

Credibility-based Trust Management and Discovery of Cloud Services



A dissertation submitted in fulfillment
of the requirements for the degree of

Doctor of Philosophy
in
Computer Science

Talal Hashem Noor

Supervisors:

A/Prof. Michael Sheng

Prof. Hong Shen

August 31st, 2013

© Copyright by
Talal Hashem Noor
2013

ORIGINALITY STATEMENT

I certify that this work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution in my name 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. In addition, I certify that no part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint-award of this degree.

I give consent to this copy of my thesis when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library catalogue and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

Talal Hashem Noor

August 31st, 2013

*To my mother and father,
my wife, little princess and prince,
my brothers and sisters,
who made all of this possible,
for their endless love, support and patience.*

ACKNOWLEDGMENTS

During my PhD journey, I enjoyed working with the school, staff and students at the University of Adelaide and I would like to thank many people who made my journey a nice graduate school experience. First of all, I would like to express my sincere gratitude to my supervisor A/Prof. Michael Sheng, a gifted teacher, an outstanding researcher and a great leader. Sheng implanted the ambition to success in me and I will never forget his words “*Aim high and never give up*”. I am still learning from him, he taught me how to be part of the research community, how to do high-quality research, how to be a good teacher and supervisor, and how to embrace my academic career. There are no enough words to express my appreciation for his encouragement and guidance. I am also grateful to my co-supervisor Prof. Hong Shen, for his continuous support, advice and motivation. There was always a constructive discussion about current research problems or future directions.

I thank my co-authors: Quan Z. Sheng, Anne H.H. Ngu, Schahram Dustdar, Sherali Zeadally, Zakaria Maamar, Jian Yu, Lina Yao, Abdullah Alfazi and Jeriel Law, for their productive and enjoyable collaborations. I would like also to thank anonymous reviewers for their valuable comments on earlier drafts of my papers.

I owe a huge debt of gratitude to my mother, my father, my wife, my little princess and prince, my brothers and my sisters for their constant encouragement and patience. They have been always there for me whenever I needed them.

Finally, I express my sincere appreciation to the Ministry of Higher Education, Kingdom of Saudi Arabia, who awarded me King’s Abdullah selective Postgraduate Scholarship and the supplementary scholarship from Taibah University, Kingdom of Saudi Arabia, to financially support me during my PhD journey.

ABSTRACT OF THE DISSERTATION

Credibility-based Trust Management and Discovery of Cloud Services

by

Talal Hashem Noor

Doctor of Philosophy in Computer Science

The University of Adelaide, 2013

Cloud computing is gaining a considerable momentum as a new computing paradigm for providing flexible and on-demand infrastructures, platforms and software as services. The trust management of services issues attracted many researchers in the past years. However, in cloud computing, with the highly dynamic, distributed and non-transparent nature of cloud services, this research area has gained a considerable significance. Robust trust management approaches will be essential in establishing trust between cloud service consumers and providers and will significantly contribute to the adoption and growth of cloud computing.

In this dissertation, we present a novel approach for credibility-based trust management and automatic discovery of cloud services in distributed and highly dynamic environments. We first propose a *Zero-Knowledge Credibility Proof Protocol* to prove the credibility of consumers' feedback without breaching consumers' privacy. We then propose an adaptive and robust *Credibility Model* for assessing the consumers' credibility in giving feedback to cloud services. To measure how experienced a consumer would be, we use the concepts of *Consumer Capability* and *Majority Consensus*. We further introduce the concepts of *Feedback Density* and *Occasional Feedback Collusion* to detect strategic and occasional behaviors of collusion attacks. To detect Sybil

attacks, we introduce the concepts of *Multi-Identity Recognition* and *Occasional Sybil Attacks*. To adjust trust results for cloud services that have been affected by malicious behaviors, we introduce the concept of *Change Rate of Trust*. We then propose a scalable *Availability Model* to manage the availability of the decentralized implementation of the trust management service. To share the workload between the trust management service nodes, we use the concept of *load balancing* thereby always maintaining a desired availability level. We introduce the concept of *operational power* to determine the optimal number of nodes and exploit particle filtering to precisely predict the availability of each node and determine the optimal number of replicas for each node.

