UNIVERSITI PUTRA MALAYSIA

ENHANCED CUCKOO MALWARE ANALYSIS PERFORMANCE USING CLOUD COMPUTING

OSAMAH LUTF HAMOOD BARAKAT

FK 2013 103

ENHANCED CUCKOO MALWARE ANALYSIS PERFORMANCE USING CLOUD COMPUTING

By

OSAMAH LUTF HAMOOD BARAKAT

Thesis Submitted to the School Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

June 2013

قال تعالى:

{ إن أريد إلا الإصلاح ما استطعت وما توفيقي إلا بالله عليه توكلت وإليه أنيب }

هود 88

DEDICATION

To my dear father and mother, Lutf and Belqees, for

their love and endless support

To my kind Wife, Rehab for her love, her loyalty, and

her support

To my lovely children (Ala and Aseel)

To my sisters and brother for their extraordinary love,

their endless care and encouragement

To all those who stand by me

Thank you

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

ENHANCED CUCKOO MALWARE ANALYSIS PERFORMANCE USING CLOUD COMPUTING

By

OSAMAH LUTF HAMOOD BARAKAT

June 2013

Chairman: Shaiful Jahari Bin Hashim, PhD

Faculty: Engineering

Modern information technology affects almost every aspect of human existence. Along with numerous positive outcomes, such comprehensive influence of modern technology on everyday life can also create unprecedented opportunities for the dissemination of malicious software within very short timeframes. The damage caused by malicious software can have a profound and lasting impact on many people across the globe.

A close look at the current approaches of malware analyzers illustrates that response time to community users is inadequately slow at present. It also demonstrates that these analyzers are not scalable to fit the escalating demand for analysis. As a consequence, they will not be able to respond to end-users enquiries in proper time.

to present a new approach to ways of enhancing the malware analyzer performance, in order for the end-users to get feedback faster than present indicators. This approach utilizes cloud computing scalability feature to reach appropriate levels of response time.

Cloud computing is emerging scalability as the main advantage to help application scale to cope with increasing customer demands. Integrating this technique with modern applications and services will provide faster solution due to scalability.

For the purposes of evaluating this approach, two systems were carefully prepared with the same malware analyzer. One of them utilizes cloud computing, and the other one is left with no changes. Both systems were put under investigation with real malware samples to drive a comparison test between the two approaches. Samples were divided into multiple groups with incremental size to study the two systems' behavior towards different submission loads.

Results obtained after processing 3000 samples indicated that cloud based malware analyzer is 23% faster than the standalone system. Although cloud enabled system was performing worse than the standalone system when low samples were submitted, it started to take the lead with noticeable performance when increasing numbers of analysis requests were submitted. With greater enhancements in cloud computing implementation levels, this percentage could increase dramatically to save time consumed while analyzing malware.

Applying this approach in Malaysia will help community members get faster replies regarding suspicious applications with respect to the huge number of IT consumers. This research could be easily extended to the nationwide malware reporting system which can improve the quality of signatures and anti-viruses.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PENINGKATAN ANALISIS CUCKOO PERISIAN MALWARE PRESTASI MENGGUNAKAN PENGKOMPUTERAN AWAN

Oleh

OSAMAH LUTF HAMOOD BARAKAT

Jun 2013

Pengerusi: Shaiful Jahari Bin Hashim, PhD

Fakulti: Kejuruteraan

Teknologi maklumat moden memberi kesan kepada hampir setiap kewujudan aspek manusia. Berserta beberapa hasil yang positif, pengaruh komprehensif teknologi moden dalam kehidupan harian juga boleh mewujudkan peluang yang belum pernah berlaku untuk penyebaran perisian berniat jahat dalam jangka masa yang sangat singkat. Kerosakan disebabkan oleh perisian berniat jahat boleh mempunyai satu mendalam dan hentaman yang kuat kepada ramai orang merentasi dunia.

