# CONCEPTUAL MODEL FOR FACTORS AFFECTING TRUSTS OF SOFTWARE AS A SERVICE USAGE IN PUBLIC NETWORK

**HONG KIM SHENG**

**UNIVERSITI TEKNOLOGI MALAYSIA**

# CONCEPTUAL MODEL FOR FACTORS AFFECTING TRUSTS OF SOFTWARE AS A SERVICE USAGE IN PUBLIC NETWORK

**HONG KIM SHENG**

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

**Advanced Informatics School**
**Universiti Teknologi Malaysia**

**JANUARY 2017**

# ACKNOWLEDGEMENT

Firstly, a million thanks to my supervisor, Dr. Nurazean Maroop who provides me guidance, supervision and directions throughout the whole process of completing this research.

Besides, I would like to extend my gratitude to my wife that always provides me supports, cheering, encouragements and always be there through the good and bad times.

Also a big thanks to my parents, for supports and encouragement with their best wishes and give me advices when needed.

Finally, I would like to thanks everyone that helped me throughout this project and appreciated for all the helps and supports given throughout this project.

# ABSTRACT

Software as a service (SaaS) is a cloud computing model that are extensively adopted and being used every day in the growing technology era. SaaS has provided variety of functionalities and flexibilities to save time, cost and efforts on how people do and run their day to day work and tasks. Although SaaS provides opportunities and convenience, there are also a lot of security issues that still exists. There are voices of public users on online articles emphasizing about how dangerous it is for connecting to a public network. Given the nature that a public network is an open connection, hackers is able to sniff the packets and penetrate into public network with penetration tools such as Wireshark, Ettercap, Burp Suite and Network Miner. Man in the middle (MITM) attack tweak the data transit on network interface card to examine the network traffic protocols such as FTP, HTTP, TCP and UDP. The scarcity of security measures particularly for public networks is at its utmost concern on usage of SaaS in a public network. Therefore, in addressing to this problem, research is conducted to identify the significant factors namely performance risks, financial risks, privacy risks, overall risks, personal disposition, familiarity, perceived security, perceived privacy and strategic thinking. The results shown that perceived privacy and overall risks are the most positively correlated with 45% correlation out of nine examined factors. This study may assist the public network providers in designing network security policies with regards to the presence of SaaS usage in public network.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATION

| | | |
|---|---|---|
| CC | - | Cloud Computing |
| CSP | - | Cloud Service Provider |
| SaaS | - | Software as a Services |
| WiFi | - | Wireless Fidelity |
| CCTV | - | Closed Circuit Television |
| KMO | - | Kaiser-Mayer Olkin’s Measure |

# LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

This chapter presents a brief outline of the overall research on SaaS usage in public network. This chapter contains seven sections which initially starts with an overview of the research in section 1.1 and followed by findings on background of problems in section 1.2 and discussions of problem statement in section 1.3. Next, section 1.4 discussed about the research objective, followed by research questions in section 1.5. While section 1.6 discussed on the scope of study for this research and significance of study in section 1.7. Lastly, section 1.7 will end the chapter the chapter with a summary.

According to a study conducted by Cisco, (2015), cloud computing (CC) adoption has been accelerating over the years and cloud user has increasingly dependency to place their trusts towards third party cloud service providers (CSP) to hold and manage sensitive data on cloud platform (Cisco, 2015). In addition, Cisco, (2011) also reported that several issues such as control, security, reliability and quality is the main security issues over the cloud to secure the private and critical information in Information Computer Technology (ICT) implementation today (Cisco, 2011).

Cloud computing often offers opportunities but so do challenges. There are variety of security issue encountered in Cloud Computing as cloud computing platform is still in immature phase and opens the vulnerabilities to security threats and attacks (Hu and Bai, 2014). The usage of cloud computing has been widely used around the world especially Software as a Services (SaaS). Examples of SaaS provider that are widely used are Microsoft OneDrive, Dropbox and various Google applications such as Google Docs, Google Drive and Google Plus (Onwubiko, 2010).

