ENHANCED ANALYSIS OF KIPPO-HONEYPOT IN CLOUD

MOHAMMED ABDULLAH OMAR ALZUBAIDI

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

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2015

I dedicate this project to my lovely and amazing parents for their support, prayers and courage to keep going

To my siblings who are part of this successful work

ACKNOWLEDGEMENT

First and foremost, I thank Allah for being with me at all time and ease for me all the hardships and troubles I met during this work. I also would like to express heartfelt gratitude to my supervisor **Dr. Anazida Bt Zainal** for her constant support. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor.

ABSTRACT

Cloud computing is a promising technology for business and individuals. Cloud computing allows companies to focus more on their core business and leave the IT management responsibilities to cloud vendors. However, not many companies have considered shifting their business to the cloud due to security issues that cloud computing has. Nevertheless, many researchers have suggested methods to mitigate those attacks, some have proposed methods to extract the features of attacks and then use them to help in detecting future attacks. This project aims to support the existing attacks analysis methods to learn more about attack patterns and attackers' behavior, which will contribute to building more reliable attack mitigation techniques and tools. The proposed system aims to enhance the analysis of honeypot data collected from attacks in cloud by implementing new data analysis tools that can extract more data from the honeypot database and correlate them to produce richer data analysis visualization, as compared to previous systems like Honeypots in the Cloud system. The analysis result is more attack informative and gives better understanding of attacks to the system administrator.

ABSTRAK

Pengkomputeran awan adalah teknologi berpotensi untuk perniagaan dan individu. Pengkomputeran awan membolehkan syarikat-syarikat memfokuskan pada perniagaan teras mereka dan meninggalkan tanggungjawab pengurusan IT kepada vendor awan. Walau bagaimanapun, tidak banyak syarikat telah mempertimbangkan umtuk beralih perniagaan mereka ke pengkomputeran awan kerana isu-isu keselamatan yang ada padanya. Walau bagaimanapun, ramai penyelidik telah mencadangkan kaedah untuk mengurangkan serangan, ada yang mencadangkan kaedah untuk mendapatkan ciri-ciri serangan dan kemudian menggunakan ciri-ciri serangan ini untuk membantu dalam mengesan serangan pada masa depan. Projek ini bertujuan untuk menambahbaik kaedah analisis serangan sedia ada untuk mengetahui lebih mendalam tentang corak serangan dan tingkah laku penyerang. Pengetahuan tentang corak serangan ini bakal menyumbang kepada pembinaan teknik serta alat menahan serangan yang lebih baik. Sistem yang dicadangkan ini bertujuan untuk meningkatkan mutu analisis data serangan awan yang dikumpul oleh honeypot dengan melaksanakan alat analisis data yang baru, yang berupaya mengeluarkan lebih banyak data daripada pangkalan data honeypot dan mengaitkan mereka untuk menghasilkan analisis yang lebih baik, serta dapat menvisualisasi data jika dibandingkan dengan sistem sebelumnya seperti Honeypots dalam sistem awan Analisa yang terhasil adalah lebih berinformasi dan dapat memberikan kefahaman yang lebih baik kepada pengendali sistem

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AWS	-	Amazon Web Service
DDOS	-	Distributed Denial of Service
DOS	-	Denial of Service
EC2	-	Elastic Cloud Compute
HTTP	-	Hypertext Transfer Protocol
IaaS	-	Infrastructure as a Service
IDS	-	Intrusion Detection System
PaaS	-	Platform as a Service
SaaS	-	Security as a Service
SSH	-	Secure Shell
VPS	-	Virtual Private Server

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cloud computing includes allotted processing of data over a network, where a piece of application or software may run on numerous associated machines in the meantime. It particularly alludes to a single or a group computing hardware gadget/s usually alluded as a server that are linked through an interaction system such as, the Internet, an intranet, LAN or WAN. A person who has the privileges to access/use the server may benefit from the computing power of the server to run an application, store some data, or carry any kind of computing process of his/her preferences (wikipedia, 2014).

In the simplest terms, cloud computing refers to the usage of internet to access, process, store, and retrieve your data instead of using your-single- hard-drive and computer machine to do all the computing tasks (PC-Magazine, 2014). Cloud is just like a representation of the term internet See figure 1.1.