Pandangan dekat di pendekatan-pendekatan semasa tentang penganalisis malware mengambarkan maklum balas kepada pengguna komuniti adalah tidak lembab pada masa kini. Ia juga menunjukkan bahawa penganalisi yang tidak berskala untuk memenuhi permintaan yang meningkat dianalisis. Akibatny, mereka tidak akan dapat

maklum balas kepada para pengguna pada pertanyaan dikemukakan pada masa yang sesuai. Tesis ini bertujaan untuk membentangkan satu pendekatan baru untuk meningkatkan prestasi penganalisis malware jadi para pengguna akan mendapatkan maklum balas lebih cepat daripada apa yang berlaku sekarang ini. Pendekatan ini menggunakan ciri berskala pengkomputeran awan untuk mencapai tahap masa tindak balas yang sesuai.

Pengkomputeran awan ini timbul kebolehskalaan sebagai kelebihan utama untuk membantu skala aplikasi untuk mengatasi peningkatan permintaan pelanggan. Menyepadukan teknik ini dengan aplikasi moden dan perkhidmatan akan memberikan penyelesaian yang lebih cepat akibat kebolehskalaan.

Untuk tujuan penilaian pendekatan ini, dua sistem telah disediakan dengan berhati-hati dengan penganalisis malware yang sama. Salah satunya menggunakkan pengkomputeran awan dan satu lagi tidada perubahan. Kedua-dua sistem telah diletakkan di bawah siasatan dengan sampel malware sebenar untuk melaksanakan satu ujian perbandingan di antara dua pendekatan. Sampel telah dibahagikan kepada pelbagai kumpulan dengan saiz tambahan untuk mengkaji kelakuan dua sistem terhadap muatan penyerahan yang berbeza.

Keputusan yang diperolehi setelah memproses 3000 sampel menunjukkan penganalisis malware sebanyak 23% lebih cepat berbanding dengan sistem tersendiri. Walaupun pengkomputeran awan melaksanakan lebih teruk berbanding dengan sistem sendiri apabila sampel yang rendah telah diserahkan, ia mula ambil langkah dengan prestasi yang ketara apabila pertambahan bilangan permohonan analisis telah diserahkan. Dengan penambahan yang lebih besar di tahap pengkomputeran awan, peratusan ini mungkin meningkatkan secara mendadak untuk menjimatkan masa yang digunakan ketika mengkaji malware.

Menggunakan pendekatan ini di Malaysia boleh membantu ahli-ahli komuniti mendapat balasan yang lebih cepat mengenai permohonan-permohonan mencurigakan dengan sejumlah besar pengguna IT. Penyelidikan ini boleh melanjutkan dengan senang kepada seluruh negara malware sistem pelaporan yang boleh memperbaiki kualiti tandatangan dan anti-virus.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Almighty Allah (S.W.T) for giving me the strength, patience, courage, and determination to complete this work. All grace and thanks belongs to Almighty Allah (S.W.T)

Many special thanks go to my supervisor Dr. Shaiful Jahari bin Hashim, for his incredible guidance, continuous support, and encouragement. He always has time for me and readily providing his technical expertise throughout the period of my study. I owe more than I can ever repay. The completion of this work becomes possible due to his supervision. His high stance of diplomatic power and professionalism set a great model for me to follow.

I would also like to thank Associate Professor Dr. Raja Syamsul Azmir bin Raja Abdullah for serving on my thesis committee. His helpful suggestions and advices on various aspects of my research work have certainly been very constructive. Without His kind cooperation and support, my graduate study would not have been accomplished.

I would also like to include acknowledgment to my colleagues, Hamdan and M. Ben Mubarak. They provided me a valuable advices and positive critics during my candidature. They guided me to blind spots while writing my thesis. Additionally, I owe a lot to Dr. Adam Alhawari for helping me during the analysis of data and thesis writing. Thanks to everyone at the Faculty of Engineering and all those who asked "how is your thesis going?" These memories at the Faculty of Engineering will always be cherished.

