Privacy in Cloud Computing: An Intelligent Approach

By

Rusul Mumtaz Taher

Supervisor

Dr.Aysh Al-Hroob

Co-Supervisor

Dr. Venus Samawi

This thesis was submitted in partial fulfillment of the requirements for the Master's Degree in Software Engineering
Faculty of Graduate Studies
ISRA University
May 2019

Authorization statement

Rusul Mumtaz Taher, authorizes Isra University to provide hard or soft copies of her thesis to libraries, institutions or individuals upon their request.

Name: Rusul Mumtaz Taher

Signature:

Date:

اقرار تفويض

أنا رسل ممتاز طاهر أفوض جامعة الاسراء للدراسات العليا بتزويد نسخ من رسالتي ورقيا والكترونيا للمكتبات أو المنظمات أو الهيئات والموسسات المعنية بالأبحاث والدراسات العليا عند طلبها.

الاسم:- رسل ممتاز طاهر

التوقيع :

التاريخ

The undersigned have examined the thesis entitled Privacy in Cloud Computing: An Intelligent Approach presented by Rusul Mumtaz Taher, a candidate for the degree of Master in Software Engineering and hereby certify that it is worthy of acceptance.

_____	_____
Date	Supervisors name
_____	_____
Date	Co-supervisors name
_____	_____
Date	committee name 1
_____	_____
Date	committee name 2

الاهداء

وإلى من تتسابق الكلمات لتخرج معبرة عن مكنون ذاتها
من علمتني وعانت الصعاب لأصل إلى ما أنا فيه
وعندما تكسوني الهموم أسبح في بحر حنانها ليخفف من آلامي .. أمي

الى من احمل اسمه بكل فخر
إلى من علمني النجاح والصبر
إلى من افتقده في مواجهة الصعاب
ولم تمهله الدنيا لأرتوي من حنانه .. أبي

إلى من بهم أكبر وعليهم أعتمد .. إلى الشموع المتقدة الي تنير ظلمة حياتي
إلى من بوجودهم أكتسب قوة ..
إلى من عرفت معهم معنى الحياة.. اخواتي

إلى من أرى التفاؤل بعينه .. والسعادة في ضحكته
إلى الوجه المفعم بالبراءة..
بمحبتك أزهرت أيامي .. زوجي

الى من كان لي الاخ قبل المعلم ..
الى الذي لم يضنَّ عليَّ بأي معلومة علمية.. دعايش الحروب

الى من علمتني الصمود مهما تبدلت الظروف
الى من ازالت غيمة الجهل التي مرت بي .. د.فينوس سماوي

ACKNOWLEDGMENT

First and foremost, I would like to sincerely thank my supervisor, Dr. Aysh Alhroub and co. Supervisor Dr. Venus Samawi. I cannot express my appreciation and thanks enough, for their valuable guidance, advice and support during my master study at the Israa University. Moreover, they have not been only my teachers, but also my mentors and advisors in every aspect of my life. Working together with them has been the best experience that I will cherish forever.

I would also like to thank my uncles for their constant support and guidance. (Maher and

Amer) I would also specially thank my friend for her continual support (Ikhlas)

I am also grateful to my friends who lived with me and spent some good time with them in Jordan. (ghofran and fatima)

Last but not least, I would like to express my heartfelt thanks to my family for their unconditional love and endless support

Finally, I will never forget to thank the person who granted me the permanent love that resonated with me even after his death and I will always hold his name proudly (my father).

TABLE OF CONTENTS

DEDICATION IV

ACKNOWLEDGMENT V

LIST OF TABLES IX

LIST OF FIGURES X

LIST OF ABBREVIATIONS XI

CHAPTER ONE: Introduction 1

1.1 Overview: 1

1.2 Problem Statement and Motivations 2

1.3 Research Questions 3

1.4 Research Objectives 4

1.5 Thesis Layout 5

CHAPTER TWO: Theoretical Concepts and Literatures 7

2.1 Cloud Computing: Deployment Models 7

2.2 Cloud Environment: Security and Privacy Threats 8

2.2.1 Intrusion Detection Techniques 11

2.2.2 Sticky Policy 13

2.2.3 Blockchain 14

2.3 Literature Review and Related Works 15

2.3.1 Literatures: Privacy in Cloud Computing 15

2.3.2 Literatures: Third Party and Data Integrity 17

2.3.3 Intrusion Detection 20

2.4 The Proposed Model: Characteristics and Differentiation 23

CHAPTER THREE: Privacy & Data Integrity Service (PDIS): The proposed Approach 24

3.1 Privacy and Data Integrity Service Layer: proposed Design 24

3.1.1 Intrusion Detection Phase 25

3.1.2 Privacy and Data Integrity Phase 27

3.1.3 AES Encryption 27
3.1.4 Policy Rules Engine 29
3.1.5 Data Integrity 31
3.2 PDIS Structure 32
3.3 The Flow Control of PDIS 33
CHAPTER FOUR : PDIS: Implementation and Analysis of Findings 35
4.1. Case Study Description 35
4.2. Implementation Layers 36
4.2.1 Layer 1: Data Owner 36
4.2.2 Layer 2: Intrusion Detection ..... 36.
4.2.3 Layer 3 (Block-chain) 37
4.3. Rule Extraction 37
4.4. Implementation of PDIS 42
4.5. Implementation Interfaces 43
4.6. Sticky Policy Evaluation Flow 47
CHAPTER FIVE: Conclusion and Future work 49
5.1 Used Methods 49
5.2 Layer 1, Data Owner 49
5.3 Layer 2, intrusion detection 50
5.4 Layer 3, Block-chain 50
5.5 Future Work 58
References 52