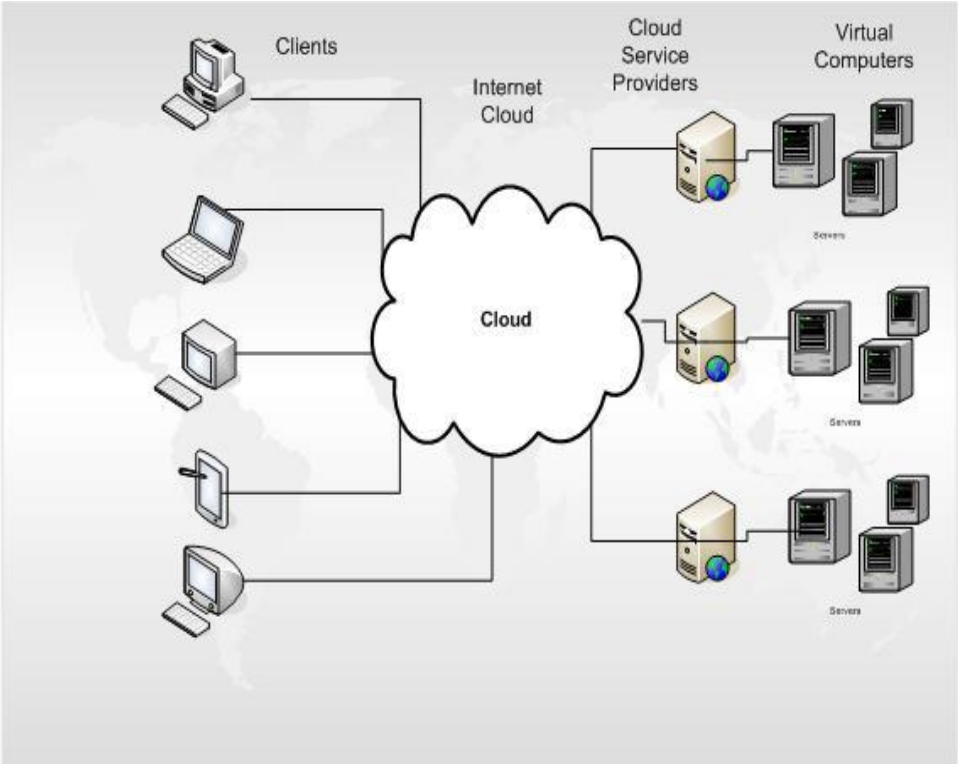

Figure 1.1 Cloud computing simple connection (GRIFFITH, 2013)

The borders between cloud computing and the "basic" local computing sometimes gets hazy. This is the result of cloud computing being integrated into many of the application in use today by people. Some software that is installed locally might in some ways have some links with cloud computing that users can't even notice (e.g Microsoft office 365). Or it could be utilizing the cloud for the storage of users' data like the Microsoft Skydirve. Besides these there are plenty of applications that utilize the cloud computing infrastructure to run the users' computing tasks or to send their data for storage and for retrieval see figure 2.1. Examples are:

- Google drive.
- Apple i Cloud.
- Amazon cloud drive.
- Dropbox.

Figure 1.2 cloud computing companies (Computing-Cloud-Storage, 2014)

Cloud computing comes with the concept of virtualization/multi-tenant, that is a single server owned by the cloud service provider can include hundreds thousands of data for many different subscribers. This multi-tenancy means a lot to attackers, gaining access to one server means the ability to access many users' data hosted at that exploited server (Tianfield, 2012).These concepts and other cloud computing concepts like outsourcing the computing building resources, and the external data warehousing widening the circle of the security issues (e.g. privacy) (Khalil *et al.*, 2014). However, according to (Chen and Zhao, 2012), despites the claims that are made by cloud providers regarding their tight security measurements security of the customers and their data is still in danger. Little and weak security countermeasures are currently implemented by those cloud providers, which provide insufficient security to the data hosted in the cloud. The year 2009 has witnessed many security breaches and accidents that had a deep impact on customers' data (Chen and Zhao, 2012).

Many researches have been done to improve the security of customers' data in the cloud. Cloud providers need to implement the tightest security rules and techniques that can convince their customers of the security level they-the customer-

can expect and make them satisfy about the level of protection of their data and private information. Countermeasures like IDSs, IPS, firewalls, and various cryptographic algorithms are being deployed by cloud service companies to their cloud infrastructures. However, the increase in the level and the frequency of attacks requires improvements and enhancements to be made to the existing security measurements. Adding new security techniques to the existing ones could also improve the security level of the cloud. For example the technology of honeypot can be integrated with current cloud security techniques to ensure better security.

