

Modelling and simulation of a new cloud computing platform based on the SPEEDOS operating system

School of Electrical Engineering and Computer Science

A thesis submitted to the

University of Newcastle, NSW, Australia

For the degree of Doctor of Philosophy in Computer Science

Ala' Said Mohammad Mughaid

June 2018



**THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA**

Abstract

Today's society is data-driven. Collecting data from people, actions, algorithms and the web has resulted in large data stores, and accommodating all these data has become a major challenge. 'Big data' tends to grow exponentially each year [1]. To handle these increasing data sizes, the concepts of shared computing, shared memory, and remote storage and access to resources have been developed. Systems such as grid computing systems, where the infrastructure combines computer resources and storage from different locations to reach a common objective; utility computing systems, a business model in which computational resources and demand are packaged as a metered service similar to electricity and the public switched telephone network; and distributed systems, which consist of either physically distributed institutions or logically related projects/groups, are examples of such concepts.

Cloud computing is a relatively recent abstraction, providing functionalities such as computation, and the sharing and storage of data for the users of computer networks. Cloud computing is attracting massive global investment [2] because of the services that it provides. However, security remains one of the top concerns for organisations and customers using cloud computing environments [3]. In fact, some security issues in cloud computing were inherited from previous computing systems, but the others were created because of its unique characteristics and architecture. Conventional security mechanisms are not sufficient to mitigate the threats in cloud systems, and new techniques are needed.

This research presents a new platform for secure cloud computing. The platform allows cloud service providers to host their clients' data in a secure environment and allows them

to operate on the services in a secure manner for transactions. The platform was designed to make the operations relatively secure and safe using a robust structure by building a general software-structuring framework to implement the cloud software resources.

The new platform provides new mechanisms that authorise only legitimate users to access data. The access to data is handled by a third-party service that checks on all of the requests by using the user's ID and authentication/authorisation details. All of the users' details and sensitive data are encrypted during transit and storage. The platform was implemented, evaluated and compared in terms its effectiveness to the existing cloud platforms over a set of criteria. The results showed that this platform worked as expected and fairly quickly as compared to the other security platforms, and provided strong security against an intruder's actions.

Keywords: security, cryptography, cloud computing, architectural model

Email: c3193420@uon.edu.au

Statement of originality

I hereby certify that the work embodied in the thesis is my own work, conducted under normal supervision. The thesis contains no material which has been accepted, or is being examined, for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. I give consent to the final version of my thesis being made available worldwide when deposited in the University's Digital Repository, subject to the provisions of the *Copyright Act 1968* and any approved embargo.

(Ala' Said Mughaid)

Acknowledgements

I would like to express my sincere gratitude to Associate Professor Frans Henskens as well as my sponsor The Hashemite University in Jordan, who made it possible for me to conduct this research on *Modelling and simulation of a new cloud platform based on the SPEEDOS operating system*. Owing to their help, I conducted extensive research and learnt a number of new things. Working under Professor Frans afforded me many benefits, including access to his wide knowledge. He provided and maintained an academic environment throughout my thesis and made this entire experience interesting and worthwhile for me. He is a great mentor, and it was an honour to conduct my research with him.

I would also like to thank my other supervisors, Dr David Paul and Dr Mark Wallis, for their belief in me and for their help throughout my study. This work would not have been possible without the time and support they provided me. I look forward to working with them long into the future. Thank you also to Right Style Editing for their copy-editing work on the final document.

To my daughter, Marlin, for the many times I have been away from you or not in the mood to spend time with you; thank you for understanding the work I've been doing and thanks for the hugs I receive every time you see me locked in my office. Being a PhD student is tiring, but you are the best reason pushing me to continue to achieve my goal. Finally, I am grateful to my wife and my parents, who have provided with moral and emotional support in my life and strength to complete this work. I am also grateful to my other family members and friends who have supported me along the way.

