INFORMATION SECURITY AWARENESS FRAMEWORK FOR ENHANCING SECURITY PRIVACY AMONG TWITTER USERS

ABBAS YASLAM SAEED HUSSEIN

UNIVERSITI TEKNOLOGI MALAYSIA

INFORMATION SECURITY AWARENESS FRAMEWORK FOR ENHANCING
SECURITY PRIVACY AMONG TWITTER USERS

ABBAS YASLAM SAEED HUSSEIN

A project submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARYR 2017

In the name of ALLAH, the Most Gracious and the Most Merciful

To my beloved father's spirit and to my beloved mother may Allah bless her who

made me see further by standing on their shoulders, and to all my family and friends.

Thank you.

ACKNOWLEDGEMENT

Alhamdulillah, all praise to Allah for the strengths and His blessing to completing this research and thesis writing. My special appreciation goes to my supervisor, **Dr. Siti Hajar Othman**, for her incomparable guiding to achieve my project objectives and for always giving me useful knowledge and constant support.

I would also thank Dr. Ali Balaid for his assistance and guidance throughout my project, his help is highly appreciated.

Besides, I would like to thank my government especially the ministry of higher education in Yemen for the moral and financial support.

Last but not least, deepest gratitude goes to my beloved family members for their endless love, prayers and encouragement and to everyone who has been involved in this project even by coincidence.

ABSTRACT

Information security awareness is a concept that help to create a significant security policy aims to protect the privacy of Social networking site. Today social network users are connected to the internet service that assist all users to create user profile account. Moreover, Twitter can be recognized as one of the biggest and largest social network site. Twitter is one of the most significant social site that makes users to connect and make new friends around world. This research project is a platform that lies a crucial role to keep secure personal users' information. Nowadays, user self-disclosed is exposed in public on the social site without proper twitter privacy setting of the user account. In adding, this research project will help all the users of social networking site to be aware of all types of vulnerabilities behind the web base. Moreover, this project called privacy security awareness educate users to keep safe their twitter profile account. Accordingly, proposed twitter security privacy framework comprise four main sections components such as user security privacy, twitter privacy settings, security awareness for building relationship profile and user self-disclosed. Thus, this research project implied data analysis of qualitative survey of questionnaires which are distributed to the respondents. Besides, proposed information security awareness framework of twitter privacy among the students will provide a good security defense mechanism and at the same time used to rise a significant direction necessary to maintain a virtuous security policy among the social users. The analysis conducted has shown that most of the social networking site users are not aware of twitter privacy settings. Therefore, this research project conducted aimed to rise and protect the social networking site users from outsiders.

ABSTRAK

Kesedaran keselamatan maklumat merupakan suatu konsep yang boleh membantu mewujudkan dasar matlamat keselamatan yang ketara untuk melindungi privasi laman rangkaian sosial. Pengguna media sosial masa kini, disambungkan kepada perkhidmatan internet yang membantu pengguna-pengguna untuk mewujudkan akaun profil pengguna. Salah satu laman sosial yang popular ialah Twitter. Projek penyelidikan ini adalah satu platform yang memainkan peranan penting bagi memastikan maklumat peribadi pengguna selamat. Pada masa kini, maklumat pengguna adalah terdedah secara tebuka di laman sosial tanpa penetapan privasi Twitter akaun pengguna yang betul. Sebagai tambahan, projek penyelidikan ini dapat membantu para pengguna laman web rangkaian sosial untuk menyedari pelbagai jenis kelemahan disebalik web yang asas. Selain itu, projek ini dikenali sebagai kesedaran privasi keselamatan bagi mendidik pengguna untuk menjaga keselamatan akaun profil twitter mereka. Sehubungan dengan itu, rangka kerja privasi keselamatan Twitter yang dicadangkan terdiri daripada empat bahagian komponen utama seperti privasi keselamatan pengguna, tetapan privasi Twitter, kesedaran keselamatan untuk membina profil hubungan dan pengguna sendiri didedahkan. Oleh itu, projek penyelidikan ini menggunakan survey kualitatif analisis data iaitu borang soal selidik yang diedarkan kepada responden. Selain itu, kerangka kesedaran keselamatan maklumat privasi Twitter yang dicadangkan di kalangan pelajar akan menyediakan mekanisme pertahanan keselamatan yang baik dan pada masa yang sama digunakan untuk meningkatkan arah yang signifikan yang diperlukan untuk mengekalkan polici keselamatan di kalangan pengguna sosial. Analisis yang dijalankan membuktikan bahawa kebanyakan pengguna laman sosial tidak menyedari kepentingan tetapan privasi Twitter. Oleh itu, projek kajian ini dijalankan bertujuan untuk meningkatkan dan melindungi para pengguna laman rangkaian sosial daripada orang luar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