I certify that a Thesis Examination Committee has met on 28 June 2013 to conduct the final examination of Osamah Lutf Barakat on his thesis entitled "Enhanced Cuckoo Malware Analysis Performance using Cloud Computing" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the University Putra Malaysia [P. U. (A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Fakhrul Zaman bin Rokhani, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Wan Azizun binti Wan Adnan, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Makhfudzah binti Mokhtar, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mahamod Ismail, PhD
Professor
Universiti Kebangsaan Malaysia
Malaysia
(External Examiner)

NORITAH OMAR, PhD
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 September 2013

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Shaiful Jahari Bin Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Raja Syamsul Azmir b. Raja Abdullah, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 27 SEP 2013

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

OSAMAH LUTF HAMOOD BARAKAT

Date: 28 June 2013

TABLE OF CONTENTS

Page

DEDICATION III
ABSTRACT VI
ABSTRAK VII
ACKNOWLEDGEMENTS X
APPROVAL XI
DECLARATION XIII
LIST OF TABLES XVI
TABLE OF FIGURES XVII
LIST OF ABBREVIATIONS XVIII

CHAPTER

1 INTRODUCTION 1
1.1 Background 1
1.2 Motivation and Problem Statement 2
1.3 Research Aim and Objectives 3
1.4 Study Scope 4
1.5 Thesis Organization 5

2 LITERATURE REVIEW 6
2.1 Introduction 6
2.2 Cloud Computing 6
2.2.1 Introduction 6
2.2.2 Terminology 7
2.2.3 Cloud classification 8
2.2.4 Cloud characteristics 10
2.2.5 Related technology 11
2.2.6 Cloud Environment Software 13
2.3 Malware Analysis 19
2.3.1 Introduction 19
2.3.2 Definitions 19
2.3.3 Static Analysis 20
2.3.4 Dynamic Analysis 21
2.3.5 Architecture Implementation 23
2.3.6 Malware Analysis Tools 27
2.4 Utilizing Cloud Computing in Malware Analysis and Detection 32

3 METHODOLOGY 35
3.1 Introduction 35
3.2 System Design and Implementation 36
3.2.1 Introduction 36
3.2.2 Hardware Installation 37
3.2.3 Cloud Environment 38
3.2.4 Cloud Enabled Malware Analyzer 42
3.3 Research Feasibility 48
3.3.1 Introduction 48
3.3.2 Maximum Cloud Capacity 49

3.3.3 Total Execution Time 50
3.3.4 Stability 51
3.3.5 Performance Evaluation 52

4 RESULTS AND DISCUSSION 54
4.1 Introduction 54
4.2 Stability Experiment 54
4.3 Experiment over Standalone Cuckoo System 55
4.4 Experiment over Cloud Enabled Cuckoo System 59
4.5 Comparative study on proposed system 62

5 CONCLUSION AND RECOMMENDATION FOR FUTURE WORK 64
5.1 Conclusion 64
5.2 Thesis Contributions 65
5.3 Future research direction 65

REFERENCES 68
APPENDICES 69
BIODATA OF STUDENT 90
LIST OF PUBLICATIONS 91

LIST OF TABLES

Table		Page
2.1	Comparison of Open-source Cloud Computing Software	17
2.2	Comparison of Malware Analyzers Software	31
3.1	Hardware Components' Specifications	38
3.2	Main Python Modules in Cloud Enabled Cuckoo System	48
4.1	Results obtained from Standalone Cuckoo System	57
4.2	Results Obtained from Cloud Enabled Cuckoo System	61
4.3	Total Saving Time Percentage	63

TABLE OF FIGURES

Figure		Page
1.1	Research Scope	4
1.2	Cloud Enabled Malware Analyzer System	5
2.1	Logical relationship between Eucalyptus components [19]	14
2.2	OpenStack Components [21]	15
3.1	Proposed System Major Components	36
3.2	LAN Connections between Hardware Components	38
3.3	Minimal Cloud Environment Components by CloudStack [23]	41
3.4	Cloud Enabled Cuckoo Steps Flow Chart	46
4.1	Results Obtained In Stability Test	55
4.2	Comparing Results from Two Systems	63

LIST OF ABBREVIATIONS

API	Application programming interface
APK	Android application Package file
CERT	Cyber Emergency Response Team
DLL	Dynamic Linking Library
EC2	Elastic Compute Cloud
GPL	GNU General Public License
IAAS	Infrastructure as a service
iSCSI	Internet Small Computer System Interface
ISO	Archive file of an optical disc
NAT	Network Address Translation
NFS	Network File System
NIST	National Institute of Standards and Technology
PAAS	Platform as a service
SAAS	Software as a service
SSH	Secure Shell
VM	Virtual Machine

CHAPTER 1

INTRODUCTION

1.1 Background

The past decade witnesses a rapid development of computing power. This development was in all directions starting from personal computer (PC) to super frame. In this decade, mobile phone technology was developed so rapidly to reach what exists now such as hand phone which yields to a very wide variety of customers who can use computer services despite first years.

