



***A MULTI-LEVEL FRAMEWORK FOR EFFICIENT SENSITIVE DATA
TRANSMISSION IN CLOUD COMPUTING***

HAIFAA JASSIM MUHASIN

FSKTM 2019 46



**A MULTI-LEVEL FRAMEWORK FOR EFFICIENT SENSITIVE DATA
TRANSMISSION IN CLOUD COMPUTING**

By

HAIFAA JASSIM MUHASIN

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfillment of the Requirements for the Degree of Doctor of Philosophy**

June 2019

COPYRIGHT

All material contained within the thesis, including without limitation text, logos, icons, photographs, and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia



DEDICATION

This thesis is dedicated to my dear Father, to spirit of my dear Mother, to the spirit of my dear sister Huda, to my beloved Husband Malik, to my beloved Brothers and Sisters, to my wonderful Daughter Farkad and my beloved Son Sarmad and his beloved wife Eman for their endless love, support, and encouragement



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment
of the requirement for the degree of Doctor of Philosophy

**A MULTI-LEVEL FRAMEWORK FOR EFFICIENT SENSITIVE DATA
TRANSMISSION IN CLOUD COMPUTING**

By

HAIFAA JASSIM MUHASIN

June 2019

Chairman : Associate Professor Rodziah Atan, PhD
Faculty : Computer Science and Information Technology

Cloud computing, as a growing field, can provide the needs of enterprises and individuals to access cloud computing resources and meet their organizational computing requirements. The popularity of cloud computing is characterized by a number of great features, such as scalability, low cost and unlimited resources. These features have encouraged many organizations and individuals to transfer their data over the cloud. However, cloud computing is constrained by security and privacy issues, particularly by factors on confidentiality, integrity, availability and privacy, apart from access control, management and internal attacks. These issues have become a major challenge in using the cloud, especially when dealing with sensitive data.

The aim of this study is to address the problem of protection in terms of privacy and security of data from the perspective of management of information systems (MIS) and its decision-making process. Here, the factors related to the management and protection of sensitive data in cloud computing are data confidentiality (DC), data integrity (DI), data privacy (DP) and data availability (DA). The analyses of these factors are performed on the basis of the interests of managers and individuals whose aim is to protect sensitive data over the cloud.

The experimental study in this research includes a pilot study, the development of a tool as a proof of concept and an experts' interview. The tool, which is developed on the basis of the proposed framework, is verified by the interviewed experts and through tool execution. The results from the interviews confirm the validity and workability of the proposed framework in enhancing the decision making of MIS and managing and protecting sensitive data over the cloud. Subsequently, the

anonymization method of the proposed framework is compared with the encryption approach of previous work.

The research applies the anonymization technique and classifies the contents of a sensitive data file by the k-anonymity technique, which can efficiently protect sensitive data and reduce the transmission time and size of a file sent over the cloud. The digital signature of the file containing sensitive data is generated and sent together with the file to ensure DI. Private and confidential data management issues of intrusion and data loss over the cloud are solved by using the proposed multi-level framework, which applies the method of responsible participation to maintain DC and DA upon request—the other major contribution of this research.

This study has achieved its stated objectives. The results obtained by the experimental study are aligned with the proposed framework and the concept of protection and management of private confidential data for effective information management decision making.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

**RANGKA KERJA BERBILANG ARAS BAGI PENGHANTARAN DATA
SENSITIF YANG CEKAP DALAM PENGKOMPUTERAN AWAN**

Oleh

HAIFAA JASSIM MUHASIN

Jun 2019

Pengerusi : Profesor Madya Rodziah Atan, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Pengkomputeran awan adalah bidang yang berkembang, mengemukakan keperluan enterpris dan individu untuk capaian sumber dalam komputeran awan bagi memenuhi keperluan pengkomputeran organisasi tersebut. Kepopularan komputeran awan adalah berdasarkan banyak ciri-ciri hebat seperti penskalaan, kos yang rendah dan sumber tanpa had. Ciri-ciri ini menggalakkan organisasi dan individu untuk memindah data mereka ke dalam awan. Justeru itu, keselamatan dan kerahsiaan menjadi isu utama dalam pengkomputeran awan yang melibatkan faktor-faktor kerahsiaan, keutuhan, kebolehsediaan dan kerahsiaan, juga kawalan capaian, pengurusan dan serangan dari dalam. Kerisauan ini menjadi cabaran terbesar dalam pengkomputeran awan, terutamanya apabila melibatkan data yang sensitif.

Matlamat kajian ini adalah untuk menumpukan perhatian terhadap permasalahan berkaitan perlindungan data peribadi dan keselamatannya dari perspektif pengurusan sistem maklumat dan pembuatan keputusan.

Faktor pengurusan dan perlindungan data sensitif dalam perkomputeran awan yang dikaji dalam kajian ini adalah kerahsiaan data (DC), keutuhan data (DI), privasi (DP) dan kebolehsediaan (DA). Analisa kepada keempat-empat faktor telah dilaksanakan berdasarkan keputusan profesional pengurus-pengurus ini. Kepentingan perkaitan.