CIA	-	Confidentiality, Integrity and Availability
IS	-	Information Security
IT	-	Information Technology
NIST	-	National Institute of Science and Technology
RI	-	Relationship Initiation
SETA	-	Security Education Training Awareness
SNSs	-	Social Networks Sites
TPS	-	Twitter Privacy Settings
UPA	-	User Privacy Awareness
USD	-	User Self-disclosure

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Information security awareness and security management is an important aspect for information security system. Everybody in the world has his /her own sensitive data that have to be protected and taken care of. One of the challenges to information security is how to protect the CIA triangle which are (confidentiality, integrity and availability) of data against threats and attacks.

Social Networking sites are web-based services that which facilitate users creating a profile in public manner of enclose system. The main ideas behind the social networks are allowed a user by communicating with the relevant users to whom they intend to share various information. Social networks are used to assist users to navigate their connection list or even share a links among the users. In today world, the social networks sites are being recognised as one of the main technological event that use to connect millions of participants all over the world. Social network sites allow a user to share the content in the form of self-expression with other complementary users (Wuest, 2010).

With the recent years, online social networking are gradually increased in term of new types of social sites as well in term of registered membership. The latest

static has been shown that more than one hundred millions active users in both well-known social networking sites which are facebook.com and twitter.com (T. Huang et al, 2013). The main advantage behind two social networking sites is to set up a confidential connection between friends by knowing share private messages and confidential information. Further, those social networking sites help users knowing the status of users practically; this will assist the users to articulate opinions, education perspective and political views as well (A. Ahmad et al, 2010).

The social network site has been identified in 1997 where it helped users to create own profile and also register and add their friends. Before the creations of social network student are not allowed to have a privilege of creating their own profile and add their friends, they only surf the web via classmate.com as social network site. The way of social network are changing communication among individuals have received media attention in the past few years. People believe that social network sites has given them the ability to link and tie in a crisis and raise awareness of an issues worldwide.

Twitter is one of the most widely utilized social media websites, As of September 2010, there were 175 million registered users and daily initiated average of 95 million tweets (retrieved February 25, 2011). Twitter describes itself as "a real-time information network that connects its users to the latest information about what they find fascinating. Moreover, twitter is an extremely personal method of communication. Twitter's users must craft a unique experience that is, and thus create a unique experience that is specific to them and carefully choose whom they follow. It has been noticed that the current numbers of user who are joining twitter are extremely increased due to the ability of large amount of personal information that is publicity available.

The security management on social networking websites particularity in twitter has inspired many researchers due to large amount of information that users aimed to reveal in public manner. One of the main reasons of users information are revealed is due to the lack of user awareness. Most of the social network profiles are

mainly open access because the majority of the users are not aware the policy of how privacy setting can be used to disclosure the information of user profile.

This project will be mainly focused on the perfect security awareness of social networking site particularly twitter, further this project aims to strength factors of user privacy setting in twitter profile. This research will put much effort on highlighting the danger behind revealing the sensitive information which users used to post and share the personal confidential information through social networking site. The major security issues in social networking site where unknown users used to post information without the real users intentions, the posted information can be unwanted message where the legitimate users do not wish the message to be posted, therefore, the security awareness of privacy setting is more crucial on social networking site (twitter). Users used to post and share personal information via social networking site is due to the lack of users' security awareness.

1.2 Problem Background

Twitter was initiated in early march 2006 by person named jack Dorsey and officially launched in early July 2006. It began as a platform for the users to send and read messages, the registered users will be able to read and post the messages as well. The users can access through the website as it's an open social networking site. This service called twitter has gradually become more popular, barely more than 100 million of registered users can post roughly 340 million of tweets daily due to his open access any person can use to create his own profile that makes to reveal the users privacy information in public manner (Kumar, 2013).

