prioritize the provider's security policy.
2. **Trust:** Trust is considered as the „assurance" and confidence that people, data, entities, information or processes to function or behave in expected ways. Trust may be human to human, machine to machine or machine to human. At a deeper level, trust is regarded as a criteria towards security or privacy objectives.
3. **Privacy:** Privacy is an important component of trust. The key issue is to enhance privacy by improving security. Security strategy is adopted in network environments to enhance privacy.

SOCIAL NETWORKS PRIVACY

Shijen et al (2012) proposed method of detect collusive fraud group in online auctions. This method adopted two algorithm. The k-core clustering algorithm used to collect real auction cases and potential collusive fraud groups, and to discover the critical accounts of the groups by page rank algorithm. The auction fraud algorithm used to evaluate the risk of each accounts the group.

JichangZhiao et al (2011) investigated the relationship between the strength and information propagation in online social networks. The empirical study proves three interesting finding strategies: the information pushing strategy, cost intensive strategy and the random selection strategy. The author explains by characterizing weak ties into positive & negative one and reveal the special bridge effect of positive weak ties.

A framework for exploring organizational structure in dynamic social networks proposed by Jangtao et al (2011). The framework combines two algorithm: Page Rank and Random Walk.

These two algorithm used to derive the community tree from social networks. The new tree learning algorithm developed to explore the organization structure dynamic social networks. Java language software was used for implementation.

Jeremy et al (2011) proposed interleaving multi agent system & social networks for organized adoption. The open system has three models: Norm governed system:

- rule of social order, an opinion formation
- rule of social exchange, mechanism design
- rule of social choice.

The logical model of the voting protocol used for computational formation.
RachaAjam et al (2012). "Address the privacy issue in mobile social networks. The author explains about the idea of Mobile Social Networks Application and Location Based Applications. The Mobile Social Networks includes three approaches:

- Identity Server and Anonymous identifier,
- Virtual Individual Server for Mobile Services and
- Resocializing social networks.

These three approaches comparison evaluated on their performance such as flexibility, operation protection, user anonymity and dependency. The privacy enhancing social network mechanism proposed by Iain et al (2012). The mechanism analysis of the privacy risk in social network routing. There are two complementary method:

- Statisticulated social network routing and
- Obfuscated social network routing.

The performance evaluated by trace driven simulation parameter methods. And also they used three metrics: delivery ratio, delivery cost and delivery delay.
A system to filter unwanted messages from Online Social Networks (OSNs) user walls proposed by Macro, et al (2011). The key idea of the proposed system is support for the content based used preferences. The system allows ONSs users to have a direct control on messages posted on their walls. This is achieved through a flexible rule based system that allows users to customize the filtering criteria to be applied to their walls. Machine learning based text classification method used to detect automatically assign with each message a set of categories text contents.

MohdIzuan & Jemal, (2011). Presented systematic analysis of various risk to privacy in publishing of Social Network Data. These analysis includes three threat analysis: Data Representation, Background Knowledge and data mapping. The privacy breaches classified into identity disclosure attacks, sensitive link disclosure and sensitive attribute disclosure. The process of retrieving information from Online Social Networks(OSNs) using Multi Agent System(MAS) proposed by Rugayya et al (2011). This paper provides a method to investigate situation which require a continuous observation of the user profile in order to track the changes that could help in understanding the structure of the OSNs. Online Social Retrieval algorithm used to speed up the extraction process of retrieval information. MySpace was selected domain for the purpose of experiment.

DISCUSSION

The security issues and privacy concerns are the major requirements of the social networking sites. But there were many deadliest attacks persists in all these social networking sites and safeguarding the potential users from these heinous attack have been the challenging task of many social analyst and developers.

The basic security attacks are classified into three categories.

- **Privacy Breach -** Find link between nodes and edges and possibly identify the relation between them.
- **Passive Attacks** - This is totally anonymous and undetectable.
- **Active Attacks** - Form the new nodes intrinsically and trying to connect to the linked nodes and gain the access to the other nodes.

The table below illustrates the clear depictions of various attacks in social media sites and given the possible solution to how to handle the attacks safely (Carl & Richard, 2010).

Table 1: Major attacks, sub-attacks, and possible preventive policies (Carl & Richard, 2010).

Major domain of attacks	Sub-attacks	Solution to handle the attacks
Social Networking Infrastructure attacks	TCP SYN Flood Attack, Smurf IP Attack,	-Use Anti-Virus and Anti-Malware Software.