Kajian eksperimen yang dilaksanakan dalam penyelidikan ini merangkumi kajian awal, pembangunan peralatan sebagai pembuktian konsep dan temubual pakar. Peralatan ini dibangunkan berasaskan rangka kerja yang dicadangkan dan peralatan

ini telah diverifikasi oleh pakar melalui sesi temubual dan pelaksanaan peralatan. Hasil dari temubual mengesahkan kesahihan dan kebolehlaksana rangka kerja yang dicadangkan bagi mempertingkatkan pengurusan pembuatan keputusan sistem maklumat data sensitif dalam persekitaran awan. Selanjutnya, kaedah *anonymization* rangka kerja yang dicadangkan dibandingkan dengan pendekatan penyulitan kerja sebelumnya.

Kajian ini mengaplikasi teknik *anonymization* dan pengelasan kandungan fail data sensitif menggunakan teknik *k-anonymity*, yang terbukti cekap untuk melindungi data sensitif, masa penghantaran lebih pantas dan saiz fail diubah yang lebih kecil yang akan dihantar ke awan. Tandatangan digital yang spesifik bagi fail yang mengandungi data sensitif tersebut akan dijana dan dihantar bersekali dengan fail bagi memastikan keutuhan data di pihak penerima. Isu pengurusan data peribadi dan sulit seperti penyamaran dan kehilangan data dalam awan dapat dicegah dengan menggunakan rangka kerja berbilang aras yang dicadangkan ini, yang mengaplikasi pendekatan penyertaan bertanggungjawab, bagi mengekalkan kerahsiaan dan kebolehcapaian fail berkeselamatan.

kajian ini telah mencapai objektif yang dinyatakan. Keputusan yang diperolehi melalui kajian eksperimental adalah selaras dengan objektif rangka kerja yang selaras dengan cabaran dalam perlindungan dan pengurusan data persendirian dan rahsia bagi pengurusan pembuatan keputusan maklumat yang lebih cekap.

ACKNOWLEDGEMENTS

In the Name of Allah, The Most Gracious and The Most Merciful Alhamdulillah, all Praises to Allah for blessing, mercy, and guidance in complete this work, and help me in every moment of my life.

I would like to express my thanks and gratitude to my supervisor Assoc. Prof. Dr. Rodziah binti Atan for her encouragement, support in all stages of the research work and provide assistance during the work, giving me experiences throughout the work.

And I would like to thank my committee members Assoc. Prof. Dr. Marzanah binti A. Jabar, Dr. Salfarina binti Abdullah for their encouragement, support, and insightful suggestions.

Also, I would like to thank my family: My husband Malik Jabbar for his help, support and encouragement. And my son Sarmad and his wife Eman, my daughter Farkad for their support and encouragement.

I certify that a Thesis Examination Committee has met on 20 June 2019 to conduct the final examination of Haifaa Jassim Muhasin on her thesis entitled "A Multi-Level Framework for Efficient Sensitive Data Transmission in Cloud Computing" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Rusli bin Hj Abdullah, PhD

Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Abu Bakar b Md Sultan, PhD

Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Wan Nurhayati binti Wan Ab. Rahman, PhD

Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Ali bin Selamat, PhD

Professor
Malaysia Japan International Institute of Technology
Universiti Teknologi Malaysia
Malaysia
(External Examiner)



ROBIAH BINTI YUNUS, PhD

Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 4 September 2019

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Rodziah binti Atan, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Marzanah A. Jabar, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

Salfarina binti Abdullah, PhD

Senior Lecturer

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

ROBIAH BINTI YUNUS, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____

Date: _____

Name and Matric No: Haifaa Jassim Muhasin, GS43046

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman
of Supervisory
Committee: Associate Professor Dr. Rodziah binti Atan

Signature: _____
Name of Member
of Supervisory
Committee: Associate Professor Dr. Marzanah A. Jabar

Signature: _____
Name of Member
of Supervisory
Committee: Dr. Salfarina binti Abdullah

TABLE OF CONTENTS

	Page
ABSTRACT	i
ABSTRAK	iii
ACKNOWLEDGEMENTS	v
APPROVAL	vi
DECLARATION	viii
LIST OF TABLES	xiii
LIST OF FIGURES	xiv
LIST OF ABBREVIATIONS	xvi
CHAPTER	
1 INTRODUCTION	1
1.1 Overview	1
1.2 Research Problem	2
1.3 Research Questions	3
1.4 Research Objectives	4
1.5 Research Motivation	4
1.6 Research Contributions	4
1.7 Research Scope	4
1.8 Thesis Organization	5
2 LITERATURE REVIEW	6
2.1 Introduction	6
2.2 Cloud Computing Environment	6
2.3 Information Systems	8
2.4 Management Information Systems	10
2.5 Data Management	11
2.6 Decision Making	12
2.7 Sensitive Data	13
2.7.1 Data Anonymization	14
2.7.2 Digital Signature	15
2.8 Security and Privacy in Transmitted Data Management	16
2.8.1 Confidentiality in Data Management	16
2.8.2 Privacy in Data Management	18
2.8.3 Integrity and authorization in Data Management	19
2.8.4 Availability in Data Management	20
2.8.5 Authentication in Data Management	20
2.8.6 Anonymization in Data Management	20
2.9 Data Security and Privacy Requirements	21
2.10 Management Sensitive Data Models and Methods	23
2.11 Gap Analysis	25
2.12 Summary	31