Nowadays, it has been found that users of twitter social networking site has been rapidly increased over last few years, unfortunately, the rapid increment of the users made to reveal their confidential personal information to the public due to

security awareness, the exposed sensitive information in to the public such as phone number, email address as well as location, therefore, publically revealing the sensitive information through social networking site become of the major issues (Verma, 2013).

Twitter security setting are generally open access visibility, the researchers have found that many users are not given much care about their security setting which are more useful and further they did not even know that their security are being manipulated by third parties (Heinz, 2015). As security setting left with careless which made it the issues of security setting in social networking site getting bigger even reveal much disclosed information of the users to the public. It's much essential that the protection of users' privacy in SNS will be considered as a first priority concern in social media.

As a micro-blogging and social network service Twitter is one amongst the popular sites that allow people and offers them huge opportunity to share tweets, each tweet consist of 140 characters in length. Twitter had over 50 million unique users, as of September 2009 (Moore, 2009). While Twitter permits users to share information among friends or "followers", the default privacy setting on Twitter is that all tweets are public, which means that is, anyone who signs up for Twitter may see those information or search for them. Moreover, tweets could be posted to a public timeline website which showcases the most recent twenty tweets (Fang, 2010).

Twitter users went beyond security settings which makes everything public specially in regards of default setting of the system, as mentioned earlier most of the users are exposed to dangers such solicitation, cyber-bulling and harassment to act may lead to a severe security issues (N.Sadeh, 2012) . It has been found that some users have experienced defamation which results for creating accurate account to intimate specific people by tagging posting inaccurate information concerning supplementary users in order to enhance and damage their friendship or dignity (Nick Hajli, 2014). Moreover, impersonation is additionally used to manipulate

others revealing their security information and images in online social networking site.

Sharing other kind of personal information on Twitter, Besides personally identifiable information, could be taken as an advantage of placing people at risk For instance, in June 2009 Israel Hyman, an Arizona-based video podcaster, tweeted that he was looking forward to his family vacation to Saint Louis where they would be visiting family friends for the week. Once, they had safely arrived in Missouri, He tweeted again. Several thousands of dollars of computer and video equipment has been stolen from their house, the moment they were away (Van Grove, 2009).

Much research has done in the way where much people used to share personal information about them by online and also broadcast their privacy concern in the public manners that leaded to major issues about revealing the sensitive information to the third party and it results as security breaches (S.Counts, 2012). Moreover, research has demonstrated that users used to disclose more personal information via online experimental settings, do not only users willingly self-disclose online experimental settings but often use to disclose personal identifiable information via online website. Generally, twitter is been classified as a complete public system platform which generate a path for exploring privacy leakage on the environment of twitter privacy settings (Wang, 2014).

It is obvious that most of the twitter users like students had a mindful awareness regarding the issues of privacy setting in social networking site. Twitter users have a reduced amount of reactive to the social networking site on security setting even though they have given with an advance application of security settings. Therefore, the primary goal of this project is get to know and identify security issues and challenge, further to describe the issue that forces the security awareness on twitter users. In addition, this project research aims to represent the issues which affect the students in term of security policy on twitter privacy setting concern. This will help to identify the degree levels of security awareness in both undergraduate

and postgraduate students in order to determine when there is any case of a momentous differences of security awareness levels instituted.

1.3 Problem Statement

With the rapidly increasing of internet usage Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing.

Social networking site have gradually shown a major attention as frequent registered membership has extremely increased nowadays. The control of privacy security is the main concern in social networking site, therefore, much effort of security for the users of twitter is the more crucial since large amount of security must be protected such as surrounding users' profiles, making an entertainment among the users, discussion on political sight, sharing private information and pictures and messages.

Nowadays, most of the social networking site users used to reveal confidential information due to the lack of knowledge on twitter security privacy settings; this will lead to the security breaches and brings a variety of dangers for the individuals who are frequently using twitter. The main factors behind lack of security awareness on privacy security settings brings those dangers which are as follows, spamming, identity theft, embarrassment, hackers, blackmail, revealing sensitive information to the third party (Abeer et al, 2016). Therefore, most of the issues raised on twitters are due to the breaks of security privacy settings which are not given much care by the most social networking users. Thus, it's much crucial to imply and propose a best solution for protecting user's information and also taking

enough consideration to raise the extent level of users' awareness on privacy settings security concern.