## 1.2 Background of Problem

In the world of technology today, WiFi or known as Wireless Fidelity has become the fundamental of connectivity and it is used to establish a connection. Most of the time, devices are connected to company network when working and connected to public network when out of office. Due to the nature of public networks provides free WiFi in wireless state, the data are transmitted through an open space where the connection is more susceptible to attacks. Meghanathan, (2014) indicates that the threats occur when data is in transmitting from sender to receiver (Meghanathan, 2014). Man-in-the-middle is able to sniff the packets that are transmitted over the network using open-source software like Wireshark, Ettercap and NetworkMiner (Noor and Hassan, 2013). Meghanathan, (2014) further indicates that a packet sniffer is able to perform study on packet structures, monitor transmissions of network traffics, and analyse packet headers (Meghanathan, 2014).

As a result, data transmitted over the network may be subject to data leakage and privacy violation. According to recent survey conducted by Dell, (2016), shows that there are four out of five respondents are reluctant to store confidential data to public cloud services like Google Drive (Dell, 2016). It raises data privacy concerns due to public cloud is vulnerable to attacks and the connection are less protected over the data transmissions (Murray et al., 2015).

A study and analysis has been conducted on several online articles and users shows that public Wi-Fi user have limited knowledge on the risks when connected to the network. According to article on Tzvi, (2015), user namely Denys Skorbenko has responded that the devices has discovers unfamiliar access point and asked if it is safe to use it? Kaspersky, (2016) indicates that public Wi-Fi user must be aware that the connection are essentially insecure and user must remember that all devices are open to risks and must treat all connections with suspicion (Kaspersky, 2016). Meanwhile, user named Janine Stier responded in article by Arthor Baxter, (2015) indicating that "I just woke up to find that my PayPal username and password has been changed and a 300 plus charge was charged to the PayPal account", resulting from data leak when user uses Wi-Fi connections to perform PayPal transactions. While article by Jeff Ehling, (2015) indicates that hacker creates a network, inviting public users to join the rogue access point and attack them by retrieving any information user are accessing on the spoofed connections. Resulting into undesirable outcome such as data leakage on photo, videos, passwords and even financial data such as bank account number. Lastly, Priya Joshi, (2015) commented that user connected to public Wi-Fi are unaware that hacker is able to gain large amount of data over the communications. As a results, there is the need of individual security knowledge on security threats, attacks and situational awareness to mitigate security threats and attacks that are prevailing over the network. Please refer to Appendix A for articles and public responses towards articles and threats.

Based on the fact that SaaS usage transmits the data remotely from cloud between cloud storage and cloud service user, there are possibilities that the connection will be intercepted or eavesdrop. According to Onwubiko, (2010), privacy issue exists in cloud

computing as personal information as well as business related confidential data are stored remotely on cloud platform (Onwubiko, 2010).

Murray et al., (2015) discussed that the effort of ensuring data privacy is required as sensitive data that will be transmitted by SaaS application are stored remotely (Murray et al., 2015). Data transmitted between cloud user and CSP are opened to web application security challenges such as data breach and data vulnerability (Murray et al., 2015). Kaur and Kaur, (2015) and Lai and Leu, (2015) stressed that the data sent or received between cloud user and CSP can be easily retrieved and eavesdrop by man-in-the-middle from user on cloud end (Kaur and Kaur, 2015), (Lai and Leu, 2015). As a result, data vulnerabilities and potential privacy issue such as data loss and data leakage will occur.