Table of Contents

Abstract	iii
Statement of originality	v
Acknowledgements.....	vii
Chapter 1.....	16
1.0 Introduction.....	16
1.1 Motivation	16
1.2 Research objectives.....	17
1.3 Problem definition	18
1.4 Research questions	18
1.5 Research methodology	19
1.6 Thesis structure	20
1.7 Contributions.....	21
Chapter 2.....	23
Computer network and cloud systems.....	23
2.0 Computer networks	23
2.1 Cloud computing concepts	24
2.2 Middleware of cloud computing.....	26
2.2.1 Software-as-a-Service	26
2.2.2 Platform-as-a-Service.....	27
2.2.3 Infrastructure-as-a-Service.....	28
2.3 Cloud computing classifications.....	30
2.4 Virtualisation in the cloud	31
2.5 Cloud computing advantages and disadvantages	35
2.6 Network security.....	37
2.7 Network security threats/attacks	39
2.7.1 Unauthorised access.....	39
2.7.1.1 Malicious association.....	40
2.7.1.2 Man-in-the-middle attack.....	40
2.7.1.3 Injections.....	41
2.7.1.4 Eavesdropping.....	42
2.7.1.5 Phishing.....	42
2.7.1.6 Accidental association.....	43
2.7.2 Denial-of-service attack	43
2.7.2.1 Slowloris	43
2.7.2.2 ICMP (ping) flood.....	44
2.7.2.3 SYN flood	44
2.8 General principles to protect networks	45
2.8.1 Firewalls.....	45

2.8.2 Intrusion detection systems	45
2.8.2.1 NIDS	46
2.8.2.2 HIDS	46
2.8.2.3 Signature-based IDS	47
2.8.3 Cryptography	47
2.8.3.1 Symmetric encryption	48
2.8.3.2 Asymmetric encryption	49
2.8.3.3 Hash functions	50
2.8.4 Security solution frameworks	51
2.8.4.1 Spring security core	52
2.8.4.2 Security assertion markup language	52
2.8.4.3 Kerberos	53
2.9 Cloud computing security	54
Chapter 3	66
Overview of computer systems	66
3.0 Introduction	66
3.1 Computer memory	67
3.2 Memory management	68
3.3 Shared memory	71
3.4 Problems with currently used operation systems	71
3.5 SPEEDOS architecture	73
3.6 SPEEDOS kernel	74
3.7 Memory in SPEEDOS	76
3.7.1 Paging	77
3.7.2 Segmentation	78
3.7.3 Containers	80
3.8 Applications in SPEEDOS	82
3.9 Processes in SPEEDOS	88
3.9.1 Out-of-process mechanism	88
3.9.2 In-process mechanism	89
3.10 Logging in and out	90
3.11 Significance of SPEEDOS system	91
3.11.1 Minimal kernel	92
3.11.2 Memory management	93
3.11.3 Representation of applications in SPEEDOS	94
3.11.4 Module capabilities	95
3.11.5 In-process communication protocol	96
3.12 SPEEDOS security benefits for cloud	96
Chapter 4	100
Designing cloud computing over SPEEDOS	100

4.1 Representation of cloud modules in SPEEDOS environment.....	101
4.1.1 Application of information-hiding principle to cloud modules	102
4.1.2 Application of capabilities linking mechanism.....	105
4.1.3 Application of qualifier system.....	106
4.2 Communication with cloud modules in SPEEDOS environment.....	108
4.3 Storage of cloud data in SPEEDOS memory	109
4.4 Protection of cloud data in SPEEDOS memory	110
4.5 Provision of cloud computing in SPEEDOS environment	111
4.5.1 Complexities developers face while learning Timor.....	112
4.5.2 Introduction of more new bugs, troubleshooting and bugs fixing	112
4.5.3 Small changes resulting in slower performance, higher resource consumption and more frequent failures and crashes.....	115
4.5.4 Hardware/driver problems.....	115
4.5.5 User interface problems/learning curve for cloud customers.....	116
4.5.6 Introduction System administrators' requirement to learn re-management of cloud software resources over SPEEDOS.....	117
4.5.7 Hardware High cost and time requirements.....	118
4.6 Proposed solution	119
4.7 Designing a cloud security service using SPEEDOS architecture.....	120
4.8 Proposed security service design	122
4.8.1 Authorisation/authentication flow.....	123
4.8.2 Proposed security scheme	126
4.8.3 Security service architecture	127
4.8.3.1 Design of cloud applications.....	128
4.8.3.2 Design of capabilities.....	129
4.8.3.3 Design of encryption/decryption mechanism.....	131
4.8.3.4 Security service responsibilities.....	132
4.8.4 Client application	137
4.9 Main methods of security service	139
4.10 Why this system should be more secure than a traditional system	141
4.11 Comparisons with other security frameworks.....	143
Chapter 5.....	146
Implementation of the cloud platform.....	146
5.0 Introduction.....	146
5.1 Grails.....	147
5.2 Plugins.....	148
5.3 Database.....	150
5.4 Implementation	150
5.4.1 Security service implementation	151
5.4.1.1 Implementing modules.....	153
5.4.1.2 Implementing capabilities	154
5.4.1.3 Encryption/decryption implementation.....	156