1.4   Research Questions

The Research Questions for this study are defined as follow:

i.   What are the types of personal sensitive information which students use to reveal on their profile on twitter?

ii.   What is the suitable conceptual framework that addresses the use of security awareness on twitter privacy settings?

iii. How to validate the proposed information security awareness framework for enhancing security privacy among twitter users?

1.5   Objectives

The objectives of this project are mentioned as follow:

i.   To investigate types of information that student commonly uses to post on the social networking site Twitter.

ii.   To propose a conceptual security awareness framework for security privacy of Twitter social networking site among the students.

iii. To evaluate and validate the proposed security awareness conceptual framework by using of survey method.

1.6   Scope of Study

    i.   This project will be focused on the use of twitter security awareness on privacy settings, the scope only limited on both postgraduate and undergraduate students of UTM Johor campus.

   ii.   This project will point up the process of twitter user security awareness on privacy setting for university Technology Malaysia (UTM) enrolling students of postgraduate and undergraduate.

  iii.   This project will be focused on the security awareness of twitter users for their confidential information

1.7   Aim of the project

       The aim of this project is to keep safe UTM students information by putting much effort to educate users to protect the use of privacy settings.

1.8   Significance of the Project

    i.   This project shows the importance of how students of Universiti Teknologi Malaysia (UTM) should use of security safety on twitter by reducing the possibility of dangers and minimizing the impact of revealing their confidential information in public manner.

   ii.   The proposed conceptual framework of user security awareness on privacy settings will facilitate students to understand the use of twitter security privacy policy by implementing actions to avoid and lesson the dangers.

REFERENCES

A. Obiniyi, O. N. O., P. Obiniyi. <Social Network and Security Issues_ Mitigating Threat through Reliable Security Model 2014.pdf>.

A. Monroy-Hern´andez, E. Kiciman, D. Boyd, and S. Counts, "Narcotweets: Social Media in Wartime." in *ICWSM*, 2012.

Abdulhamid, S. M., Ahmad, S., Waziri, V. O., and Jibril, F. N. (2014). Privacy and national security issues in social networks: The challenges. *arXiv preprint arXiv:1402.3301*.

Abeer, A.-M., Hassan, M., and Nada, A.-S. (2016). Security Issues in Social Networking Sites. *International Journal of Applied Engineering Research, 11*(12), 7672-7675.

AlSagri, H. S., and AlAboodi, S. S. (2015). *Privacy awareness of online social networking in Saudi Arabia.* Paper presented at the Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on, 1-6.

Almakrami, H. A. A. (2015). Online self-disclosure across cultures: A study of Facebook use in Saudi Arabia and Australia.

A. Ahmad et al., "Information Leaking through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," *Conference proceeding of the 8th Australian Information Security Management Conference*, Edith Cowan University, Perth Western Australia, 30 November 2010.

Baatarjav, E.-A., Amin, A., Dantu, R., and Gupta, N. K. (2010). *Are you my friend? [Twitter response estimator].* Paper presented at the 2010 7th IEEE Consumer Communications and Networking Conference, 1-5.

Beebe, L. H. (2007). What can we learn from pilot studies? *Perspectives in psychiatric care, 43*(4), 213-218.

Cavoukian, A. (2009). Privacy by design... Take the challenge. Information and Privacy Commissioner of Ontario: Canada.

Chaudhary, M., and Kumar, H. (2015). *Challenges in protecting personnel information in social network space.* Paper presented at the Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on, 99-104.

Chen, X., and Shi, S. (2009). *A literature review of privacy research on social network sites.* Paper presented at the 2009 International Conference on Multimedia Information Networking and Security, 93-97.

C. Wüest, "The Risks of Social Networking, " *Symantec,* vol. I, p. 32, 2010.

Daehnhardt, E., Taylor, N. K., and Jing, Y. (2015). *Usage and Consequences of Privacy Settings in Microblogs.* Paper presented at the Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 667-674.

Daubert, J., Böck, L., Kikirasy, P., Mühlhäuser, M., and Fischer, M. (2014). *Twitterize: Anonymous Micro-Blogging.* Paper presented at the 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), 817-823.