As a result, any malicious attacks can affect a wide variety of users. Symantec thread report [1], which was published in 2012, reported that there were 5.5 billion attacks blocked in 2011 whereas there were 3 billion attacks only in 2010, which is closed to be doubled. Moreover, malicious attacks started to be one of the used weapons in cyber war between countries as in Stuxnet [2], which was attacking a nuclear reactor in Iran, also flame [3] which was attacking Middle East users. This terror role was not the only one as malicious software used also to steal money or attack economic systems of companies and countries. All these manifestations required security experts to counter those attacks and create new tools to face those challenges, especially that zero-day threats need on average 10 months to be discovered [4].

On another way, cloud computing appeared in the last four years as a promise IT paradigm. This technology presented a good solution to utilize resources effectively and enhance the consumed power [5]. In addition, it started as an economic solution to ease beginning of small business without spending too many resources on needed computing power. Amazon [6] started its public cloud in 2006, which provided computing resources on a rental basis. Although this idea was known before from theoretical point of view, this was the first time to be implemented as real service to public customers. Cloud computing comes with another term called outsourcing, which means that computing power and operations will be moved from small and medium organizations to warehouses where it will be share to public users and companies .

This technology can be used to enhance and support malware analyzers in massive scanning routines to automate this process, speed up the process, and secure customers' devices. This study is presenting an approach to utilize cloud computing features to support and enhance the malware analysis process. After that, a compartment study is shown as prove of its reliability and functionality.

1.2 Motivation and Problem Statement

The impact of new technology development on security needs by users increases daily. As mentioned previously, there were 5.5 billion attacks reported. Thus, security engineers should respond in a manner at least equivalent or better than those attacks. However, existing malware analysis services still beyond these needs. Main reason behind that is these analyzers are not scalable enough to respond in appropriate time to end users. Being quick in responses leads to two possibilities where first one is developing a faster hardware system which yields more money spending on infrastructure. Second possibility is to hire more employees, which result in more money spending in salaries and over time payment.

The most known paradigm which provides high speed using normal hardware was grid [7] but building a grid need to plan for maximum load to cope with huge incoming software to be analyzed. In the published report [1] there were 5.5 billion attacks blocked in 2011 while there were 3 billion attacks only in 2010, which is almost double. Thus, the capacity including hardware and manpower should be doubled to keep security analysts on track. Therefore, the solution presented in this study should save time by speeding up the analysis process and save cost by provision the needed hardware only and save manpower by automate the maximum possible workflow phases.

Another view on this problem can be considered if the workflow was highlighted. What happen now if someone wants to send software for analysis purpose and make sure that software is safe? The user simply can use any of available submission tools that provided by that malware analyzer and upload whatever he wants to be analyzed. After that, he should wait for results which it depends on how powerful is that analyzer and whether it works automatically or needs a human interaction which depends in turn if the file submitted on working hours or not. All these factors lead to inevitability of automating the whole process so that interaction between malware analyzer and users fully fits the user needs.

1.3 Research Aim and Objectives

The main goal of this study is to build a scalable and automatic malware analyzer utilizing the technology of cloud computing. In this study, the focus will be on saving total consumed time within the whole process. From this goal, other objectives were determined and listed as the following:

1. Design a system which uses a private scalable cloud environment to extend a standalone automated malware analyzer.

2. Implement the designed system in order to test the stability, scalability.

3. Design and implement a comparative study between the cloud computing enabled malware analyzer and the standalone approach in terms of scalability.

1.4 Study Scope

The scope of this research is illustrated in Figure 0.1 and Figure 0.2 . The dotted lines represent the component in general malware analyzer, where this research will take place to achieve the stated objectives.