3	RESEARCH METHODOLOGY	32
3.1	Introduction	32
3.2	Research Activity Design	32
3.2.1	Related Work Reviews	33
3.2.2	Framework Design	34
3.2.3	Pilot Study Design	34
3.2.4	Research Design	38
3.2.5	Implementation of MLF Tools	39
3.2.6	Validity and Data Analysis Design	39
3.3	Summary	39
4	NEW PROPOSED MULTI-LEVEL FRAMEWORK	40
4.1	Introduction	40
4.2	Sensitive Data Management Factors	40
4.2.1	Hypothesis Model	42
4.3	MLF Design	44
4.3.1	Part 1: User-Side Module Design	46
4.3.1.1	Data Anonymity	49
4.3.1.2	Digital Signature Creation	52
4.3.2	Part 2: Cloud-Side Module Design	57
4.3.2.1	User Authorization Module	63
4.3.2.2	Authentication Module	66
4.3.2.3	Save or Retrieve Data File	74
4.3.2.4	User Request	77
4.4	Summary	79
5	RESULTS AND DISCUSSION	80
5.1	Introduction	80
5.2	Results of Pilot Study	80
5.2.1	Structured Interview Results	80
5.2.2	Survey Results	85
5.3	Programming Language	92
5.4	User Side	93
5.4.1	Data Anonymity Function	93
5.4.2	Digital Signature Creation	94
5.5	Cloud Side	94
5.5.1	User Authorization	95
5.5.2	Authentication	96
5.5.3	Save or Retrieve Data File	97
5.6	Validation of the Current Research	97
5.6.1	Validation of the Proposed MLF	99
5.6.2	Validation of the Implementation Program	101
5.6.3	Validation of the Contributions of the Research	102
5.7	Comparison of results of our research and those of previous studies	103
5.8	Discussion	104
5.9	Summary	105

6	CONCLUSION AND FUTURE WORK	106
6.1	Introduction	106
6.2	Conclusion	106
6.3	Contribution of the Current Research	107
6.4	Future Research	107
	REFERENCES	109
	APPENDICES	119
	BIODATA OF STUDENT	184
	LIST OF PUBLICATIONS	185



LIST OF TABLES

Table		Page
2.1	Factors that influence the information system decision on sensitive data management	21
2.2	Gap analysis	26
2.3	Factors that affect sensitive data in cloud computing and their connection to related work	27
5.1	Results of the structured interviews	83
5.2	Frequency of responses from the nine experts, with percentages	84
5.3	Mapping the hypotheses of the MLF framework based on the instrument questions and the results of the reliability tests	87
5.4	Statistics of reliability coefficients 1	91
5.5	Statistics of reliability coefficients 2	92
5.6	Validation test from the experts' interview	98
5.7	Details of interview respondents for validation research	98
5.8	Comparison between anonymity and encryption of files in terms of time and size	104
5.9	Evaluation and validation objectives	105

LIST OF FIGURES

Figure	Page	
2.1	Distinct functions of information systems	10
2.2	Classification of attributes in anonymization technique	15
2.3	Factors the affect sensitive data management over the cloud	23
3.1	Research activities	33
3.2	Pilot experiment design and processes	35
4.1	The research model with the factors of decision making of information systems on sensitive data management	41
4.2	Proposed model hypothesis	42
4.3	Proposed MLF	43
4.4	The proposed framework explains all parts and modules	46
4.5	Flow of user-side modules	47
4.6	User-part module flowchart	48
4.7	Main screen of the user-part modules	49
4.8	File content before sending. (pre-anonymization)	50
4.9	File content after anonymiztion (post-anonymization)	50
4.10	Data anonymity module flow	51
4.11	Asymmetric encryption method of RSA to compute hash $H(M)$	54
4.12	Digital signature by DSA for sensitive data file flow	57
4.13	Management information system of sensitive data in cloud computing for the comprehensive flow of the MLF tool	60
4.14	Registration page	61
4.15	Login page	61
4.16	Sign-in login page	62
4.17	Main screen to manage sensitive data in cloud computing	62
4.18	User authorization flow	64

4.19	Manager directory attributes	66
4.20	Authentication flow	68
4.21	'Entered encrypted code' flow	69
4.22	'Verify Digital Signature' Flow	73
4.23	SAP directory and shared file directory attributes	74
4.24	'Save or Retrieve Data File' Flow	75
4.25	CSP directory attributes	76
4.26	User request flow	78
5.1	User-side interface screen	93
5.2	Cloud-side main interface screen	95

LIST OF ABBREVIATIONS

CSLs	Certificate Symbols Lists
CSP	Cloud Service Provider
DA	Data Availability
DAMA	Data Management Association
DC	Data Confidentiality
DI	Data Integrity
DP	Data Privacy
DSA	Digital Signature Algorithm
IaaS	Infrastructure-as-a-Service
IDEC	Information and communications Development Center
IS	Information System
ISMS	Information Security Management Systems
IT	Information Technology
LR	Literature Review
MCDB	Multi Cloud DataBase
MIS	Management Information Systems
MLF	Multi-level Framework
NIST	National Institute for Standards and Technology
NoAcM	Number of Access Control from Manager
NoAu	Number of Access User
NoAUs	Number of Authorized Users
NoDCs	Number of Data Centers
NoDTs	Number of Data Types
NoEncCs	Number of Encrypted Codes
NoRs	Number of Resources