The techniques presented in this dissertation are implemented in *Cloud Armor*, a prototype that provides a set of functionalities to deliver Trust as a Service (TaaS). Finally, we conduct extensive experimental and performance studies of the proposed techniques using a collection of real-world trust feedbacks on cloud services. We particularly develop a Cloud Service Crawler Engine for cloud services collection. The collected datasets include meta-data of nearly 6,000 real-world cloud services (1.06GB). The experimental results shows that our system i) is able to effectively distinguish between feedbacks from experienced and amateur consumers; ii) is more adaptive and robust in trust calculations by effectively detecting collusion and Sybil attacks without breaching consumers' privacy no matter attacks occur in a strategic or occasional behavior; iii) is more scalable and maintains a desired availability level in highly dynamic environments and iv) provides an efficient support for identifying, collecting, validating, categorizing and recommending cloud services based on trust.

TABLE OF CONTENTS

1	Introduction	1
1.1	Motivating Scenario	3
1.2	Research Issues	5
1.3	Contributions Overview	7
1.3.1	Zero-Knowledge Credibility Proof Protocol	7
1.3.2	Robust and Adaptive Feedback Credibility Assessment	8
1.3.3	Scalable and Distributed Service Nodes Management	9
1.3.4	Cloud Service Crawler Engine (CSCE)	9
1.3.5	Datasets Collection	10
1.3.6	Implementation and Performance Study	10
1.4	Dissertation Organization	11
2	Background	14
2.1	Overview of Services in Cloud Environments	14
2.1.1	Cloud Service Models	15
2.1.2	Cloud Service Deployment Models	17
2.2	Overview of Trust Management	20
2.2.1	Trust Management Techniques	21
2.2.1.1	Policy as a Trust Management Technique (PocT)	22
2.2.1.2	Recommendation as a Trust Management Technique (RecT)	24

2.2.1.3	Reputation as a Trust Management Technique (RepT)	26
2.2.1.4	Prediction as a Trust Management Technique (PrdT)	28
2.3	An Analytical Framework for Trust Management	29
2.3.1	Layers of the Trust Management Analytical Framework . . .	30
2.3.2	Dimensions for Evaluating Trust Management Research Pro- totypes	32
2.3.2.1	The Trust Feedbacks Sharing Layer	32
2.3.2.2	The Trust Assessment Layer	34
2.3.2.3	The Trust Results Distribution Layer	36
2.4	Research Prototypes	37
2.4.1	Overview of Major Research Prototypes	37
2.4.2	Evaluation of Trust Management Research Prototypes	43
2.4.2.1	The Trust Feedback Sharing Layer (TFSL)	45
2.4.2.2	Trust Assessment Layer (TAL)	45
2.4.2.3	Trust Result Distribution Layer (TRDL)	46
2.5	Cloud Service Providers	48
2.5.1	Trust Characteristics in Cloud Services	48
2.5.2	Comparison of Major Cloud Service Providers	50
2.6	Summary	52
3	A Framework for Trust Management and Discovery of Cloud Services .	55
3.1	Design Overview	56
3.2	The Zero-Knowledge Credibility Proof Protocol	59

3.2.1	Identity Management Service (IdM)	60
3.2.2	Trust Management Service (TMS)	61
3.2.3	Assumptions and Attack Models	62
3.3	Related Work	63
3.4	Summary	64
4	A Robust and Adaptive Credibility Model for Feedback Credibility Assessment	67
4.1	Consumer Experience	68
4.1.1	Consumer Capability	69
4.1.2	Majority Consensus	70
4.2	Feedback Collusion Detection	71
4.2.1	Feedback Density	71
4.2.2	Occasional Feedback Collusion	74
4.3	Sybil Attacks Detection	76
4.3.1	Multi-Identity Recognition	76
4.3.2	Occasional Sybil Attacks	78
4.4	Feedback Credibility	80
4.5	Change Rate of Trust Results	80
4.6	Related Work	83
4.7	Summary	84
5	A Scalable Availability Model for Distributed Service Nodes Management	86
5.1	Operational Power	87