	UDP Flood Attack, Ping of death, Tear Drop	-Install appropriate Intrusion Detection System.
Malware Attacks Crimeware,	Spyware, Adware, Browser Hijackers, Downloader, Tool Bars	-Use of Anti-Virus. -Do not go for unknown links, friends, applications, email attachments etc., -Disable Cookies, Sessions, ActiveX if unknown or no counter-measures available.
Phishing Attacks	Deceptive phishing (emails), Malwarebased phishing, Keyloggers, Search engine phishing	-Examine the emails carefully. -Validate the source of the data. - Beware of ads with offers
Evil Twin Attacks	Social engineering attack	-Careful about having friends and sharing information. -Authenticate the user profile and share the data. -Try to completely understand the policies of having friends in the social networking sites.
Identity Theft Attacks	Dumpster diving	-Use complex passwords, avoid password re-usage. -Shred your email or documents properly.
Cyberbullying	Cyberbullying	-Do not acknowledge the messages that are intended to hurt or threat. -Save and Archive the messages as evidences. -Take all threats seriously -Do not share personal information with all users.

Physical Attacks	Impersonation, Harassment through messages	-Need a well-defined social networking policy. -Background security and privacy checks. -Properly make use of privacy settings options.

SECURITY AND PRIVACY SETUP ON SOCIAL NETWORKING SITES

Social network sites destinations work to reinforce privacy settings. Facebook and other long range social communication destinations limit protection as a major aspect of their default settings. It's essential for clients to go into their client settings to alter their protection choices. These locales like Facebook give clients the alternative to not show individual data, for example, conception date, email, telephone number, and business status. For the individuals who decide to incorporate this material, Facebook permit clients to limit access to their profile to just permit the individuals who they acknowledge as "companions" to see their profile. Be that as it may, even this level of privacy can't keep one of those companions from sparing a photograph to their own PC and posting it somewhere else. Be that as it may, at present less social media site clients have constrained their profiles.

For example, let us take how the users restrict the profile visibility to others in different social media sites:

- Facebook: Facebook's privacy setting for new users is set to Friends Only. To set this, visit Settings > Privacy >
- Twitter**:** Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets.
- LinkedIn: To change this: Settings > Account > Helpful Links > Edit your public profile.
- Google+: To change this setting, type the name of a Circle in the "To" field below your post before you publish it.

SECURITY OBJECTIVES OF SOCIAL NETWORK

Privacy, Integrity, and Availability Security objectives are requirements that have to be satisfied in order to protect the system from potential threats and

attacks. In this chapter we provide an overview of important security objectives for online social networks.

First of all we notice that classical requirements of confidentiality, integrity, and availability, have a special touch when considered in the scope of SNs. While integrity and availability have only subtle differences compared to other communication systems, in that they mostly address the content provided by the users, the requirement of confidentiality (usually associated with encryption) is no longer sufficient and should be extended to the more comprehensive security objective -privacy.

While potential breach of user privacy and integrity of user-provided contents may lead to economic damages for the users, cause embarrassing situations, and also tarnish their reputation (even in the real world), the missing availability of contents or services may also decrease the attractiveness of the actual SN platform and harm its provider (Gross & Acquisti, 2015). It is extremely difficult to cope with all these goals simultaneously. Especially privacy of SN users is challenging since the amount of personal information is huge and this information may be available not only from a particular SN platform but also from the web. In the following, we describe privacy, integrity and availability objectives for social networks, while also mentioning potential threats with regard to not only the profile owner, but also other

PRIVACY RELATED THREATS IN SOCIAL NETWORK (SN)

The diversity of available OSN platforms opens doors for a variety of attacks on privacy of the users, integrity of their profiles, and the availability of the user provided contents are as follows:

Plain Impersonation: With plain impersonation attack the adversary aims to create fake profiles for real-world users as depicted on the figure below. In this sense a real-world user will be impersonated within the SN platform. The success of this attack strongly depends on the authentication mechanisms deployed in the registration process.

Profile Cloning: The goal of the adversary here is to create a profile for some user that is already in possession of some valid profile in the same network. From the technical point of view this attack can be realized through the registration of the new profile using the same (or similar) content as the existing one.