NoSecPrM	Number of Security and Privacy Mechanism
PaaS	Platform-as-a-Service
PHR	Personal Health Record
PII	Personally Identifiable Information
SaaS	Software-as-a-Service
SAP	Security Auditor Party
SPSS	Statistical Package for the Social Science



CHAPTER 1

INTRODUCTION

1.1 Overview

Cloud computing offers three major types of service models: software-as-a-service (SaaS) model, platform-as-a-service (PaaS) model and infrastructure-as-a-service (IaaS) model. The information technology (IT) of a cloud computing infrastructure consists of networks based on IP software, services and virtual interfaces. The cloud uses different models of services, such as hybrid, community, private or public cloud models. Cloud computing has created a new understanding amongst companies and organizations in conducting information exchange. This scheme requires the existence of a third party, also called a service provider in cloud computing, to manage the relationship. The relationships in cloud computing creates many security and privacy gaps. Thus, security in cloud computing is mainly focused on protection and the guarantee of data transmission security.

Knowing who the users are and what services are equipped by the cloud is important in understanding the risks of and threats to data storage over the cloud. Youseff et al. (2008) defined users (also called clients or customers) as individuals, companies or governments seeking the use of infrastructure and services over the cloud, whereas service providers are individuals, companies or governments with abilities to offer infrastructure and services for general consumption.

Modern cloud computing technology has enabled the access of required resources, such as servers, applications, network and services. The process utilizes common computing models based on data traffic, in which a third party handles the regulation (Kumar and Vajpayee, 2016). Security and privacy remain the major challenge in handling sensitive information in the cloud environment (Loganayagi and Sujatha, 2012). Sensitive information is defined as data that must be protected from unauthorised access to safeguard the privacy and security of individuals or organisations (Rouse, 2014).

Sensitive data represent the data related to a person or an organization, such as social security number, driver's license number, credit card number, medical and health data, financial data or confidential legal and personally identifiable information (PII). PII, including name, address, phone number or e-mail address, is a type of information that identifies a person and can be used to identify or locate a person. The three main types of sensitive data are *personal information*, *business information* and *classified information* (Rouse, 2014).

This study is conducted to seek the factors affecting sensitive data and the transmission of information by public cloud domain management. Subsequently, a framework for the effective decision making of information systems is proposed for the management of sensitive data and private information.

1.2 Research Problem

Managing data security and privacy is difficult, but the situation is more difficult in cloud computing. The cloud environment is intangible, and data are handled by software dispersed from the user's location. Thus, privacy and security are a major challenge for many companies and users (Loganayagi and Sujatha, 2012). The above problems can be explained in three aspects: data, privacy and security and persons or companies:

The first aspect related to data can be further divided into three issues.

- i. Data integrity:* This aspect may include cases, such as error cases, when data are transmitted from one place to another or from one computer to another. The other possible issue is exposure to hardware and system malfunctions, such as viruses or crashed disks (Anitha, 2013).
- ii. Data access control:* Private data can be accessed illegally due to the lack of access control to confidential data. The accessibility of sensitive data in the cloud computing environment is regarded a security challenge and thus needs to be addressed (Anitha, 2013).
- iii. Loss of data and stolen data:* Cloud computing is used to process and store data on external servers for cost-effective and flexible operation. However, this feature opens opportunities for data theft, which is a serious problem in cloud computing, especially with financial or banking transactions (Anitha, 2013).

The second aspect is related to privacy and security.

- i. Protection and privacy:* The security of personal information is extremely important in cloud computing. Most servers are located externally, which implies that vendors must ensure the security of information from other operators (Anitha, 2013).
- ii. Infected and malicious applications:* A service provider needs to have the full right to use the server for the purpose of observing and preserving the server (Anitha, 2013). This scheme can prevent intruders from sending infected applications to the cloud; moreover, this problem will strongly affect cloud service and client service (Anitha, 2013).

The third aspect is related to persons or companies.

- i. User-level security issues:* Users must ensure that their own data can be protected from losses or manipulation by other users in the same cloud (Anitha, 2013).
- ii. Provider-level security issues:* Providers should install layers of security features for customers and users (Anitha, 2013).

Most approaches and processes in the previous research to assure data privacy (DP) are limited to common methods, such as data encryption, that require high time and space costs for data storage, which subsequently lead to slow transmission speed for data storage and retrieval. The encryption technology also needs alternative encryption keys to reduce risks against unauthorized detection and penetration, which may lead to data breach (Xu et al., 2013; Gupta et al., 2014; Liu et al., 2014; Tebaa and Hajji, 2014; Zhao et al., 2014; Jogdand et al., 2015).

This research addresses all the above three issues related to data or information protection against malicious insiders (Zhou, 2013; Chintawar and Ismail, 2014), security issues due to breaches and losses (Khan, 2013; Daniel, 2014; Liu et al., 2014) and loss of privacy of sensitive data of organizations and users who transmit data over the public cloud domain, especially because the cloud environment is used to process and store data.

1.3 Research Questions

The following questions are forwarded in this research, which is about sensitive data management over the public cloud domain, for the effective decision making of information systems:

- 1- How can privacy and sensitive data transmission management be effectively achieved in public cloud computing?
- 2- What policy attributes and factors are needed to manage sensitive data in cloud computing?
- 3- How can the factors be effectively combined into a method to manage sensitive data in cloud computing?