In addition, Lai and Leu, (2015) discussed that the security events detection on the application programming interface (API) have the controls over cloud computing services (Lai and Leu, 2015). API are used in cloud computing applications to meet their objective on resource sharing. Lai and Leu, (2015) added that Cloud application API do contains many security vulnerabilities such as system authorization and identity validation issues (Lai and Leu, 2015). According to, Hande and Mane, (2015), cloud user have limited control over the data, applications and resources stored in cloud computing platform and made available when the data is requested by cloud service users (Hande and Mane, 2015). Cloud users need to rely on CSP to ensure the data privacy and security. Hande and Mane, (2015) also stressed that public cloud are often more vulnerable to malicious threats and security attacks due to lesser protections on public cloud where both public and private cloud charges different costs to provide different cloud features such as security, storage limit, speed, flexibility, and data reliability of the services (Murray et al., 2015). On July 2012, Dropbox (2012) officially announced and apologize for security breaches. Dropbox, (2012) reported that small amount of Dropbox username and password were stolen from other websites that are used to login Dropbox account. This security breaches has caused small number of Dropbox account containing customer project document with email address are leaked. As a result, all affected email address receives spam messages (Dropbox, 2012).

## 1.3 Problem Statement

Software as a Service (SaaS) user uses public networks to connect to cloud for data transmission over the network. This opens the vulnerability to different security risks and threats that may compromise data confidentiality on a public network due to public network is an open access network that can be easily accessed by anyone. A recent survey conducted by Kaskersky, (2016) shows 70% of tablet and 53% of smartphone user connects their devices to public WiFi hotspots. Data sent over public network can be easily intercepted and may leads to data privacy risks and financial risks on a shared open public network access. Therefore, perceived behavioural on tendency to protect data privacy is needed to mitigate the privacy risks and financial risks on usage of SaaS in a public network. An evaluated model is proposed to examine the mitigation methods from risks and human perspective and ultimately helps to mitigate the risks of being attacked when using SaaS in a public network.

## 1.4 Research Question

Several research questions have been identified to derive the research objective. In conclusion, this study is to investigate several questions that arise on factors affecting trusts of SaaS usage in a public network:

i. Why the usage of software as a service in public network is vulnerable to security attacks?

ii. How to design the proposed conceptual model for security measures on usage of Software as a Service (SaaS) in public network?

iii. How designed conceptual model can be evaluated for security measures on usage of Software as a Service (SaaS) in public network?

## 1.5 Research Objective

After the studies of this research has been completed, these three objective must be achieved as follow:

i. To identify security threats on usage of Software as a Service (SaaS) in public network.

ii. To develop a conceptual model usage of Software as a Service (SaaS) in public network.

iii. To evaluate the proposed conceptual model for security measures on usage of Software as a Service (SaaS) in public network.

## 1.6 Scope of Study

Scope of study are highlighted as limitation in this research as follow:

i. The scope of study is individual SaaS user in a public network. E.g. shopping centres, airport, university and public restaurant.

ii. Target audience for questionnaire in this research will be teenagers from age 18 onwards due to sensitive data and belonging often held by adult and teenagers that are already working.

iii. Data collection methodology will be mixed mode method with combination of questionnaire and interview.

iv. Data collected will be analysed using SPSS software version. 23.0.

## 1.7 Significance of Study

A discussion on significance of study will be covered in this section on both theoretical and practical contributions. The rationale of this study aims to provide potential benefits and its overall influence and impact on the study.

### 1.7.1 Theoretical Contribution

In this research, theory model from various researchers will be examined and analysed. These models and approach will be consolidated to develop a conceptual model to identify factors affecting trusts on usage of SaaS in public network.

### 1.7.2 Practical Contribution

As cloud computing has been widely used as a trend to connect and store data remotely, this research will identify the security issues on usage of SaaS in public network. It could help to raise security awareness among public network users This research helps to assist cloud users how to protect the sensitive information and data better over the cloud.

## 1.8 Summary

This section covers the overview of cloud computing architecture and the problem statements is identified when cloud users connects to a public network for cloud service usage. The vulnerability is exposed when the network connection is shared among the publics as the security of the connected public network are connected at its own risks. Thus, a conceptual model will be proposed in this research to mitigate the security risks on the usage of cloud computing in a public network.