Honeypot as a security technology, whose value reset in being explored, hijacked and/or tampered with. This technology does provide some level of prevention against security threats and hackers attacks; it works by luring attackers that they are facing a real system. This feeling gives the attacker the freedom to behave normally as if they are performing their malicious acts. For the honeypot owners this chance is like a zoologist studying the behaviors of animals in the wild, this would allow him-the system owner- to have a full and uninterrupted sight of how an attacker acts when attacking the system, what sort of information they are typically looking for and most importantly how they do the search (Noordin, 2004).

Data gathered by the honeypots systems can reveal much of information about the attacks and the attackers. The information can be utilized to improve the security measurements of the computing system (i.e cloud computing systems).

1.2 Problem Background

Moving the systems and IT management of the organization to the cloud is thought to be a step towards better security and data safety than hosting them on the premises of the organization. However, the reports made by various security firms rebuttal that thought (Barker, 2014).

According to the 2014 security report made by (Alert-Logic, 2014) the number of attacks targeted cloud is in a significant increase. The percentage of Brute Force attacks has risen from 30 to 44 percent. While the vulnerability scan has increased from 27 to 44 percent. Cross Site Scripting (XSS) made about 69 percent of blocked attacks at the end of 2012 according to (Infosecurity-Magazine, 2013). Moreover, DoS and its advanced version DDoS are among those threats that target the cloud. This attack is considered to be amongst the most serious attacks that a system would face (Kamal and Kaur, 2011), due to its impact in making the system irresponsive to its legitimate users and thus loses its value.

However, the use of defense appliances such as firewall to defeat DDoS is not effective approach of defense due to the position of the firewall (at the border of the network) which makes the firewall unable to detect the DDoS attacks once they exist on the network (Liu and Chen, 2011).Intrusion Detection Systems (i.e IDS) are very significant in cloud computing environment, for the detection of intrusions as cloud is very attractive to attackers and also due to the huge amount of processing made at the cloud and the amount of information stored there. (Lee *et al.*, 1998) Proposed a data mining framework for intrusion detection. Association rules and frequent periods that were computed from the audit data will be used for feature selection. These features will then be fed into a classifier to detect the intrusion. System and network logs are the source of the audit data used to find useful association rules or the frequent patterns. However, the limitation of this proposed framework is the lack of detecting new intrusions due to lack of knowledge about their patterns. (Lo *et al.*, 2010) suggested a framework to detect DDoS attacks by exchanging the alert information between IDSs in the same cloud computing region. In this framework IDSs will send out their alert information to other IDSs in the region to improve early detection and prevention of DDoS attacks. IDS system will compose of four parts: Intrusion detection to collect and analyses packets, alert clustering to define the danger level of those packets have not been identified as malicious packets by the intrusion detection component for improved detection, intrusion response is the third component of the system and functions to block bad packets and communicating alerts with other IDSs, last component is the cooperative operation and is used to test the trustworthiness of the alerts received by the IDS. When detecting a malicious

packet the IDS will drop that packet and send alert notifications to other IDS so that they can detect the malicious packet when arriving at their networks. The limitation of this proposed framework is that new attacks cannot be identified by the IDS due to lack of information about their patterns.

Moreover, Malware are amongst the big threats of today's internet it causes great damage to the system they attack. Signature based detection is one way of malware detection that uses the malware signature derived by analysing the malware instructions. However, a slight modification on the malware code can greatly help in avoiding detection (Murad *et al.*, 2010). Dynamic malware analysis is yet another way of malware detection. The dynamic analysis is done by executing the malware code to see how it would behave when it runs. Nevertheless, the huge number of new malware that requires automatic detection degrades the effectiveness of this method (Gandotra *et al.*, 2014).(Nataraj *et al.*, 2011) proposed an approach that uses image processing technique to classify the malware through visualization. However, this approach can be easily beaten because it uses global image based features.

Due to the wide scale of the cloud compare to the traditional IT environments, currently-traditional-attack defense mechanisms are not very effective (Chen and Zhao, 2012).With the rapid development of technology it is a must to ensure these mechanisms are able to handle new attacks. Development of these effective mechanisms rests on the attack patterns which these mechanisms have been fed with and are able to detect them when attacks strike. These patterns are the result of the analysis process of attacks. Therefore, improving the attack analysis techniques can be seen as the core of this whole process, and can lead to effective attack mitigation mechanisms.