1.4 Research Objectives

The main objectives of this research are as follows:

- 1- To propose a multi-level framework (MLF) to enhance the privacy of sensitive data and prevent data breach and data loss.
- 2- To define the main factors that affect the decision making of information systems for the management of sensitive data transmission.
- 3- To develop a tool to manage the transfer of sensitive data to cloud-computing storage space.

1.5 Research Motivation

The review of previous studies highlights the importance of protecting and managing sensitive data in cloud computing. Considering that the three aspects are inadequately studied from the MIS perspective in the previous research, the present study is motivated to provide a framework for data protection, privacy and security from the MIS perspective.

1.6 Research Contributions

This research offers the following contributions:

- i. The factors that affect the decision making of information systems for sensitive data management in cloud computing environments are defined.
- ii. A framework to enhance the management of sensitive data in cloud environments is verified.
- iii. A tool to support and prove the framework is proposed.
- iv. The results of an experimental test are used as evidence to prove that the proposed framework can effectively manage sensitive data.

1.7 Research Scope

This research is scoped down to protect transmissions for sensitive and private data in public cloud environment. The protection covers attacks from malicious insiders, security breaches and data losses from private and confidential files to public clouds. Due to many available factors for the management and protection of sensitive data, which are not pertinent to the study scope, therefore, this study only focuses on confidentiality, integrity, privacy and availability factors. Public cloud environment is the domain for this study as it is popularly used to process and store data, including private and confidential data.

1.8 Thesis Organization

This thesis is divided into seven chapters. The first chapter is about the introduction and explains briefly the problem statement, research questions, research objectives and research contribution.

Chapter 2, which is about the literature review, presents the definition of cloud computing and discusses its characteristics, technology and security and compliance. Chapter 2 also includes a discussion about MIS and its decision-making process and the scope of this research.

Chapter 3 describes the research methodology, including the justification of the research design, population and sample, instrumentation and data collection and analysis.

Chapter 4 describes the design and the implementation of the new proposed MLF and its practical applications.

Chapter 5 presents the analysis of the results, the validation results, and related discussions.

Chapter 6 concludes the research and presents recommendations for future research.

REFERENCES

- Abbasi, A. G. (2011). Generic Security Framework for Cloud Computing Environments. *Doctoral Dissertation in Communication Systems, School of Information and Communication Technologies (ICT) Stockholm, Sweden.*
- AbuOliem, A. (2013). Cloud Computing Regulation: An attempt to protect Personal Data transmission to Cross-Border Cloud Computing Storage Services. *International Journal of Computer and Communication Engineering*, 2(4), 521.
- Aguiar, E., Zhang, Y., & Blanton, M. (2014). An overview of issues and recent developments in cloud computing and storage security. In *High Performance Cloud Auditing and Applications* (pp. 3-33). Springer, New York, NY.
- Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. In *Data Mining and Intelligent Computing (ICDMIC), 2014 International Conference on* (pp. 1-6). IEEE.
- Allard, T., Anciaux, N., Bouganim, L., Guo, Y., Le Folgoc, L., Nguyen, B., ... & Yin, S. (2010). Secure personal data servers: a vision paper. *Proceedings of the VLDB Endowment*, 3(1-2), 25-35.
- Alter, S. (2008). Defining information systems as work systems: implications for the IS field. *European Journal of Information Systems*, 17(5), 448-469.
- AlZain, M. A., Soh, B., & Pardede, E. (2012). A new model to ensure security in cloud computing services. *Journal of Service Science Research*, 4(1), 49-70.
- Anitha, Y. (2013). Security issues in cloud computing-A Review. *International Journal of Thesis Projects and Dissertations (IJTPD)*, 1(1), 1-6.
- Asarani, N. A. M., & Ab Rahim, N. Z. (2016). Preliminary study of online training implementation from multiple respective in Malaysia public sector. *Journal of Theoretical and Applied Information Technology*, 90(1), 77.
- Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). Cloud computing synopsis and recommendations. *NIST special publication*, 800, 146.
- Baldwin, A., Beres, Y., Duggan, G. B., Mont, M. C., Johnson, H., Middup, C., & Shiu, S. (2013). Economic methods and decision making by security professionals. In *Economics of Information Security and Privacy III* (pp. 213-238). Springer, New York, NY