LIST OF TABLES

Table 2.1: Data integrity and 3rd. parity literatures: summary 19
Table 2.2: ID literatures: Summary 22
Table 4.1: Accuracy results of various IDSs compared with the proposed approach 42

LIST OF FIGURES

Figure 1.1: Cloud computing: Main service models 2
Figure 2.1: Popular cloud environment threats 9
Figure 2.2: Hierarchy of network attacks classification 12
Figure 2.3: Latest statistics about CCS attacks (McAfee Labs report, 2018) 13
Figure 3.1: The proposed cloud computing main service models 25
Figure 3.2: NIDS general framework 26
Figure 3.3: AES Encryption process (adapted from [Mohan and Reddy, 2012]) 29
Figure 3.4: Sticky Policy Components in CCS (Adapted from [Li et, al., 2015]) 30
Figure 3.5: General PDIS workflow for data security and privacy in CCS 32
Figure 4.1: Main System layer 35
Figure 4.2: Weka Tool used for Preprocess steps 39
Figure 4.3: The decision tree (J48) using cross validation (10-folds) 39
Figure 4.4: Preprocess steps applied in R 40
Figure 4.5: Rule extracted using R 41
Figure 4.6: Login Form 43
Figure 4.7: Verification e-mail 44
Figure 4.8: Verification Code 44
Figure 4.9: student form interface 45
Figure 4.10: instructor's activity log 45
Figure 4.11: Unlocking files for authorized users 46
Figure 4.12 chain file upload for instructors 46
Figure 4.13: Audit window 47

LIST OF ABBREVIATIONS

	Abbreviation	Mean
1.	AES	Advanced Encryption Standard
2.	ANFIS	Adaptive Neural Fuzzy Inference System
3.	AP	Access Permission
4.	CCSs	Cloud Computing Services
5.	CCSs	Cloud Computing Services
6.	CFS	Correction-Based Feature Selection
7.	CPS	Cyber Physical System
8.	CPS	Cyber Physical System
9.	DBMS	database management systems
10.	DBSCAN	Density-based spatial clustering of applications with noise
11.	DES	Data Encryption System
12.	DMP	Decision Making Phase
13.	FCM	Fuzzy C Means
14.	HIDS	Host Based Intrusion Detection
15.	HVI	Hyper visor Introspection
16.	HVI	Hypervisor Introspection
17.	IaaS	Infrastructure-as-a-service
18.	IBE	Identify Based Encryption
19.	IPS	Intelligent Privacy Service
20.	KNN	k-Nearest Neighbors
21.	LGP	Linear genetic programming

22.	NIDS	Network Based Intrusion Detection
23.	PaaS	Platform-as-a-Service
24.	PDIS	Privacy & Data Integrity Service
25.	PKI	Public Key Infrastructure
26.	PM	Physical Machine
27.	PM	Physical Machine
28.	POCC	Privacy Of Out Sourcing In Cloud Computing
29.	RDA	Remote Data Auditing
30.	RSIC	Remote Data Integrity Auditing
31.	SaaS	Software-as-a-Service
32.	SLA	Self –Learning Algorithms
33.	SVM	Support Vector Machine
34.	UML	Unified Modeling Language
35.	VM	Virtual Machine
36.	VMI	Virtual Machine Infrastructure

ABSTRACT

Due to the abundance of data that needs large storage space in various fields, cloud computing has become a haven for many companies, institutions and many other companies. Despite all the benefit, cloud computing faces many challenges in many areas including security and privacy issues. Main problems concerning, how to maintain data stored in the cloud, and how to gain customer confidence. All these security issues and privacy issues encourage us to propose a developed approach that contributes to increase security and privacy in cloud environment.

In this work, the developed approach is proposed to solve three security and privacy issues. Malware and Network Intrusion Detection (NID), privacy and access control to prevent unauthorized users from accessing client's data without their permission, data integrity to prevent data updating and modification without data owner awareness. To solve NID problem, set of normal-access rules are generated based on CIC-IDS2017 dataset, at which data mining approach (decision tree J48) is used to improve the classification accuracy and reduce feature-set before generating set of rules that are used to detect normal-access records. The system accuracy reaches 99.8%, which outperforms (or comparable) to previous related researches.

To preserve privacy and access control, a set of policies stick to the data file by the owner utilizing sticky policy approach. Data are encrypted using Advanced Encryption Standard (AES) ciphering algorithm as a second level of data protecting to preserve privacy. Finally, a simple block-chain approach is used to preserve data integrity, at which set of trustees (chain list) are identified by the data owner along with more confident level of accessing polices. A data modification done by a trusty member (chain member) will be reported to all trusty group including the owner. This will preserve auditing data changing (by who, when, in addition to last data updates).

The developed approach is a privacy and data integrity service (PDIS) layer to be part of the cloud computing main service model. The proposed service layer is placed on top of the other service layers. PDIS is a private infrastructure deployment model, which is managed and maintained in organization. Final, a web based application is implemented to act as a case study to check flow-control of the proposed PDIS.