

الآية

قال تعالى :

"فَبَدَأَ بِأَوْعِيَّتِهِمْ قَبْلَ وِعَاءِ أَخِيهِ ثُمَّ اسْتَخْرَجَهَا مِنْ وِعَاءِ أَخِيهِ كَذَلِكَ كِدْنَا لِيُوسُفَ مَا كَانَ لِيَأْخُذَ أَخَاهُ فِي دِينِ الْمَلِكِ إِلَّا أَنْ يَشَاءَ اللَّهُ تَرْفَعُ دَرَجَاتٍ مَن نَّشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ"

صدق الله العظيم

سورة يوسف الآية (76)

DEDICATION

..... To My father, who taught me that the best kind of knowledge to have is that
which is learned for its own sake.

..... To My mother, who taught me that even the largest task can be
accomplished if it is done one step at a time.

.... To My beloved brother and sisters.

.... My friends who encourage and support me,

All the people in my life who touch my heart,

I dedicate this research.



AKNOWLEDGEMENTS

I would like to express my deep gratitude to Dr.Faisal Mohammed Abdalla Ali, my research supervisors, for their patient guidance, enthusiastic encouragement and useful critiques of this research work.

I would also like to extend my thanks to the IT department in National Telecommunications Corporation (NTC) for their help in offering me the resources in running the program.

I would like to take this opportunity to say warm thanks to all my beloved friends,who have been so supportive along the way of doing
my thesis.

I also would like to express my wholehearted thanks to my familyfor their generous supportthey provided me throughout my entire life and particularly through theprocess of pursuing the master degree.

Because of their unconditional love and prayers, I have the chance to
complete this thesis.



ABSTRACT

Now a days, cloud computing is one of the dominant methods used for providing computing infrastructure for Internet services, Cloud computing offers computing and software services on demand by connecting to computing resources and access to IT managed services with an ease. This flexibility of cloud based services comes with risk of security and privacy of user's data. Client privacy is a tentative issue as all clients do not have the same demands regarding privacy.

In this thesis, the proposed system provides the cloud data security for private cloud computing environment using the homomorphic encryption technique. This technique provides functionality to perform operations on encrypted data without using the private key and without decrypting that data. After decrypting the result of this operation, it is the same as if we carried out the calculation on the plain data. This major strength of homomorphic encryption allows the cloud service providers to perform operations on encrypted client data without compromising on the client data privacy.

المستخلص

إن مفهوم الحوسبة السحابية بات أحد أهم الموضوعات المطروحة للنقاش في الصناعة خلال الفترة الماضية. الحوسبة السحابية هي تكنولوجيا تعتمد على نقل المعالجة والإدارة ومساحة التخزين الخاصة بالحاسوب إلى جهاز خادم يتم الوصول إليه عن طريق الإنترنت، كبديل للمخدمات المحلية أو أجهزة الحاسوب الشخصية. وقد أصبحت الحوسبة السحابية حالياً أحد أساليب الحوسبة، التي يتم فيها تقديم الموارد الحاسوبية كخدمات، ويتاح للمستخدمين الوصول إليها عبر شبكة الإنترنت (السحابة) بطريقة سهلة وبمبسطة تجعل من هذه الآلية آلية مرنة . لكن من المعلوم ان المرونة والتأمين كفتاء ميزان يجب الموازنة بينهما فقد أوجدت هذه الآلية مخاطر قد تفكك بأمن وخصوصية بيانات المستخدم.

جاءت هذه الدراسة لتقدم نظام مقترح يوفر التأمين والخصوصية للبيانات ، بإستخدام تقنية التشفير التماثلي ، وهي تقنية تسمح بالقيام بعمليات على النص المشفر للحصول على نتيجة مشفرة تطابق عند فك تشفيرها نتيجة عمليات تمت على النص الأصلي. وهي ميزة تمكن مزودي خدمة الحوسبة السحابية من إجراء عمليات على بيانات العملاء دون إنتهاك لخصوصية هذه البيانات.