# REFERENCES

Abolfazli, S., Sanaei, Z., Tabassi, A., Rosen, S., Gani, A., Khan, S.U., 2015. Cloud Adoption in Malaysia: Trends, Opportunities, and Challenges. Cloud Comput. IEEE 2, 60–68.

Aime, M.D., Calandriello, G., Lioy, A., 2007. Dependability in wireless networks: Can we rely on WiFi? Secur. Priv. IEEE 5, 23–29.

Alan Pearson, (2014), How Do I Know If My VPN Is Trustworthy? Retrieved 22 February, 2016, from http://lifehacker.com/how-do-i-know-if-my-vpn-is-trustworthy-508866499

Arthur Baxter, (2015). How to stop hackers from stealing your information on public Wi-Fi. Retrieved 23 February, 2016, from http://thenextweb.com/insider/2015/08/08/how-to-stop-hackers-from-stealing-your-information-on-public-wi-fi/#gref

Badger, L., Grance, T., Patt-Corner, R., Voas, J., 2011. Draft cloud computing synopsis and recommendations. NIST Spec. Publ. 800, 146.

Bird, D.K., 2009. The use of questionnaires for acquiring information on public perception of natural hazards and risk mitigation–a review of current knowledge and practice. Nat. Hazards Earth Syst. Sci. 9, 1307–1325.

Cameron, R., 2009. A sequential mixed model research design: Design, analytical and display issues. Int. J. Mult. Res. Approaches 3, 140–152.

Cheng, N., Wang, X., Cheng, W., Mohapatra, P., Seneviratne, A., 2013. Characterizing privacy leakage of public WiFi networks for users on travel, in: INFOCOM, 2013 Proceedings IEEE. IEEE, pp. 2769–2777.

Chris Hoffman, (2014), Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites. Retrieved 26 February, 2016, from http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites

Cisco. (2011). Cloud Computing Concerns in the Public Sector, How Government, Education, and Healthcare Organizations Are Assessing and Overcoming Barriers to Cloud Deployments. Retrieved 20 March, 2016, from http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pscloudconcerns.pdf

Cisco. (2015). Cloud Security - Trust Cisco to Protect Your Data. Retrieved 20 February, 2016, from http://www.cisco.com/c/dam/en/us/solutions/collateral/trends/cloud/cloud-security.pdf

Coakes, S. J., Steed, L., and Ong, C. (2009). Analysis without Anguish: SPSS Version 16.0 for Windows. John Wiley and Sons, Australia.

Cohen, J (1988) Statistical power analysis for the behavioral sciences (2nd ed.). Hillsdale, NJ: Erlbaum.

De Vaus, D.A., de Vaus, D., 2001. Research design in social research. Sage.

Delice, A., 2010. The Sampling Issues in Quantitative Research. Educ. Sci. Theory Pract. 10, 2001–2018.

Dell. (2016). 2016 Dell Data Security Survey. Retrieved 02 March, 2016, from http://futurereadyworkforce.dell.com/wp-content/uploads/2016/03/DDS_Report_V4.pdf

Dhami, A., Agarwal, N., Chakraborty, T.K., Singh, B.P., Minj, J., 2013. Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook, in: Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, pp. 465–469.

Dropbox. (2012). Dropbox Blog - Security update and new features. Retrieved 18 February, 2016, from https://blogs.dropbox.com/dropbox/2012/07/security-update-new-features/

Dropbox. (2016). What is LAN sync? Retrieved 18 February, 2016, from https://www.dropbox.com/en/help/137

Evans, J. D. (1996). Straightforward Statistics for the Behavioral Sciences. Pacific Grove, CA: Brooks/Cole Publishing

Frank Ohlhorst, (2014) Minimizing the threats of public Wi-Fi and avoiding evil twins. Retrieved 22 February, 2016, from http://www.techrepublic.com/article/minimizing-the-threats-of-public-wi-fi-and-avoiding-evil-twins

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston: Allyn & Bacon.