Cloud security needs lots of researches to be conducted to enhance its effectiveness and efficiency in attacks defense. The infrastructure of cloud computing is changing rapidly. This fast change requires a frequent update to the security countermeasures and policies adopted in cloud at the same time matching the security level with the change of cloud behavior and the change on the type of

attacks (Khalil, *et al.*, 2014).The lack of enough knowledge about the patterns of the attacks as well as the behaviors of attackers is one of the prime reasons current defense mechanisms fail when facing the sophisticated types of attacks. Some security tools and services can significantly help the security community to learn more about the enemies of information systems and their malicious activities. The use of new tools or the adoption of new approach in the analysis process that is proved to be effective can be a great step towards more reliable attack mitigation mechanisms. For example, Honeypot is a security tool which is used to lure attackers and collect helpful information about them (Noordin, 2004) (e.g. attack source, tools used to perform the attack, and attackers IP address).

1.3 Problem Statement

Honeypot systems can have very large sets of data in their logs about the attacks they can detect and log. The sets can be used to study and learn about those attacks and the behavior of the attackers too. Performing data analysis over those sets helps to draw a picture that tells the system administrators about the attacks their system receive and about the attackers too. However, the analysis approaches used nowadays are not making a full use of these data sets and hence, the picture about these attacks is not complete. Still lots of useful and informative details can be extracted from the data sets.

1.4 Aim of the Project

The aim of this project is to extract attacks patterns by analyzing data collected about attacks targeted the system. A honeypot system will be used in cloud to collect these data and analysis tool (e.g Kippo-graph) will be used to perform the data analysis process. This will contribute to enhance and support the existing security of the cloud.

1.5 Objectives of the Project

1. To study the current approaches to analyze Kippo honeypot data logs, and explore the current SSH-brute force attack mitigation techniques.
2. To configure the cloud platform, the honeypot system and the analysis tool.
3. To perform the analysis over the collected data, present the enhanced analysis result and compare the result with a previous work

1.6 Project Scope

The scope that sets the boundaries of the project is:

1. SSH-Brute force attacks on cloud
2. Amazon EC2 will be used as the cloud platform for this project.
3. Kippo honeypot to be installed on the cloud.
4. Kippo graph will be the tool used to visualize the data collected by the honeypot.

1.7 Significance of the Project

The Importance of this study is to contribute to the security measurements improvements of cloud computing by integrating honeypots technology to the security infrastructure of cloud computing. Also the study will contribute to the attack analysis and thus to the improvements of the attack mitigation techniques.

1.8 Chapter Organization

This project includes six chapters. Chapter one presents the introduction, problem background, problem statement, Objectives, scopes and importance of this project. Chapter two will be the literature review of the honeypot, cloud computing, its service and deployment models, and security issues, the chapter will also talk about attacks on the cloud environment and discuss the related mitigation techniques and their drawbacks. Finally malware detection methods will be discussed in this chapter. Chapter three discusses the methodology used to conduct this project. Chapter four will discuss the design and the implementation of the system. Chapter five discusses result of study. In the end, conclusion, recommendations and future works are discussed in chapter six.

REFERENCES

Alert-Logic. 2014. Cloud Security Report

Alliance, C. S. 2010. Top threats to cloud computing v1. 0. *Cloud Security Alliance,USA*.

Anubis. 2014, from http://anubis.iseclab.org/

Aviram, A., Hu, S., Ford, B. and Gummadi, R. 2010. Determinating timing channels in compute clouds. Proceedings of the 2010 *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 103-108.

Awadhi, E. A., Salah, K. and Martin, T. 2013. Assessing the security of the cloud environment. Proceedings of the 2013 *GCC Conference and Exhibition (GCC), 2013 7th IEEE*, 251-256.

Barati, M., Abdullah, A., Udzir, N., Behzadi, M., Mahmod, R. and Mustapha, N. 2014. INTRUSION DETECTION SYSTEM IN SECURE SHELL TRAFFIC IN CLOUD ENVIRONMENT. *Journal of Computer Science*, 10(10), 2029-2036.

Barker, I. 2014. Cloud attacks increase as the IT world looks to the skies. Retrieved from http://betanews.com/2014/04/23/cloud-attacks-increase-as-the-it-world-looks-to-the-skies/

BAT, C. 2011, from https://www.honeynet.org/node/315

Bayer, U., Kruegel, C. and Kirda, E. 2006. *TTAnalyze: A tool for analyzing malware*: na.