5.4.2 Client application implementation.....	158
5.4.3 Implementation of client and server communications.....	163
5.5 Capability service plug-in	164
5.6 Implementation of security scheme.....	165
Chapter 6	167
Security overview and experimental results.....	167
6.0 Introduction	167
6.1 Security overview and experiment.....	167
6.2 Overview of attacks	168
6.2.1 Malware or malicious software	168
6.2.2 Man-in-the-middle and eavesdropping.....	169
6.2.3 Test for web storage SQL injection	170
ACL-SQL injection inquiry.....	170
ACL-SQL injection output	171
Security service -SQL injection inquiry	172
Security service-SQL injection output.....	172
ACL-SQLMAP injection inquiry	172
ACL-SQLMAP injection output	173
Security service-SQLMAP injection query	174
Capability-SQLMAP injection output.....	175
6.2.4 Shared memory threats/unauthorised access to the security service.....	176
Dumbing the security service memowry	177
6.2.5 Client application threats.....	178
6.2.5.1 Malicious user.....	179
6.2.5.2 Compromised user/application	183
6.3 Test analysis report	183
Bank application using ACL mechanism experiment	184
Bank application using security service experiment	188
Chapter 7	194
Conclusion and future work	194
7.0 Introduction	194
7.1 Research question 1	195
7.2 Research question 2	196
7.3 Research question 3	197
7.4 Future work	197
Bibliography	199

List of Figures:		
Figure 2.1:	Virtual architecture and traditional architecture	31
Figure 2.2:	Symmetric encryption	48
Figure 2.3:	Asymmetric encryption	49
Figure 3.1:	Representation of conventional memory management	68
Figure 3.2:	Representation of memory in SPEEDOS system	77
Figure 3.3:	Representation of a segment capability	79
Figure 3.4:	Representation blocking qualifier	85
Figure 3.5:	Representation of body instruction qualifier	86
Figure 3.6:	Representation of testing qualifier	87
Figure 3.7:	Representation of callout bracket method qualifier	87
Figure 4.1:	Conventional bank system example	102
Figure 4.2:	SPEEDOS bank system example	103
Figure 4.3:	Information hiding code example	105
Figure 4.4:	Application of capability access rights programming language	106
Figure 4.5:	Application of qualifier and capability access rights	108
Figure 4.6:	Platform design	124
Figure 4.7:	Structure of capability	129
Figure 4.8:	Platform communication diagram	136
Figure 5.1:	Capability code structure	155
Figure 5.2:	Capabilities encryption representation in the database	157
Figure 5.3:	Server application	158
Figure 5.4:	Client platform authentication	158
Figure 5.5:	Creating bank accounts in the system	160
Figure 5.6:	Creating new social account process	161
Figure 5.7:	Capability interface methods	162
Figure 5.8:	HTTP call method in the remote service	164
Figure 6.1:	Requesting admin details of ACL application	170
Figure 6.2:	Administrator detail from ACL application	171
Figure 6.3:	Requesting administrator details from the security service	172
Figure 6.4:	Administrator detail from the security service	172
Figure 6.5:	Requesting admin details of ACL-bank system	172
Figure 6.6:	Administrator detail from the ACL-bank system	173
Figure 6.7:	Requesting admin details of security service-bank system	174
Figure 6.8:	Administrator detail from the security service-bank system	175
Figure 6.9:	Capability SQL results.	177
Figure 6.10:	Passwords and encryption keys of the security service	178
Figure 6.11:	User trying to retrieve data using capability URL through web browser	181
Figure 6.12:	Logged-in user trying to retrieve further data using URL	182
Figure 6.13:	User trying to retrieve data of other applications by using valid capability	182
Figure 6.14:	Revocation capabilities option	183
Figure 6.15:	Creating of users and requests	185
Figure 6.16:	Server responses to users with ACL access	186
Figure 6.17:	Server response to users without ACL access	187
Figure 6.18:	Analysis of results of ACL experiment	187
Figure 6.19:	Data analysis for requests of users with ACL access	188
Figure 6.20:	Data analysis for requests of users without ACL access	188
Figure 6.21:	Average total time of the experiment	188
Figure 6.22:	Creating of users and requests	189
Figure 6.23:	Admin requests successfully	190

Figure 6.24:	User requests successfully	190
Figure 6.25:	Analysis of experimental results	191
Figure 6.26:	Data analysis for admin requests	191
Figure 6.27:	Data analysis for user requests	191
Figure 6.28:	Average total time of the experiment	192
Figure 6.29:	Comparison between the two experiments	193

List of Tables:		
Table 4.1:	Platform methods, data inputs and outputs	139
Table 7.1:	Summary of research objectives	195