De Cristofaro, E., Soriente, C., Tsudik, G., and Williams, A. (2012). *Hummingbird: Privacy at the time of twitter.* Paper presented at the 2012 IEEE Symposium on Security and Privacy, 285-299.

DiMicco, J. M., and Millen, D. R. (2007). *Identity management: multiple presentations of self in facebook.* Paper presented at the Proceedings of the 2007 international ACM conference on Supporting group work, 383-386.

Durahim, A. O., and Coşkun, M. (2015). # iamhappybecause: Gross National Happiness through Twitter analysis and big data. *Technological Forecasting and Social Change, 99,* 92-105.

D. K. K. Akriti Verma, "Privacy and Security: Online Social Networking, " *International Journal of Advanced Computer Research,* vol. III, no. 8, p. 7, 2013.

Dwyer, C., Hiltz, S., and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

E, A., x0Ef, meur, Gambs, S., and Ho, A. (2009, 24-28 May 2009). UPP: User Privacy Policy for Social Networking Sites. Paper presented at the Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on, 267-272.

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

Faghani, M. R., and Saidi, H. (2009). *Malware propagation in Online Social Networks*. Paper presented at the MALWARE, 8-14.

Furnell, S., and Phippen, A. (2012). Online privacy: a matter of policy? Computer Fraud & Security, 2012(8), 12-18.

Fodeman, D., and Monroe, M. (2009). The impact of Facebook on our students. Teacher Librarian, 36(5), 36.

Gawale, N. S., and Patil, N. N. (2015). *Implementation of a system to detect malicious URLs for Twitter users*. Paper presented at the Pervasive Computing (ICPC), 2015 International Conference on, 1-5.

Gayathri, K., Thomas, T., and Jayasudha, J. (2012). Security issues of media sharing in social cloud. *Procedia Engineering, 38*, 3806-3815.

Gu, L. L., Skierkowski, D., Florin, P., Friend, K., and Yi, Y. (2016). Facebook, Twitter, & Qr codes: An exploratory trial examining the feasibility of social media mechanisms for sample recruitment. *Computers in Human Behavior, 60*, 86-96.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Editorial-partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. Long Range Planning, 46(1-2), 1-12.

Hinson, G. (2010). Industrial Espionage. *NoticeBored Newsletter*, 1-7.

Hittleman, D., & Simon, A. (2002). Interpreting educational research: An introduction for consumers of research Upper Saddle River, NJ: Merrill. Education LB1028. H, 537.

Hua, W., and Zhang, Y. (2013). *Threshold and associative based classification for social spam profile detection on twitter*. Paper presented at the Semantics,

Knowledge and Grids (SKG), 2013 Ninth International Conference on, 113-120.

J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh, "Who's viewed you?: the impact of feedback in a mobile location-sharing application," in *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems*. New York, NY, USA: ACM, 2009, pp. 2003–2012.

Khan, Z. C., and Mashiane, T. (2014). *An analysis of Facebook's graph search*. Paper presented at the 2014 Information Security for South Africa, 1-8.

Kumar, A., Gupta, S. K., Rai, A. K., and Sinha, S. (2013). Social networking sites and their security issues. *International Journal of Scientific and Research Publications, 3*(4), 1-5.

K. L. Lujun Fang, "Privacy Wizards for Social Networking Sites, " *Raleigh,* p. 10, 2010

Mahmood, S. (2012). *New privacy threats for Facebook and Twitter users.* Paper presented at the P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2012 Seventh International Conference on, 164-169.

Mbanaso, U., Dandaura, E., Ezeh, G., and Iwuchukwu, U. (2015). *The use of social networking service among Nigerian youths between ages 16 and 25 years.* Paper presented at the Cyberspace (CYBER-Abuja), 2015 International Conference on, 14-21.

Micro, T. (2012). Spear-phishing email: Most favored apt attack bait. *Trend Micro,* http://www. trendmicro. com. au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait. pdf (accessed 1 October 2014).

Mikal, J., Hurst, S., and Conway, M. (2016). Ethical issues in using Twitter for population-level depression monitoring: a qualitative study. *BMC medical ethics, 17*(1), 1.

Mollett, A., Moran, D., and Dunleavy, P. (2011). Using Twitter in university research, teaching and impact activities.