Bayer, U., Moser, A., Kruegel, C. and Kirda, E. 2006. Dynamic analysis of malicious code. *Journal in Computer Virology*, 2(1), 67-77.

Brown, S., Lam, R., Prasad, S., Ramasubramanian, S. and Slauson, J. 2012. Honeypots in the Cloud.

Chen, D. and Zhao, H. 2012. Data security and privacy protection issues in cloud computing. Proceedings of the 2012 *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 647-651.

Computing-Cloud-Storage. 2014, 06 May 2014. Cloud Service Provider Retrieved from http://www.computingcloudstorage.com/cloud-service-provider/

Egele, M., Scholte, T., Kirda, E. and Kruegel, C. 2012. A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys (CSUR)*, 44(2), 6.

Explorer, P. 2014, from http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

FireEye. 2013. The Need for Speed Incident Response Survey.

fullonn. 2011. computer security threats malicious programs malwares. Retrieved from http://fullonn.blogspot.com/2011/07/computer-security-threats-malicious.html

Gandotra, E., Bansal, D. and Sofat, S. 2014. Malware Analysis and Classification: A Survey. *Journal of Information Security*, 2014.

Gandotra, E., Bansal, D. and Sofat, S. 2014. Malware Analysis and Classification: A Survey. *Journal of Information Security*, 2014.

Girdhar, A. and Kaur, S. 2012. Comparative Study of Different Honeypots System. 2(10), 23-27.

Google. 2012. Kippo Retrieved May 20,2014, from http://code.google.com/p/kippo

GRIFFITH, E. 2013. What Is Cloud Computing. Retrieved from http://www.matthewb.id.au/index.php?option=com_content&view=article&id=31:cloudcomputingpossibilities&catid=1:information-technology&Itemid=2&showall=1

Grosse, E. H., Ransome, J., Reavis, J. and Jim Schmidt, S. 2010. Cloud computing roundtable.

Hofstede, R., Hendriks, L., Sperotto, A. and Pras, A. (2014). SSH compromise detection using NetFlow/IPFIX. *ACM SIGCOMM computer communication review*, 44(5), 20-26.

IDAPro. 2014, from https://www.hex-rays.com/products/ida/support/download_freeware.shtml

Infosecurity-Magazine. 2013. Cross-site scripting attacks up 160% in Q4 2012.

Ion. 2014, from http://bruteforce.gr/kippo-graph

Ion. 2014, from http://bruteforce.gr/kippo-graph

Jesús, J. D. 2012. Navigating the IBM cloud, Part 1: A primer on cloud technologies

Kamal, S. and Kaur, R. 2011. Cloud Computing Security Issue: Survey. Proceedings of the 2011 *2ND INTERNATIONAL CONFERENCE ON METHODS AND MODELS IN SCIENCE AND TECHNOLOGY (ICM2ST-11)*, 149-153.

Karnwal, T., Sivakumar, T. and Aghila, G. 2012. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. Proceedings of the 2012 *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, 1-5.

Khalil, I. M., Khreishah, A. and Azeem, M. (2014). Cloud computing security: a survey. *Computers*, 3(1), 1-35.

Lee, W., Stolfo, S. J. and Mok, K. W. (1998). Mining Audit Data to Build Intrusion Detection Models. Proceedings of the 1998 *KDD*, 66-72.

Liu, S.-T. and Chen, Y.-M. 2011. Retrospective detection of malware attacks by cloud computing. *International Journal of Information Technology, Communications and Convergence*, 1(3), 280-296.

Lo, C.-C., Huang, C.-C. and Ku, J. 2010. A cooperative intrusion detection system framework for cloud computing networks. Proceedings of the 2010 *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*, 280-284.

Lo, C.-C., Huang, C.-C. and Ku, J. 2010. A cooperative intrusion detection system framework for cloud computing networks. Proceedings of the 2010 *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*, 280-284.

LordPE. 2010.

ltys, K. K. 2013. An in-depth look at Kippo: an integration perspective.

Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S. 2002. Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review*, 32(3), 62-73.

Mansfield-Devine, S. 2012. Interview: Tatu Ylönen, SSH Communications Security. *Computer Fraud & Security*, 2012(5), 13-16.

Mcafee. 2013. Infographic: The State of Malware.