- Bennett, S., Myatt, M., Jolley, D., & Radalowicz, A. (2001). *Data Management for Surveys and Trials. A Practical Primer Using EpiData*. The EpiData Documentation Project. Available: www.epidata.dk/downloads/dmepidata.pdf.
- Beresford, B., & Sloper, P. (2008). *Understanding the dynamics of decision-making and choice: A scoping study of key psychological theories to inform the design and analysis of the Panel Study*. York: Social Policy Research Unit, University of York.
- Bocchino W. A., (1975), Systemy informacyjne zarządzania. Narzędzia i metody., WNT, Warszawa
- Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.
- Cheng, F. C., & Lai, W. H. (2012). The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy. *Procedia Engineering*, 29, 241-251.
- Chintawar, S., & Ismail. (2014). A brief survey on privacy preserving data Anonymization Techniques on Cloud. *International Journal of Computer Engineering and Applications*, Volume VIII, Issue II, Part I, November 14.
- Choi, C., Choi, J., & Kim, P. (2014). Ontology-based access control model for security policy reasoning in cloud computing. *The Journal of Supercomputing*, 67(3), 711-722.
- Commissioner, D. P. (2004). *Data Protection Acts 1988 and 2003: A Guide For Data Controllers*. Dublin: Office of the Data Protection Commissioner.
- Computing, S. C. (2013). Building Trust and Compliance in the Cloud with Intel® Trusted Execution Technology. media13.connectedsocialmedia.com.
- Corti, L., Van der Eynden, V., Bishop, L., & Morgan-Brett, B. (2011). Managing and sharing data: training resources. UK Data Archive.
- Coyne, L., Dain, J., Forestier, E., Guitani, P., Haas, R., Maestas, C. D., ... & Vollmar, C. (2018). *Ibm private, public, and hybrid cloud storage solutions*. IBM Redbooks.
- Dai Yuefa, W. B., Yaqiang, G., Quan, Z., & Chaojing, T. (2009). Data security model for cloud computing. In *Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009)* (pp. 141-144).
- Daniel, W. (2014a). Challenges on privacy and reliability in cloud computing security. *Information Science, Electronics and Electrical*.

- Daniel, W. (2014b). Challenges on Privacy and Reliability in Cloud Computing Security. In *Information Science, Electronics and Electrical Engineering (ISEEE)*, 2014 International Conference on (Vol. 2, pp. 1181-1187). IEEE.
- Ferrari, E., & Thuraisingham, B. (2004). Security and privacy for web databases and services. In *International Conference on Extending Database Technology* (pp. 17-28). Springer, Berlin, Heidelberg.
- Futral, W., & Greene, J. (2013). *Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters*. Apress.
- Gholami, A. (2016). *Security and privacy of sensitive data in cloud computing* (Doctoral dissertation, KTH Royal Institute of Technology).
- Gholami, A., & Laure, E. (2016). Security and privacy of sensitive data in cloud computing: a survey of recent developments. *arXiv preprint arXiv:1601.01498*.
- Gordon, K. (2013). *Principles of Data Management: Facilitating Information Sharing* Second Edition. BCS.
- Gorondutse, A. H., & Hilman, H. (2012). The influence of Business Social Responsibility (BSR) on Organizational Performances: A pilot Study. *International Journal of Business and Management Tomorrow*, 2(12), 1-6.
- Gostin, L. (1997). Health care information and the protection of personal privacy: ethical and legal considerations. *Annals of Internal Medicine*, 127(8_Part_2), 683-690.
- Gunasekhar, T., Rao, K. T., Reddy, V. K., Kiran, P. S., & Rao, B. T. (2015). Mitigation of Insider Attacks through Multi-Cloud. *International Journal of Electrical and Computer Engineering*, 5(1), 136.
- Gupta, A., & Chourey, V. (2014). Cloud computing: Security threats & control strategy using tri-mechanism. In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2014 International Conference on (pp. 309-316). IEEE.
- Gupta, S. K., Rawat, S., & Kumar, P. (2014). A novel based security architecture of cloud computing. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*, 2014 3rd International Conference on (pp. 1-6). IEEE.
- Hair, J., Anderson, R., Babin, B., & Black, W. (2010). *Multivariate data analysis: A global perspective*.
- HUBER MW, PIERCY CA and MCKEOWN PG (2007) *Information Systems: Creating Business Value*, John Wiley & Sons, Hoboken, NJ.

- Hyseni, D., Luma, A., Selimi, B., & Cico, B. (2018). The Proposed Model to Increase Security of Sensitive Data in Cloud Computing. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, 9(2), 203-210.
- JESSUP L and VALACICH J (2008) *Information Systems Today: Managing in the Digital World*, 3rd ed., Pearson Prentice Hall, Upper Saddle River, NJ.
- Jogdand, R. M., Goudar, R. H., Sayed, G. B., & Dhamanekar, P. B. (2015). Enabling public verifiability and availability for secure data storage in cloud computing. *Evolving Systems*, 6(1), 55-65.
- Kaisler, S., Money, W. H., & Cohen, S. J. (2012). A decision framework for cloud computing. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 1553-1562). IEEE.
- Kayarkar, H. (2012). Classification of various security techniques in databases and their comparative analysis. *arXiv preprint arXiv:1206.4124*.
- Kelbert, F. (2013). Data usage control for the cloud. In *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on* (pp. 156-159). IEEE.
- Khosrowshahi, F., & Howes, R. (2005). A framework for strategic decision-making based on a hybrid decision support tools. *Journal of Information Technology in Construction*, 10, 111-124.
- Klein, D. A. (2013). Data security for digital data storage. *U.S. Patent No. 14,022,095*. Washington, DC: U.S. Patent and Trademark Office.
- Krautheim, F. J. (2010). Building Trust into Utility Cloud Computing. Ph.D. Dissertation, Faculty of the Graduate School of the University of Maryland, Baltimore County (2010).
- Krishna, B. H., Kiran, S., Murali, G., & Reddy, R. P. K. (2016). Security issues in service model of cloud computing environment. *Elsevier*, 246–251.
- KROENKE DM (2008) *Experiencing MIS*, Pearson Prentice Hall, Upper Saddle River, NJ.
- Kuacharoen, P. (2011). Design and analysis of methods for signing electronic documents using mobile phones. In *Int. Conf. on Comput. Applicat. and Network Security* (pp. 154-158).
- Kulkarni, G., Waghmare, R., Palwe, R., Waykule, V., Bankar, H., & Koli, K. (2012). Cloud storage architecture. In *Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on* (pp. 76-81). IEEE.