Molok, N. N. A., Ali, A. M., Talib, S., and Mahmud, M. (2014). *Information security awareness through the use of social media.* Paper presented at the

Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on, 1-6.

Moore, R. J. (2009, October 5). Twitter data analysis: An investor's perspective. Retrieved November 1, 2009, from http://www.techcrunch.com/2009/10/05/twitter-data-analysisan- investors-perspective/.

Musial, K., and Kazienko, P. (2013). Social networks on the internet. *World Wide Web, 16*(1), 31-72.

Nagy, J., and Pecho, P. (2009). *Social networks security.* Paper presented at the 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 321-325.

Najaflou, Y., Jedari, B., Xia, F., Yang, L. T., and Obaidat, M. S. (2015). Safety challenges and solutions in mobile social networks. IEEE Systems Journal, 9(3), 834-854.

Nguyen, N. P., Xuan, Y., and Thai, M. T. (2010). *A novel method for worm containment on dynamic social networks.* Paper presented at the Military Communications Conference, 2010-MILCOM 2010, 2180-2185.

Onuma, M., Kimura, A., and Mukawa, N. (2013). *Exploring social cognition related to privacy settings in SNS usage.* Paper presented at the Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on, 1077-1082.

P. S. S. V. S. P. Damera Vijay Kumar, "Security Issues in Social Networking, " *IJCSNS International Journal of Computer Science and Network 120 Security,* no. 6, p. 5, 2013.

Posey, C., Lowry, P. B., Roberts, T., and Ellis, S. (2009). Proposing the Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities. European Journal of Information Systems (EJIS), 19(2), 181-195.

R. Gross, A. Acquisti, and H. J. Heinz, III, "Information revelation and privacy in online social networks," in *WPES '05: Proceedings of the 2015 ACM workshop on Privacy in the electronic society.* New York, NY, USA: ACM, 2015, pp. 71–80.

S. A. O. W. N. J. Shafi'i M. Abdulhamid, "Privacy and National Security Issues in Social Networks: The Challenges., " *International Journal of the Computer, the Internet and Management,* vol. III, no. 19, p. 7, 2011.

Shariff, S. M., and Zhang, X. (2014). *A survey on deceptions in online social networks.* Paper presented at the Computer and Information Sciences (ICCOINS), 2014 International Conference on, 1-6.

Shen, H., and Li, Z. (2014). Leveraging social networks for effective spam filtering. *IEEE Transactions on Computers, 63*(11), 2743-2759.

Song, J., Lee, S., and Kim, J. (2016). Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata. *IEEE Transactions on Dependable and Secure Computing, 13*(3), 340-354.

Thakur, K., and Kumar, H. (2015). *Challenges in protecting personated information in cyber space.* Paper presented at the Emerging Trends in Networks and Computer Communications (ETNCC), 2015 International Conference on, 167-171.

T. Huang et al., "An Analysis of Socware Cascades in Online Social Networks," in *Conference proceedings of the International World Wide Web Conference,* Rio de Janeiro, Brazil, May 13-17, 2013.

Thomas, A., Sang, H., John, C., and Richard, M. (2005). A Study of the Reliability and Validity of the Felder-Soloman Index of Learning Styles. Paper presented at the American Society for Engineering Education Annual Conference & Exposition.

Tsan-sheng Hsu, Churn-Jung Liau and Da-Wei Wang, "A logical framework for privacy-preserving social network publication," Journal of Applied Logic, Vol 12, Issue 2, pp. 151–174, June 2014.

Tuunainen, V. K., Pitkänen, O., and Hovi, M. (2009). Users' awareness of privacy on online social networking sites-case Facebook. *Bled 2009 Proceedings,* 42.

Van Grove, E. (2009). Twitter your way to getting robbed. Retrieved October 19th, from http://mashable.com/2009/06/01/twitter-related-burglary/

Verma, A., Kshirsagar, D., and Khan, S. (2013). Privacy and security: Online social networking. *International Journal of Advanced Computer Research, 3*(8), 310-315.

X. L. Nick Hajli, "Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information, " *Springer Science +Business Media Dordrecht,* p. 111, 2014.

Zhang, W. (2015). *Privacy and security concern of online social networks from user perspective.* Paper presented at the 2015 International Conference on Information Systems Security and Privacy (ICISSP), 246-25.