5.2	Replication Determination	89
5.3	Trust Result Caching	94
5.4	Instances Management	94
5.5	Related Work	96
5.6	Summary	99
6	Cloud Service Crawler Engine (CSCE)	102
6.1	Design Overview	104
6.2	Cloud Services Ontology	107
6.3	Datasets Collection	111
6.4	Design Challenges	113
6.5	Related Work	115
6.6	Summary	116
7	Implementation and Performance Study	119
7.1	Cloud Armor Overview	120
7.1.1	The Trust Data Provisioning Layer	120
7.1.2	The Trust and Credibility Assessment Function Layer	121
7.1.3	The Trust-Based Cloud Services Recommendation Layer	122
7.2	Demo Scenario	124
7.2.1	Provisioning Trust Data	125
7.2.2	Assessing Trust and Credibility	126
7.2.3	Recommending Cloud Services Based on Trust Results	126
7.3	Statistical Analysis and Crawling Results	127

7.3.1	Cloud Services Identification	127
7.3.2	Locations and Languages	129
7.3.3	Cloud Service Providers Categorization	132
7.3.4	Cloud Services and Quality of Service (QoS)	133
7.3.5	Cloud Computing and Service-Oriented Computing (SOC) . .	134
7.3.6	Discussion	137
7.4	Experimental Evaluations and Performance Studies	138
7.4.1	Credibility Model Experiments	138
7.4.1.1	Consumer Experience Determination	141
7.4.1.2	Robustness Against Collusion Attacks	143
7.4.1.3	Robustness Against Sybil Attacks	145
7.4.2	Availability Model Experiments	147
7.4.2.1	Availability Prediction Accuracy	147
7.4.2.2	Trust Results Caching Accuracy	148
7.4.2.3	Reallocation Performance	149
7.5	Summary	150
8	Conclusions	153
8.1	Summary	153
8.2	Future Directions	157
	Bibliography	164
A	Curriculum Vitae	179

LIST OF FIGURES

1.1	Motivating Scenario	4
2.1	Cloud Service Models	17
2.2	Cloud Service Deployment Models	18
2.3	Trust Management Perspectives	21
2.4	Trust Management (TM) Techniques	25
2.5	Architecture of the Trust Management Analytical Framework	31
2.6	Evaluation of Trust Management Research Prototypes	44
2.7	Statistical Information of Research Prototypes Evaluation	47
3.1	The Trust Management Framework	57
4.1	Trust Feedback Density Determination	73
4.2	Occasional Attacks Detection	75
4.3	The Identity Records Matrix (IM) Translation to the Multi-Identity Recognition Matrix (MIRM)	77
5.1	Particle Filtering based Algorithm	92
5.2	Trust Management Service Replication Number Determination	93
5.3	Trust Results & Credibility Weights Caching Algorithm	95
5.4	Instances Management Algorithm	97
6.1	Architecture of the Cloud Service Crawler Engine	105
6.2	Cloud Service Discovery Algorithm	108

6.3	A Small Part of the Cloud Services Ontology	109
6.4	Advertised Cloud Services	112
7.1	Cloud Armor's Architecture	121
7.2	The Cloud Services Trust Assessment	125
7.3	Trust-Based Cloud Services Recommendation	127
7.4	Cloud Services Location Detection	131
7.5	Languages Used in Cloud Services	132
7.6	Cloud Service Providers Categorization	133
7.7	Cloud Service Consumers Trust Feedback	134
7.8	Cloud Services in WSDL/WADL	135
7.9	Cloud Services Advertised on Search Engines	136
7.10	Cloud Services' IPs	136
7.11	Attacking Behavior Models	140
7.12	With Consumer Experience factors VS. Without Consumer Experience factors	142
7.13	Consumer Capability factor VS. Majority Consensus factor	143
7.14	Robustness Against Collusion Attacks Experiments	144
7.15	Robustness Against Sybil Attacks Experiments	146
7.16	Availability Prediction Accuracy: Actual Availability VS. Estimated Availability	148
7.17	Trust Results Caching Accuracy	149
7.18	Reallocation Performance	151

LIST OF TABLES

2.1	Notation and Meanings in Chapter 2	29
2.2	Comparison: Representative Cloud Service Providers VS. Service Trust Characteristics	51
4.1	Notation and Meanings in Chapter 4	82
5.1	Notation and Meanings in Chapter 5	96
7.1	Enabling Technologies in Cloud Armor	124
7.2	Breakdown of Cloud Services Crawling Results	128
7.3	Error Codes for Inactive Cloud Services	129
7.4	Behavior Experimental Design	141