George, D., & Mallery, M. (2010). SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 update (10th ed.) Boston: Pearson.

Hair, J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis (7th ed.). Upper saddle River, New Jersey: Pearson Education International.

Hamlen, K., Kantarcioglu, M., Khan, L., Thuraisingham, B., 2010. Security Issues for Cloud Computing: Int. J. Inf. Secur. Priv. 4, 36–48. doi:10.4018/jisp.2010040103

Hande, S.A., Mane, S.B., 2015. An analysis on data Accountability and Security in cloud, in: Industrial Instrumentation and Control (ICIC), 2015 International Conference on. IEEE, pp. 713–717.

Harbach, M., Fahl, S., Brenner, M., Muders, T., Smith, M., 2012. Towards privacy-preserving access control with hidden policies, hidden credentials and hidden decisions, in: 2012 Tenth Annual International Conference on Privacy, Security and Trust (PST). Presented at the 2012 Tenth Annual International Conference on Privacy, Security and Trust (PST), pp. 17–24. doi:10.1109/PST.2012.6297915

Hole, K.J., Dyrnes, E., Thorsheim, P., 2005. Securing wi-fi networks. Computer 38, 28–34.

Huang, L., Shen, Y., Zhang, G., Luo, H., 2015. Information System Security Risk Assessment Based on Multidimensional Cloud Model and The Entropy Theory. IEEE Computer Society, pp. 11–14.

Hu, Y., Bai, G., 2014. A Systematic Literature Review of Cloud Computing in Ehealth. Health Inform. - Int. J. 3, 11–20. doi:10.5121/hiij.2014.3402

Jeff Ehling, (2015). Hackers Set Up Fake Wi-Fi Hotspots To Steal Your Information. Retrieved 19 February, 2016, from http://abc13.com/technology/hackers-set-up-fake-wi-fi-hotspots-to-steal-your-information/835223

John E DunnAugust, (2015), Are public Wi-Fi hotspots a security risk? Security risks of using public Wi-Fi explained. Retrieved 24 February, 2016, from http://www.computerworlduk.com/security/are-public-wi-fi-hotspots-really-major-security-risk-3623447

Kaur, R., Kaur, J., 2015. Cloud computing security issues and its solution: A review, in: Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on. IEEE, pp. 1198–1200.

Kaspersky, (2016), Public Wi-Fi Security. Retrieved 25 February, 2016, from http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi#.VyqLU4R97IU

Kaspersky, (2016), How to Avoid Public WiFi Security Risks. Retrieved 25 February, 2016, from http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks#.VyqLSoR97IU

Krejcie, R.V., Morgan, D.W., 1970. Determining Sample Size for Research Activities. Educ. Psychol. Meas. 30, 607–610. doi:10.1177/001316447003000308

Kumar, A., 2014. A study on Cloud computing in libraries. ASIAN J. Multidiscip. Stud. 2.

Lai, S.-T., Leu, F.-Y., 2015. A Security Threats Measurement Model for Reducing Cloud Computing Security Risk. IEEE, pp. 414–419. doi:10.1109/IMIS.2015.64

Larry Higgs, (2013), Free Wi-Fi? Beware of security risks. Retrieved 23 February, 2016, from http://www.usatoday.com/story/tech/2013/07/01/free-wi-fi-risks/2480167

Lexy Savvides, (2015). Staying safe on public Wi-Fi. Retrieved 22 February, 2016, from http://www.cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi

Li, W., Wan, H., Ren, X., Li, S., 2012. A Refined RBAC Model for Cloud Computing, in: 2012 IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS). Presented at the 2012 IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS), pp. 43–48. doi:10.1109/ICIS.2012.13

Li, X., Zhao, X., 2013. Survey on Access Control Model in Cloud Computing Environment, in: 2013 International Conference on Cloud Computing and Big Data (CloudCom-Asia). Presented at the 2013 International Conference on Cloud Computing and Big Data (CloudCom-Asia), pp. 340–345. doi:10.1109/CLOUDCOM-ASIA.2013.103

Lourida, K., Mouhtaropoulos, A., Vakaloudis, A., 2013. Assessing database and network threats in traditional and cloud computing. Int. J. Cyber-Secur. Digit. Forensics IJCSDF 2, 1–17.

