Achieving Trust-oriented Data Protection in the Cloud Environment

A thesis submitted in fulfilment of the requirements for

the degree of Doctor of Philosophy

ARN laboratory, iNext research centre

University of Technology, Sydney

by

Lingfeng Chen

Supervised by

Professor Doan B. Hoang

2014

DEDICATION

To my Parents and my Grandparents

To my Wife and my Parents-in-Law

Thank you for your love and support

ACKNOWLEDGEMENTS

I sincerely express my deepest gratitude to my principal supervisor, Professor Doan B. Hoang, for his supervision and continuous encouragement throughout my whole PhD study. His guidance, wisdom, and enthusiasm have made me both more mature as a person and more confident to be a good researcher. He has been outstanding in providing insightful feedback and creating the perfect balance of my research engagement and my casual teaching work. From the beginning of determining the research direction to publishing fruitful research outcome, he always commits to foster my research skills. Without his guidance, I would still be in the marsh of research career. Further, I thank him for offering me a number of research grants that were really helpful to support my research and study. I feel so fortunate to have him as my supervisor for the past three and half years.

I thank the University of Technology Sydney for offering me an IRS scholarship throughout my doctoral program. I also thank the iNext research centre for providing valuable resources, including funding for attending conferences. Special thanks go to the School of Computing and Communication at the University of Technology Sydney for offering me the teaching internship that has significantly increased my teaching experience in academia. Thanks to these funding and support, that makes me could concentrate on my research work without the burden of living.

My thanks also go to staff members and research students in the ARN lab for their help, suggestions, friendship and encouragement: special thanks to Fatima Furqan, Dr. Minh Hoang Phung, Dr. Venki Balasubramanian, Najmeh Kamyabpour, Nor Faizah Ahmad.

Furthermore, I thank my parents for their upbringing and encouragement to succeed in my study and my grandparents for their meticulous care and attention. Then, I express my gratitude and appreciation to my wife for her love and support. Her selfless sacrifices and commitment to the family, made it possible for me to finish my PhD studies. Finally, I would like to thank my brother, my parents and brother-in-law for their encouragement, and thank all the people who helped me and contributed to this study.

CERTIFICATE OF ORIGINAL AUTHORSHIP

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Student:

Date:

THE AUTHOR'S PUBLICATIONS

International Conference Publications and Proceedings:

CHEN, L. & HOANG, D. B. 2013. Adaptive data replicas management based on active data-centric framework in cloud environment. 2013 IEEE International conference on High Performance Computing and Communications (HPCC). (ERA ranking: B)

CHEN, L. & HOANG, D. B. 2013. Addressing data and user mobility challenge in the cloud. 2013 IEEE International conference on Cloud Computing (CLOUD), 549-556. (ERA ranking: B)

CHEN, L. & HOANG, D. B. 2012. Active data-centric framework for data protection in cloud environment. 2012 23rd Australasian Conference on Information Systems (ACIS), 1-11. (ERA ranking: A)

CHEN, L. & HOANG, D. B. 2011. Towards scalable, fine-grained, intrusion-tolerant data protection models for healthcare cloud. 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 126-133. (ERA ranking: A)

CHEN, L. & HOANG, D. B. 2011. Novel data protection model in healthcare cloud. 2011 IEEE International Conference on High Performance Computing and Communications (HPCC), 550-555. (ERA ranking: B)

HOANG, D. B. & CHEN, L 2010. Mobile Cloud for Assistive Healthcare (MoCAsH). 2010 IEEE International Conference on Asia-Pacific Services Computing Conference (APSCC), 6-10 Dec. 2010. 325-332. (ERA ranking: C)

ABSTRACT

Cloud computing has gained increasing acceptance in recent years. In privacy-conscious domains such as healthcare and banking, however, data security and privacy are the greatest obstacles to the widespread adoption of cloud computing technology. Despite enjoying the benefits brought by this innovative technology, users are concerned about losing the control of their own data in the outsourced environment. Encrypting data can resolve confidentiality and integrity challenges, but the key to mitigating users' concerns and encouraging broader adoption of cloud computing is the establishment of a trustworthy relationship between cloud providers and users.

In this dissertation, we investigate a novel trust-oriented data protection framework adapted to the cloud environment. By investigating cloud data security, privacy, and control related issues, we propose a novel data protection approach that combines active and passive protection mechanisms. The active protection is used to secure data in an independent and smart data cube that can survive even when the host is in danger. The passive protection covers the actions and mechanisms taken to monitor and audit data based on third party security services such as access control services and audit services. Furthermore, by incorporating full mobility and replica management with the active and passive mechanisms, the proposed framework can satisfy *confidentiality*, *integrity*, *availability*, *scalability*, *intrusion-tolerance*, *authentication*, *authorization*, *auditability*, and *accountability*, increasing users' confidence in consuming cloud-based data services.