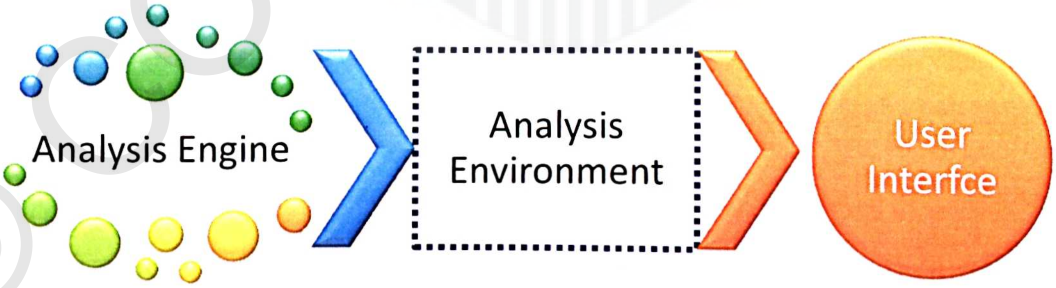

Figure 0.1 Research Scope

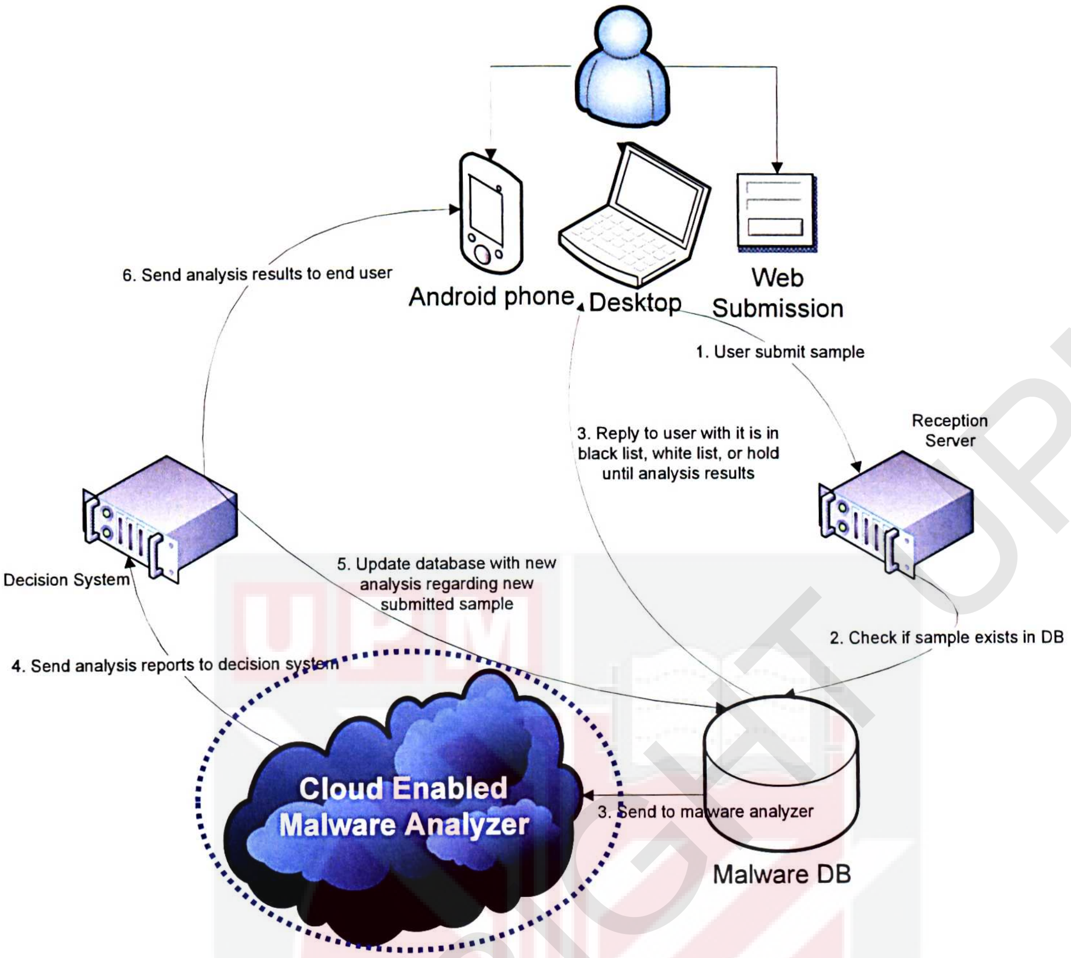
Android phone
Desktop
Web Submission
1. User submit sample
Reception Server
2. Check if sample exists in DB
3. Reply to user with it is in black list, white list, or hold until analysis results
Malware DB
3. Send to malware analyzer
Cloud Enabled Malware Analyzer
4. Send analysis reports to decision system
Decision System
5. Update database with new analysis regarding new submitted sample
6. Send analysis results to end user