Luis Corrons, (2015), Public WiFi networks. Are they safe? Retrieved 23 February, 2016, from http://www.pandasecurity.com/mediacenter/security/public-wifi-networks-safe

Luo, X., Li, H., Zhang, J., Shim, J.P., 2010. Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decis. Support Syst. 49, 222–234. doi:10.1016/j.dss.2010.02.008

Malaysia. Unit Perancang Ekonomi (Ed.), 2015. Eleventh Malaysia plan, 2016-2020: anchoring growth on people. Economic Planning Unit, Prime Minister's Department, Putrajaya, Malaysia.

Meghanathan, N., 2014. A Tutorial on Network Security: Attacks and Controls. ArXiv Prepr. ArXiv14126017.

Miller, M., 2008. Cloud computing: Web-based applications that change the way you work and collaborate online. Que, Indianapolis, Ind.

Murray, A., Begna, G., Nwafor, E., Blackstone, J., Patterson, W., 2015. Cloud Service Security & Application Vulnerability, in: SoutheastCon 2015. IEEE, pp. 1–8.

Noor, M.M., Hassan, W.H., 2013. Wireless networks: developments, threats and countermeasures. Int. J. Digit. Inf. Wirel. Commun. IJDIWC 3, 125–140.

Onwubiko, C., 2010. Security Issues to Cloud Computing, in: Antonopoulos, N., Gillam, L. (Eds.), Cloud Computing. Springer London, London, pp. 271–288.

ORG, W.B., 2011. MALWARE RISKS AND MITIGATION REPORT.

Priya Joshi, (2015). Free Wi-Fi at public places: Pros and Cons. Retrieved 21 February, 2015, from http://www.careerride.com/view.aspx?id=22418

Rightscale. (2016). STATE OF THE CLOUD REPORT - Hybrid Cloud Adoption Ramps as Cloud Users and Cloud Providers Mature. Retrieved 08 March, 2016, from http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf

Rockmann, R., Weeger, A., Gewald, H., 2015. IT Capabilities and Organizational Utilization of Public Cloud Computing.

Sabahi, F., 2011. Cloud computing security threats and responses, in: Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, pp. 245–249.

Suderman, J., 2015. Contexts for trust in cloud-based services: An historical perspective, in: 2015 Digital Heritage. IEEE, pp. 367–370.

Sekaran, U. & Bougie, R., (2009). Research Method for Business 5th ed., John Wiley and Son Ltd.

Teddlie, C., Yu, F., 2007. Mixed Methods Sampling: A Typology With Examples. J. Mix. Methods Res. 1, 77–100. doi:10.1177/2345678906292430

Tzvi Kasten, Andriy Okhrimets and Artem Kharchenko, (2015). Is it safe to use public Wi-Fi networks? Retrieved 21 February, 2016, from http://www.networkworld.com/article/2904439/wi-fi/is-it-safe-to-use-public-wi-fi-networks.html

Wyld, D.C., 2010. Risk in the clouds?: Security issues facing government use of cloud computing, in: Innovations in Computing Sciences and Software Engineering. Springer, pp. 7–12.

Yang, S.-J., Lai, P.-C., Lin, J., 2013. Design Role-Based Multi-tenancy Access Control Scheme for Cloud Services, in: 2013 International Symposium on Biometrics and Security Technologies (ISBAST). Presented at the 2013 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 273–279. doi:10.1109/ISBAST.2013.48

Zhou, T., 2012a. Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. J. Electron. Commer. Res. 13, 135.