Monitor, P. 2014, from http://technet.microsoft.com/enus/sysinternals/bb896645.aspx

Moser, A., Kruegel, C. and Kirda, E. 2007. Limits of static analysis for malware detection. Proceedings of the 2007 *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, 421-430.

Murad, K., Shirazi, S. N.-u.-H., Zikria, Y. B. and Ikram, N. 2010. Evading virus detection using code obfuscation *Future Generation Information Technology* (pp. 394-401): Springer.

Nataraj, L., Karthikeyan, S., Jacob, G. and Manjunath, B. 2011. Malware images: visualization and automatic classification. Proceedings of the 2011 *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, 4.

Nataraj, L., Karthikeyan, S., Jacob, G. and Manjunath, B. 2011. Malware images: visualization and automatic classification. Proceedings of the 2011 *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, 4.

Nataraj, L., Yegneswaran, V., Porras, P. and Zhang, J. 2011. A comparative assessment of malware classification using binary texture analysis and dynamic analysis. Proceedings of the 2011 *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, 21-30.

Noordin, M. 2004. Honeypots Revealed. *SecurityDocs. com.—2004*.

Noordin, M. 2004. Honeypots Revealed. *SecurityDocs. com.—2004*.

OllyDbg. 2000 Retrieved May 20,2014, from http://www.ollydbg.de/

OllyDump. 2007.

Park, Y., Reeves, D., Mulukutla, V. and Sundaravel, B. 2010. Fast malware classification by automated behavioral graph matching. Proceedings of the 2010 *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 45.

PC-Magazine. 2014. http://www.pcmag.com/article2/0,2817,2372163,00.asp Retrieved 04 May 2014, 2014

Pouget, F., Dacier, M. and Debar, H. 2003. Honeypot, honeynet, honeytoken: Terminological issues. *Institut Eurécom (EURECOM), Sophia Antipolis, France, Research Report RR-03-081*.

Process-Hackerreplace. 2008, from http://processhacker.sourceforge.net/

Regshot. 2010, from http://sourceforge.net/projects/

Sandbox, N. 2005, from http://sandbox.norman.no

Savage, S., Wetherall, D., Karlin, A. and Anderson, T. 2000. Practical network support for IP traceback. *ACM SIGCOMM Computer Communication Review*, 30(4), 295-306.

Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Kent, S. T., et al. 2001.Hash-based IP traceback. Proceedings of the 2001 *ACM SIGCOMM Computer Communication Review*, 3-14.

Song, D. X. and Perrig, A. 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the 2001 *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 878-886.

Spitzner, L. 2003. *Honeypots: tracking hackers* (Vol. 1): Addison-Wesley Reading.

The-Scalar-Blog. 2013. Mitigating common cloud computing risks. Retrieved from http://blog.scalar.ca/Blog/bid/87248/Mitigating-common-cloud-computing-risks

Tianfield, H. 2012. Security issues in cloud computing. Proceedings of the 2012 *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*, 1082-1089.

w3techs. 2014. Usage of operating systems for websites Retrieved Nov 20,2014

wikipedia. 2012. Cloud_Computing_Stack Retrieved May 20, 2014, from http://en.wikipedia.org/wiki/File_talk:Cloud_Computing_Stack.svg

wikipedia. 2014. http://en.wikipedia.org/wiki/Cloud_computing Retrieved 05 May 2014, 2014

Willems, C., Holz, T. and Freiling, F. 2007. Toward automated dynamic malware analysis using cwsandbox. *IEEE Security and Privacy*, 5(2), 32-39.

Wireshark. 2008, from http://www.wireshark.org/

Yaar, A., Perrig, A. and Song, D. 2003. Pi: A path identification mechanism to defend against DDoS attacks. Proceedings of the 2003 *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, 93-107.

Yang, J. and Chen, Z. 2010. Cloud computing research and security issues. Proceedings of the 2010 *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, 1-3.

You, I. and Yim, K. 2010. Malware Obfuscation Techniques: A Brief Survey. Proceedings of the 2010 *BWCCA*, 297-300.

You, P., Peng, Y., Liu, W. and Xue, S. 2012. Security issues and solutions in cloud computing. Proceedings of the 2012 *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, 573-577.

Zolkipli, M. F. and Jantan, A. 2011. An approach for malware behavior identification and classification. Proceedings of the 2011 *Computer Research and Development (ICCRD), 2011 3rd International Conference on*, 191-194.