Figure 0.2 Cloud Enabled Malware Analyzer System

1.5 Thesis Organization

This thesis is organized in five chapters, including this introduction chapter. The cloud computing technology will be defined and discussed in chapter 2. Additionally, malware analysis also will be explored with some highlights on some analyzers. After that, chapter 3 will explain the methodology used to prove the feasibility of the proposed idea. It will elaborate the conducted experiments in addition to used settings. Then, the results obtained from those experiments will be presented in chapter 4. Finally, a conclusion and future research directions will be in chapter 5.

REFERENCES

[1] G. Egan, K. Haley, D. Mckinney, T. Millington, J. Mulcahy, T. Parsons, A. Watson, M. Nisbet, N. Johnston, and S. Hittel, "Internet Security Threat Report," 2012.

[2] T. Chen, "Stuxnet, the real start of cyber warfare? [Editor's Note]," *IEEE Network*, vol. 24, no. 6, pp. 2–3, Nov. 2010.

[3] R. S. Security, "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East," 2012. [Online]. Available: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east. [Accessed: 08-Jul-2013].

[4] G. Andy, "Hackers Exploit 'Zero-Day' Bugs For 10 Months On Average Before They're Exposed," 2012. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2012/10/16/hackers-exploit-software-bugs-for-10-months-on-average-before-theyre-fixed/. [Accessed: 01-Jul-2013].

[5] B. J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green Cloud Computing : Balancing Energy in Processing, Storage, and Transport," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 149–167, 2011.

[6] Amazon, "Amazon Cloud EC2." [Online]. Available: http://aws.amazon.com/ec2/. [Accessed: 08-Jul-2013].

[7] I. Foster and C. Kesselman, *The Grid 2: Blueprint for a New Computing Infrastructure*, 2nd ed. Elsevier, p. 748, 2003.

[8] D. F. Parkhill, *The challenge of the computer utility*. AddisonWesley, p. 206, 1966.

[9] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication*. p. 7, 2011.

[10] K. Jeffery and B. Neidecker-Lutz, "The Future Of Cloud Computing Oppprtunities For European Cloud Computing Beyond 2010," 2010.

[11] "RackSpace." [Online]. Available: http://www.rackspace.com. [Accessed: 08-Jul-2013].

[12] "Google App Engine." [Online]. Available: http://code.google.com/appengine. [Accessed: 08-Jul-2013].

[13] "Microsoft Windows Azure." [Online]. Available: www.microsoft.com/azure. [Accessed: 08-Jul-2013].

[14] "SalesForce.com." [Online]. Available: www.salesforce.com. [Accessed: 08-Jul-2013].

[15] I. Foster, “What is The Grid? A Three Point Checklist,” 2002. [Online]. Available: http://dlib.cs.odu.edu/WhatIsTheGrid.pdf. [Accessed: 08-Jul-2013].

[16] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A Break in the Clouds: Towards a Cloud Definition,” *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2009.

[17] R. Goldberg, “Survey of Virtual Machine Research,” *IEEE Computer*, vol. 7, no. 6, pp. 34–45, 1974.

[18] “Eucalyptus.” [Online]. Available: http://www.eucalyptus.com/. [Accessed: 08-Jul-2013].

[19] E. Systems, “Installation Guide for Eucalyptus.” Eucalyptus, pp. 1–124, 2010.