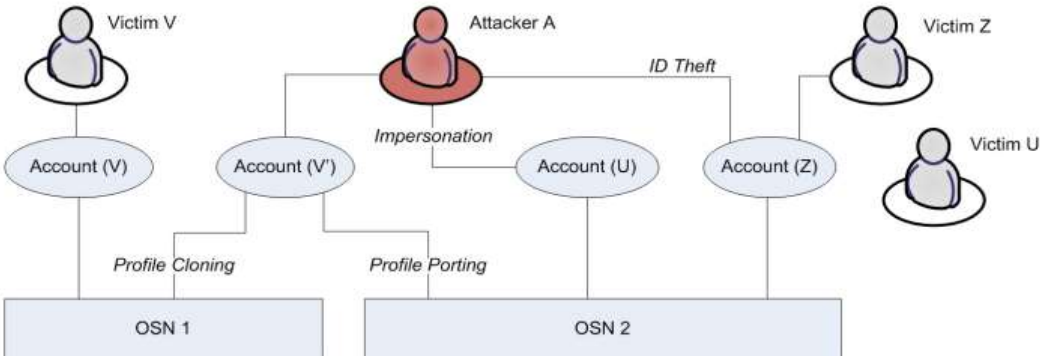

Fig. 3.1. Privacy related threats in social network (Gross & Acquisti, 2015)

Profile Hijacking: The goal of the adversary mounting a profile hijacking attack is to obtain control over some existing profile within an OSN platform. Many OSN platforms protect user access to their own profiles via passwords. Hence, from the technical point of view profile hijacking is successful if the adversary can obtain passwords of other users. This can be done by many means. First, it is a well-known fact that the majority of users choose weak passwords that can be recovered via an automated dictionary attack.

Profile Porting: By profile porting we understand another type of impersonation where some profile that exists within one SN platform is cloned into another OSN platform. From the technical point of view this attack can be realized via registration of a profile using some new email address. Profile porting is appealing since not every user has her own profile on every available SN platform.

ID Theft: An adversary mounting the ID theft attack should be able to convince anyone about the ownership of some particular OSN profile. In this way the adversary can possibly misuse the reputation or expertise of the real profile owner for own benefit, while leaving the owner unaware of the attack. One way for a successful ID theft attack is to take control over the target profile. This requires the same effort as for the profile hijacking attack.

Other privacy related threats include; Fake Requests, Crawling and Harvesting, profiling

REASONS BEHIND ONLINE SOCIAL MEDIA SECURITY ISSUES

Social media addresses one of the most unique, unstructured, and unregulated datasets anyplace in the advanced world and this scene is arising quickly all over the globe. Every day millions of people upload their photos and other

multimedia content on social media to share it with their friends. This is prompting the development of digital risk monitoring. The development of web-based media has presented new security standards that put clients (representatives, clients, and partners) solidly in the aggressor's line of sight. The social network has become the new digital milestone where attackers think that it's simple to target victims. It has presented one of the biggest, most powerful dangers to authoritative security. Attackers influence social media for the accompanying three reasons:

1. **The scale of social media:** since a huge mass of people spend their time on social media for various purposes, attacks can spread like any other viral trend.
2. **Trusted nature of social media:** adversaries take advantage of the trusting nature of social media. People sometimes accept an unknown friend request on the basis of mutual friends that requester has.
3. **Invisibility to security team:** majority of people in the world spend most of their time on social media networks.

SECURITY AND PRIVACY GUIDELINES IN SOCIAL NETWORK

1. Use a strong password
2. Limit location sharing
3. Be selective with friend requests.
4. Be careful about what you share
5. Be aware of links and third-party applications
6. Install internet security software
7. Enable two-step authentication for all your social media accounts wherever possible.

Methodology

Investigate the social information of the potential users and acquire the much needed details such as demographic data, temporal data, user profile etc., of the respondents. To augment this process, we had taken a survey system that will be thoroughly utilized and disseminated to over more than 200 social media users and the populace will be dictated by the non–probability testing strategy. Spiral testing and respondent-driven examining have additionally permits analysts to make gauges about the interpersonal organization joining the

shrouded populace to solicit them on the protection from the current social network communities. Hence, this comprehensive study has focused more on privacy concerns hinges on the social networks and jolt out the privacy breaches effectively. We had identified some of the privacy concerns that the social users can undertake before they uses the social sites and embed their privacy setting on the site to prevent any breach of violation.

This study goes for discovering the security and privacy in social network sites locales recognition among Social Media clients. A specimen of 250 understudies was chosen haphazardly from distinctive piece of the world. A net of 185 polls were filled effectively and returned. Almost 78% of the respondents were males, while about 22% of them were females. On the other hand, roughly 72 of respondents were in the age bunch 20-35 years of age. Be that as it may, the quantity of respondents in the age gatherings "between 28-41 practically got 19% where different gatherings 50 or more is right around zero. Instructive level played a high effect subsequent to 58% are four year certification and graduate degrees are 21%. The years of utilizing Internet think about the commonality of interpersonal organization on the grounds that from those are utilizing the web for over 10 years are 56% and in the event that we connect the use with nature of SN it indicates 51 % for decently recognizable and 49% for extremely well known . Then again 90% of this study populace is utilizing Facebook and 36 % utilizing Islam Tag and 62% twitter so this is leeway for us to think about Facebook protection model.