- Kumar, S. N., & Vajpayee, A. (2016). A Survey on Secure Cloud: Security and Privacy in Cloud Computing. *American Journal of Systems and Software*, 4(1), 14-26.
- Kuraś, M. (1994). Zmiana organizacyjna jako cel modernizacji systemu informacyjnego. In *Materiały IV Konferencji Rozwoju Systemów Informatycznych i ich Bazy Sprzętowej w Hutnictwie, Krynica, październik* (pp. 93-113).
- Laudon, K. C., & Laudon, J. P. (2007) *Management Information Systems: Managing the Digital Firm*, 10th ed., Pearson Prentice-Hall, Upper Saddle River, NJ.
- Laudon, K. C., & Laudon, J. P. (2016). *Management information system*. Pearson Education India.
- Laudon, K. C., & Laudon, J. P. (2018). *Management information systems: managing the digital firm*. Pearson.
- Leng, C., Yu, H., Wang, J., & Huang, J. (2013). Securing personal health records in the cloud by enforcing sticky policies. *Indonesian Journal of Electrical Engineering and Computer Science*, 11(4), 2200-2208. TELKOMNIKA.
- Li, W., Ping, L., & Pan, X. (2010). Use trust management module to achieve effective security mechanisms in cloud environment. In *Electronics and Information Engineering (ICEIE), 2010 International Conference On* (Vol. 1, pp. V1-14). IEEE.
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*.
- Liu, W. (2012). Research on cloud computing security problem and strategy. In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* (pp. 1216-1219). IEEE.
- Liu, W., Peng, S., Du, W., Wang, W., & Zeng, G. S. (2014). Security-aware intermediate data placement strategy in scientific cloud workflows. *Knowledge and information systems*, 41(2), 423-447.
- Loganayagi, B., & Sujatha, S. (2012). Enhanced cloud security by combining virtualization and policy monitoring techniques. *Procedia Engineering*, 30, 654-661.
- Mantra, EDINA, & Data Library, University of Edinburgh. (2014). Research Data MANTRA (online course). Retrieved April 20, 2015, from <http://datalib.edina.ac.uk/mantra#sthash.c9HnlX89.dpuf>

- March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: an introduction to the special issue on design science research. *MIS quarterly*, 725-730.
- Margaret Rouse. (2014). Sensitive Information. WhatIs.com.
- Mariusz Grabowski, Piotr Soja, Ryszard Tadeusiewicz, Jan Trąbka, Agnieszka Zajac. *Management Information Systems*. book January 2014, Publisher: Cracow University of Economics, ISBN: 978-83-64509-09-4
- Martucci, L. A., Zuccato, A., Smeets, B., Habib, S. M., Johansson, T., & Shahmehri, N. (2012). Privacy, security and trust in cloud computing: The perspective of the telecommunication industry. In *Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on* (pp. 627-632). IEEE.
- McLeod, R., & Schell, G. P. (2007). *Management information systems*. USA: Pearson/Prentice Hall.
- McLeod, R., & Schell, G. P. (2007) *Management Information Systems*, 10th ed., Pearson Prentice-Hall, Upper Saddle River, NJ.
- Mishra, S., Tripathy, A. K., & Joshi, P. (2016). Making a Cloud Data Secure and Effective for Better Performance of Services. *Indonesian Journal of Electrical Engineering and Computer Science*, 2(3), 695-702.
- Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012). Enhanced data security model for cloud computing. In *Informatics and Systems (INFOS), 2012 8th International Conference on* (pp. CC-12). IEEE.
- Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2013). Data security model for cloud computing. *Journal of Communication and Computer*, 10(08), 1047-1062.
- Moura, J., & Serrão, C. (2015). Security and privacy issues of big data. In *Handbook of research on trends and future directions in big data and web intelligence* (pp. 20-52). IGI Global.
- O'Brien, J. A., & Marakas, G. M. (2006). *Management information systems* (Vol. 6). McGraw-Hill Irwin.
- Ohm, P. (2014). Sensitive information. *S. Cal. L. Rev.*, 88, 1125.
- Palmius, J. (2005). Defining the information part of information system: a base for simulation.
- Pandey, A., Tugnayat, R. M., & Tiwari, A. K. (2013). Data Security Framework for Cloud Computing Networks. *International Journal of Computer Engineering & Technology (IJCET)*, 4(1), 178-181.