[20] G. von Laszewski, J. Diaz, F. Wang, and G. C. Fox, “Comparison of Multiple Cloud Frameworks,” in *2012 IEEE Fifth International Conference on Cloud Computing*, pp. 734–741, 2012.

[21] “OpenStack.” [Online]. Available: http://www.openstack.org/. [Accessed: 08-Jul-2013].

[22] X. Wen, G. Gu, Q. Li, Y. Gao, and X. Zhang, “Comparison of Open-source Cloud Management Platforms: OpenStack and OpenNebula,” in *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 2457–2461, 2012.

[23] “CloudStack.” [Online]. Available: http://incubator.apache.org/cloudstack/. [Accessed: 08-Jul-2013].

[24] G. McGraw and G. Morrisett, “Attacking Malicious Code: A Report to the Infosec Research Council,” *IEEE Software*, vol. 17, no. 5, pp. 33–41, Sep. 2000.

[25] A. Moser, C. Kruegel, and E. Kirda, “Exploring Multiple Execution Paths for Malware Analysis,” in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 231–245, 2007.

[26] M. Christodorescu and S. Jha, “Static analysis of executables to detect malicious patterns,” in *SSYM’03 Proceedings of the 12th conference on USENIX Security Symposium*, p. 12, 2003.

[27] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, “Semantics-Aware Malware Detection,” in *2005 IEEE Symposium on Security and Privacy (S&P’05)*, pp. 32–46, 2005.

[28] C. Kruegel, W. Robertson, and G. Vigna, “Detecting Kernel-Level Rootkits Through Binary Analysis,” in *20th Annual Computer Security Applications Conference,* pp. 91– 100, 2004.

[29] H. Chen, D. Dean, and D. Wagner, "Model Checking One Million Lines of C Code," in *Proceedings of Network and Distributed System Security Symposium*, pp. 171 – 185, 2004.

[30] M. Egele, M. Szydlowski, E. Kirda, and C. Kruegel, "Using Static Program Analysis to Aid Intrusion Detection," in *Detection of Intrusions and Malware & Vulnerability Assessment*, vol. 4064/2006, Springer Berlin / Heidelberg, pp. 17–36, 2006.

[31] A. Moser, C. Kruegel, and E. Kirda, "Limits of Static Analysis for Malware Detection," in *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, pp. 421–430, 2007.

[32] P. Szor, *Art of Computer Virus Research and Defense*, 1st ed., vol. 3722. Addison-Wesley Professional, p. 744, 2005.

[33] T. Yetiser, "Polymorphic Viruses: Implementation, Detection, and Protection," *The Hack Academy*, 1993. [Online]. Available: http://www.thehackademy.net/madchat/vxdevl/papers/avers/yetiser.txt. [Accessed: 08-Jul-2013].

[34] M. Oberhumer, L. Molnár, and J. F. Reiser, "UPX: Ultimate Packer for eXecutables," 2005. [Online]. Available: http://upx.sourceforge.net/.

[35] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A Survey on Automated Dynamic Malware-Analysis Techniques and Tools," *ACM Computing Surveys*, vol. 44, no. 2, pp. 1–49, Feb. 2012.

[36] Y.-M. Wang, R. Roussev, C. Verbowski, A. Johnson, M.-W. Wu, Y. Huang, and S.-Y. Kuo, "Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management," in *Proceedings of the 18th USENIX conference on System administration*, pp. 33–46, 2004.

[37] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, and J. Nazario, "Towards an Understanding of Anti-virtualization and Anti-Debugging Behavior in Modern Malware," in *2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN)*, pp. 177–186, 2008.

[38] K. Fall, "Network Emulation in The VINT/NS Simulator," in *Proceedings IEEE International Symposium on Computers and Communications (Cat. No.PR00250)*, pp. 244–250, 1999.

[39] F. Bellard, "QEMU, a Fast and Portable Dynamic Translator," in *Proceedings of the annual conference on USENIX Annual Technical Conference*, pp. 41–46, 2005.

[40] R. Paleari, L. Martignoni, G. F. Roglia, and D. Bruschi, "A Fistful of Red-pills: How to Automatically Generate Procedures to Detect CPU Emulators," in *the 3rd USENIX conference on Offensive technologies (WOOT'09)*, p. 2, 2009.