TABLE OF CONTENT

1.1 INTRODUCTION	1
1.2 RESEARCH PROBLEM:	1
1.3 PROJECT OBJECTIVES :	2
1.4 METHODOLOGY:	2
1.5 ORGANIZATION OF RESEARCH:	3
2.1 BACK GROUND	4
2.1.1 What Is Cloud Computing?	4
2.1.1.1 Definition Of Cloud Computing	4
2.1.1.2 Essential Characteristics of Cloud Computing :	4
2.1.1.3 Service Models Of Cloud Computing	5
2.1.1.3.1 Software as a Service (SaaS) :	6
2.1.1.3.2 Platform as a Service (PaaS):.....	6
2.1.1.3.1 Infrastructure as a Service (IaaS):	6
2.1.1.4 Deployment Models of Cloud Computing :	5
2.1.2 Cloud Actors :	8
2.1.3 Importance of Security in Cloud Computing:	9
2.1.4 Important Security Issues in the Cloud :	9
2.2. INTRODUCTION :	11
2.2.1 SECURITY ISSUES AND USE OF CRYPTOGRAPHY IN CLOUD COMPUTING:	11
2.2.2 DATA SECURITY IN CLOUD COMPUTING WITH ELLIPTIC CURVE CRYPTOGRAPHY:	12
2.2.3 PRIVACY AND CONFIDENTIALITY ISSUES IN CLOUD COMPUTING ARCHITECTURES:	14
3.1 METHODOLOGY:	15
3.2 PROPOSED SYSTEM DESIGN:	16
4 INTRODUCTION:	18
4.1 TOOLS AND ENVIROMENTS:	18

4.1.1 Ubuntu	18
4.1.2 OpenStack:	18
4.1.2.1 OpenStack services	18
4.1.2.2 Storage in OpenStack:	20
Ephemeral Storage.....	20
Persistent Storage	20
Object Storage.....	21
Block Storage.....	21
Shared File Systems Service	21
Object Store.....	24
4.1.2.3 Encryption and Key Management	24
4.1.3 J2EE (Java 2 Enterprise Edition)	25
4.1.3.1 Java Servlets:	25
4.1.3.2 JSP Technology	25
4.1.4 Eclipse IDE	26
4.2 TECHNIQUES	26
4.2.1 homomorphic encryption:	26
4.2.1 definition:	26
4.2.2 Introduction to Homomorphic Encryption	26
4.2.3 Homomorphic Encryption types:	27
4.2.3.1 Partially Homomorphic Encryption Systems.....	27
4.2.3.2 Additive Homomorphic Encryption Systems	27
4.2.3.3 Multiplicative Homomorphic Encryption Systems	27
4.2.3.4 Additive and Multiplicative Homomorphic Encryption Systems	28
4.2.3.4 Fully Homomorphic Encryption Systems.....	28
4.2.4 Homomorphic Encryption Applied to Cloud Computing Security:.....	28
4.2.5 Paillier cryptosystem.....	29
5.1 INTRODUCTION:	30
5.2 IMPLEMENTATION STEPS:.....	30
5.2.1 Cloud Server:	30
5.2.1.1 Login Interface:.....	31

5.2.1.2 Users Account:.....	31
5.2.1.3 Admin Panel Interface:.....	31
5.2.1.4 Containers Interface:	32
5.2.1.5 Client Objects Interface:	33
5.2.2 Web Based Application :.....	33
5.2.2.2 Home Page :.....	34
5.2.2.3 File Upload Mechanism.....	35
5.2.2.4 File Encryption Module:.....	35
5.2.2.5 Download Encrypted File:	35
5.2.2.6 Decryption Mechanism:	36
5.2.2.7 Homomorphic addition Mechanism:	37
5.3Discussions :.....	37
5.4 Results:.....	38
Sample of results:.....	38
6.1 INTRODUCTION.....	41
6.2 CONCLUSION	41
6.3 RECOMMENDATION	41
6.4 OBSTACLES:	41
REFERENCES:	42
APPENDIX	44
APPENDIX I:.....	44
Paillier’s Algorithm:	44
APPENDIX II:	49
Installing OpenStack Icehouse on Ubuntu 14.04 LTS:.....	49

LIST OF FIGURES

Figure 3.1:Basic Architecture for Preserving Data Privacy in the Cloud	15
Figure 3.2: Proposed System Flow Chart Diagram.....	17
Figure 5.1 Login Interface.	31
Figure 5.2 Users Accounts Interface.	32
Figure 5.3: Admin Interface.	32
Figure 5.4: Shows The Containers Interface.....	33
Figure 5.5: Shows The Objects Interface.....	33
Figure 5.6: Shows The Login Interface.	34
Figure 5.7: Shows The User Interface.	34
Figure 5.8:The Upload Interface.	35
Figure 5.9: The download interface.....	36
Figure 5.10: The Decryption Interface.	36
Figure 5.11: The Addition Interface.	37
Figure 5.12: The plain text file.....	38
Figure 5.13: The encrypted text file after downloaded.....	39
Figure 5.14: The encrypted modified text file after downloaded.....	39
Figure 5.15: The decrypted modified text file.....	40

LIST OF TABLES

Table 4.1 list of 1OpenStack services	19
Table 4.2 Comparison of differing types of storage in openStack	23