- Paul, R. J. (2010). What an information system is, and why is it important to know this. *Journal of computing and information technology*, 18(2), 95-99.
- Pearson, S., & Charlesworth, A. (2009). Accountability as a way forward for privacy protection in the cloud. In *IEEE International Conference on Cloud Computing* (pp. 131-144). Springer, Berlin, Heidelberg.
- Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing* (pp. 3-42). Springer, London.
- Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges. In *MIPRO, 2010 proceedings of the 33rd international convention* (pp. 344-349). IEEE.
- Qiong, S., Liu, M., & Pang, S. (2013). Cloud Computing Application of Personal Information's Security in Network Sales-channels. *Indonesian Journal of Electrical Engineering and Computer Science*, 11(12), 7331-7338. TELKOMNIKA.
- RAINER RK, TURBAN E and POTTER RE (2007) *Introduction to Information Systems*, John Wiley & Sons
- Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. P. (2010). The cloud: understanding the security, privacy and trust challenges.
- Salim, A., Tiwari, R. K., & Tripathi, S. (2011). Security Techniques for protecting data in Cloud Computing. *International Journal of Computer Engineering and Applications*, Volume XI, Issue IX, September.
- Saranya, M., & Senthamil Selvi, R. (2015). Data Anonymization Approach for Privacy preserving in cloud. *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol. 6 No. 04 (pp. 193-197). ISSN:2229-3345.
- Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 280-288). IEEE.
- Sastry, K. N., Rao, B. T., & Gunasekhar, T. (2015). Novel Approach for Control Data Theft Attack in Cloud Computing. *International Journal of Electrical and Computer Engineering*, 5(6).
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*. Elsevier, 79, 88–115.

- Soja, P. (2008). Examining the conditions of ERP implementations: lessons learnt from adopters. *Business Process Management Journal*, 14(1), 105-123.
- Strasser, C., Cook, R., Michener, W., & Budden, A. (2012). Primer on data management: what you always wanted to know
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), 1-11.
- Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, 10(7), 190903.
- Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 557-570.
- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, (6), 24-31.
- Tari, Z., Yi, X., Premarathne, U. S., Bertok, P., & Khalil, I. (2015). Security and privacy in cloud computing: Vision, trends, and challenges. *Ieeexplore.ieee.org*, 2 (2), 30–38.
- Tebaa, M., & Hajji, S. E. (2014). From single to multi-clouds computing privacy and fault tolerance. *IERI procedia*, 10, 112-118.
- TECHWEB (2008) “information system” in *TechEncyclopedia*, viewed on Feb. 1, 2008.
<http://www.techweb.com/encyclopedia/defineterm.jhtml?term=information+system>
- The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK), 1st Edition 2009, p.4
- Turpin, S. M., & Marais, M. A. (2004). Decision-making: Theory and practice. *orion*, 20(2), 143-160.
- Vogt, W. P. (2006). Quantitative research methods for professionals in education and other fields. *Columbus, OH: Allyn & Bacon*.
- Wainfan, L. (2010). *Multi-perspective strategic decision making: Principles, methods, and tools*. The Pardee RAND Graduate School.
- Walpole, R. E., Myers, R. H., Myers, S. L., & Ye, K. (1993). *Probability and statistics for engineers and scientists* (Vol. 5). New York: Macmillan.

- Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on computers*, 62(2), 362-375.
- Wang, Z. (2011). Security and privacy issues within the Cloud Computing. In *Computational and Information Sciences (ICCIS), 2011 International Conference on* (pp. 175-178). IEEE.
- Warasart, M., & Kuacharoen, P. (2012). based document authentication using digital signature and QR code. In *4TH International Conference on Computer Engineering and Technology (ICCET 2012)*.
- Watson RT, ed., (2008) *Information Systems*. Release 6, Global Text Project, viewed on Sept. 1, 2008 at <http://homepage.mac.com/rickwatson/filechute/IS%20bookE1R6.pdf>
- Wikman, A. (2006). Reliability, validity and true values in surveys. *Social Indicators Research*, 78(1), 85.
- Woulds, J. (2001). *A Practical Guide to the Data Protection Act*. Constitution Unit, University College London. First Published December 2004
- Wu, F., Chen, C. H., & Clarke, D. (2014). Sensitive Data Protection on Mobile Devices. *Editorial Preface*, 5(9).
- Xiaoping, X., & Junhu, Y. (2012). Research on cloud computing security platform. In *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*(pp. 799-802). IEEE.
- Xu, L., Cao, X., Zhang, Y., & Wu, W. (2013). Software Service Signature (S 3) for authentication in cloud computing. *Cluster computing*, 16(4), 905-914.
- Yang, K., & Jia, X. (2013). An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. *IEEE Trans. Parallel Distrib. Syst.*, 24(9), 1717-1726.
- Youseff, L., Butrico, M., & Da Silva, D. (2008). Toward a unified ontology of cloud computing. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). IEEE.
- Zarató, P. (2010). Cooperative decision support systems. In *Strategic Information Systems: Concepts, Methodologies, Tools, and Applications* (pp. 1551-1558). IGI Global
- Zarató, P., Konate, J., & Camilleri, G. (2013). Collaborative Decision Making Tools: A Comparative Study Based on Functionalities. In *13th International Conference Group Decision and Negotiation (GDN 2013)* (pp. pp-111).

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, 1(1), 7-18.

Zhao, F., Li, C., & Liu, C. F. (2014). A cloud computing security solution based on fully homomorphic encryption. In *Advanced Communication Technology (ICACT), 2014 16th International Conference on* (pp. 485-488). IEEE.

Zhou, M. (2013). Data security and integrity in cloud computing. *University of Wollongong Thesis Collection*.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.