[41] T. Raffetseder, C. Kruegel, and E. Kirda, “Detecting System Emulators,” in *Lecture Notes in Computer Science*, vol. 4779, J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–18, 2007.

[42] “Anubis Malware Analyzer.” [Online]. Available: http://anubis.iseclab.org/. [Accessed: 08-Jul-2013].

[43] U. Bayer, C. Kruegel, and E. Kirda, “TTAnalyze: A Tool for Analyzing Malware,” in *15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR)*, 2006.

[44] C. Willems, T. Holz, and F. Freiling, “Toward Automated Dynamic Malware Analysis Using CWSandbox,” *IEEE Security and Privacy Magazine*, vol. 5, no. 2, pp. 32–39, Mar. 2007.

[45] “GFI SandBox.” [Online]. Available: http://www.gfi.com/malware-analysis-tool. [Accessed: 08-Jul-2013].

[46] “CWSandbox Behavior-based Malware Analysis.” [Online]. Available: http://mwanalysis.org/. [Accessed: 08-Jul-2013].

[47] “Cuckoo sandbox.” [Online]. Available: http://cuckoobox.org/. [Accessed: 08-Jul-2013].

[48] A. Dinaburg, P. Royal, M. Sharif, and W. Lee, “Ether,” in *Proceedings of the 15th ACM conference on Computer and communications security - CCS '08*, pp. 51–62, 2008.

[49] G. Pék, B. Bencsáth, and L. Buttyán, “nEther: In-guest Detection of Out-of-the-guest Malware Analyzers,” in *Proceedings of the Fourth European Workshop on System Security - EUROSEC '11*, pp. 1–6, 2011.

[50] “Norman sandBox.” [Online]. Available: http://www.norman.com/security_center/security_tools/. [Accessed: 08-Jul-2013].

[51] J. Clausing, “Building an Automated Behavioral Malware Analysis Environment using Open Source Software.” SANS Institute, p. 31, 2009.

[52] H.-D. Huang, C.-S. Lee, H.-Y. Kao, Y.-L. Tsai, and J.-G. Chang, “Malware Behavioral Analysis System: TWMAN,” in *2011 IEEE Symposium on Intelligent Agent (IA)*, pp. 1–8, 2011.

[53] L. Martignoni, R. Paleari, and D. Bruschi, “A Framework for Behavior-Based Malware Analysis in The Cloud,” in *5th International Conference, ICISS 2009*, vol. 5905, pp. 178–192, 2009.

[54] C. Adrian Martinez, G. Isaza Echeverri, and A. G. Castillo Sanz, “Malware Detection Based on Cloud Computing Integrating Intrusion Ontology

Representation," in *2010 IEEE Latin-American Conference on Communications*, pp. 1–6, 2010.

[55] J. Oberheide, E. Cooke, and F. Jahanian, "CloudAV: N-version Antivirus in The Network Cloud," in *Proceedings of the 17th conference on Security symposium*, pp. 91–106, 2008.

[56] S.-T. Liu and Y.-M. Chen, "Retrospective Detection of Malware Attacks by Cloud Computing," in *2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 510–517, 2010.

[57] "Hadoop." [Online]. Available: http://hadoop.apache.org/. [Accessed: 27-Jul-2012].

[58] X. Sun, "The Relation of Scalability and Execution Time," in *Proceedings of International Conference on Parallel Processing*, no. 1063, pp. 457–462, 1996.

[59] I. Martin and F. Tirado, "Relationships Between Efficiency and Execution Time of Full Multigrid Methods on Parallel Computers," *IEEE Transactions on Parallel and Distributed Systems*, vol. 8, no. 6, pp. 562–573, Jun. 1997.

[60] U. Bayer, E. Kirda, and C. Kruegel, "Improving the Efficiency of Dynamic Malware Analysis," in *Proceedings of the 2010 ACM Symposium on Applied Computing - SAC '10*, p. 1871, 2010.

[61] C. E. Brown, "Coefficient of Variation," in *Applied Multivariate Statistics in Geohydrology and Related Sciences*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 155–157, 1998.