In this work we begin by introducing cloud data storage characteristics and then analyse the reasons for issues of data security, privacy and control in cloud. On the basis of results of analysis, we identify desirable properties and objectives for protecting cloud data. In principle, cryptography-based and third party based approaches are insufficient to address users' concerns and increase confidence in consuming cloud-based data services, because of possible intrusion attacks and direct tampering of data. Hence, we propose a novel way of securing data in an active data cube (ADCu) with smart and independent functionality. Each ADCu is a deployable data protection unit encapsulating sensitive data, networking, data manipulation, and security

verification functions within a coherent data structure. A sealed and signed ADCu encloses dynamic information-flow tracking throughout the data cube that can precisely monitor the inner data and the derivatives. Any violations of policy or tampering with data would be compulsorily recorded and reported to bundled users via the mechanisms within the ADCu. This active and bundled architecture is designed to establish a trustworthy relationship between cloud and users.

Subsequently, to establish a more comprehensive security environment cooperating with an active data-centric (ADC) framework, we propose a cloud-based privacy-aware role-based access control (CPRBAC) service and an active auditing service (AAS). These components in the entire data protection framework contribute to the passive security mechanisms. They provide access control management and audit work based on a consistent security environment. We also discuss and implement full mobility management and data replica management related to the ADCu, which are regarded as significant factors to satisfy data accountability, availability, and scalability.

We conduct a set of practical experiments and security evaluation on a mini-private cloud platform. The outcome of this research demonstrates the efficiency, feasibility, dependability, and scalability of protecting outsourced data in cloud by using the trust-oriented protection framework. To that end, we introduce an application applying the components and mechanisms of the trust-oriented security framework to protecting eHealth data in cloud.

The novelty of this work lies in protecting cloud data in an ADCu that is not highly reliant on strong encryption schemes and third-party protection schemes. By proposing innovative structures, concepts, algorithms, and services, the major contribution of this thesis is that it helps cloud providers to deliver trust actively to cloud users, and encourages broader adoption of cloud-based solutions for data storage services in sensitive areas.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AA	Active Auditor
AAS	Active Auditing Service
ABAC	Attribute Based Access Control
ACID	Atomicity, Consistency, Isolation, and Durability
ACL	Access Control List
ADC	Active Data-centric
ADCu	Active Data Cube
ADNI	Active Data Network Information
AES	Advanced Encryption Standard
AF	Access Frequency
AP	Access Point
AS	Attribute Set
ATC	Average Time Consumption
CIA	Cloud Information Accountability
CPRBAC	Cloud-based Privacy-aware Role-Based Access Control
CR	Consistency Requirement
CR	Concurrent Requests
CSPs	Cloud Service Provider
CT	Current Time
DAC	Discretionary Access Control
Ddes	Data Descriptor
DMM	Data Mobility Management
DP	Data Permission

DPA	Data Permission Assignment
EHR	Electronic Health Record
EPAL	Enterprise Privacy Authorization Language
ES	Executable Segment
GCM	Google Cloud Messaging
GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
HWNE	Heterogeneous Wireless Network Environment
IaaS	Infrastructure as a Service
JAR	Java Archive
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LSP	Location Service Provider
MAC	Mandatory Access Control
MQTT	Message Queue Telemetry Transport
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OC	Operation Cost
ODBC	Open Database Connectivity
OS	Operation System
PaaS	Platform as a Service
PDP	Provable Data Possession
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PI	Pervasive Informing

PK	Pervasive Knowing
PL	Participants List
POR	Proof Of Retrievability
QoS	Quality of Service
RA	Role Assignment
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control
RESTFUL	Representational State Transfer
RMI-SSL	Remote Method Invocation over Secure Socket Layer
SaaS	Software as a Service
SAN	Storage Area Networks
SAML	Security Assertion Markup Language
SID	Security Identifier
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TDFS	Triggerable Data File Structure
TPM	Trusted Platform Module
TCG	Trusted Computing Group
TLS	Transport Layer Security
TTL	Time-To-Live
UF	Update Frequency
UMM	User Mobility Management
UUID	Universally Unique Identifier

VLAN	Virtual Local Area Networks
VM	Virtual Machine
VT	Verification Token
WS	Web Service
WSDL	Web Services Description Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
ZK	Zero-Knowledge