When getting some information about privacy and security be are mindful of protection and terms of conditions, 52% are modestly acquainted with the elements and redesigns in Social Media protection which was demonstrated that they are acquainted with the protection when 87% confine get to some for certain part in their profile. Be that as it may, in the matter of changing protection 43% change their privacy setting often which implies just if anything happened and 47% once in a while change their protection setting and the same goes for privacy and record setting.

We had identified the different privacy mechanisms that the social media site offered to the users to set in and engage in the privacy concerned activities. There would be a wide range of discrimination persists in the social media sets in offering the privacy policies to the users and from the survey taken, it has largely been noted that many of the users of social media site has.

CONCLUSION

It has been observed that privacy concerns are very feeble in the social networking sites and the users endeavours to make the appropriate changes on their social media privacy is substantially lower than other mode of security operations. If we would go for enforcing a set of well-defined policies for social media, like, a strong password, awareness of changing password often, awareness of information disclosure, purpose of antivirus or related software, and proprietary software etc.

RECOMMENDATIONS

Social network plays a vital role in our day to day activities, in order to ensure the security and privacy of our social network account, it is recommended that;

1. We should be aware of links and third-party applications
2. Internet security software should be installed
3. Two-step authentication should be enabled for all your social media accounts wherever possible.

REFERENCES

Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. (2019). "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks". In 18th Intl. World Wide Web Conference.

Carl, T. & Richard, P. (2010). "Seven Deadliest Social Network Attacks". Syngress Publishing.

Correa, T., Hinsley, A.W. & De Zuniga, H.G. (2010). "Who interacts on the web?: The intersection of users‟ personality and social media use," Computers in Human Behavior, vol. 26, no.2, pp. 247–253.

Gail-Joon, A., Mohamed, S. & Anna, S. (2011). "Security and Privacy in Social Networks". IEEE Internet Computing; 15(3): 10-12.

Gross, R. & Acquisti, A. (2015). "Information revelation and privacy in online social networks". In ACM Workshop on Privacy in the Electronic Society, pages 71 – 80.

Iain, P., & Tristan, H. (2012). "Privacy-enhanced social-network routing", Computer Communications (Elsevier)35 pp. 62–74.

Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. (2017). "Social phishing". Communications of the ACM, pages 94–100.

Jeremy, P., Daniel, R.C., & MoezDraief, A.A. (2011). "Interleaving multi-agent systems and social networks for organized adaptation", Springer.

Jiangtao, Q.Z.L. (2011). "A framework for exploring organizational structure in dynamic social networks", Decision Support Systems (Elsevier) 51 (2011) 760–771.

Jichang Z., JunjieWu, X. & HuiXiong, K. (2011). "Information propagation in online social networks: a tie-strength perspective", Springer-Verlag London.

Lin, K.Y. & Lu, H.P. (2011). "Why people use social networking sites: An empirical study integrating network externalities and motivation theory,"Computers in Human Behavior, vol. 27, no. 3, pp. 1152–1161.

Marco, V., Elisabetta, B.C., Moreno, C. & Elena, F. (2011). "Content-Based Filtering in On-Line Social Networks", Springer-Verlag Berlin Heidelberg.

MohdIzuan, H. N. & Jemal, A. (2011). "Privacy Threat Analysis of Social Network Data", Springer-Verlag Berlin Heidelberg, pp. 165–174.

Park, J. & Sandhu, R. (2017). "Towards usage control models: beyond traditional access control". In SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies, pages 57–64, New York, NY, USA. ACM.

Patrick, V.E. & Maarten, T. (2010). "Privacy and social networks". Computer Law & Security Review; 26(5):535-546.

RachaAjami, N.A.Q. & Noha, R. (2012). "Privacy Issues in Mobile Social Networks", Procedia Computer Science (Elsevier) 10, pp. 672 – 679.

Ruqayya, A., Daniel, N. & Holton, D.R.W. (2011). "Multi Agent System for Historical Information Retrieval from Online Social Networks", Springer-Verlag Berlin Heidelberg, pp. 54–63.

Shijen, L, Yi-Ying, J. & Cheng-Hsien Y. (2012). "Security Concept: Combining ranking concept and social network analysis to detect collusive groups in online auctions", Expert Systems with Applications (Elsevier) 39 9079–9086.

Von, L.A., Blum, M., Hopper, N. J. & Langford, J. (2015). "CAPTCHA: Using Hard AI Problems for Security". In EUROCRYPT, volume 2656 of LNCS, pages 294–311. Springer.

Zheleva, E. & Getoor, L. (2019). "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles". In WWW, pages 531–540. ACM.