الآية

قال تعالي :

"فَبَدَأَ بِأَوْعِيَتِهِمْ قَبْلَ وِعَاءِ أَخِيهِ ثُمَّ اسْتَخْرَجَهَا مِن وِعَاءِ أَخِيهِ كَذَٰلِكَ كِدْنَالِيُوسُفَ مَاكَانَ لِيَأْخُذَأَخَاهُ فِي دِينِ الْمَلِكِ إِلَّا أَن يَشَاءَ اللَّهُ ۚنَرْفَع دَرَجَاتٍ مَّن نَّشَاءُوَفَوْق كُلِّ ذِي عِلْمٍ عَلِيمٌ "

صدق الله العظيم

سورة يوسف الاية (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 forproviding computing infrastructure for Internet services, Cloud computing offerscomputing and software services on demand by connecting to computing resources andaccess to IT managed services with an ease. This flexibility of cloud based servicescomes with risk of security and privacy of user's data. Client privacy is a tentative issueas 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 usingthe homomorphic encryption technique. This technique provides functionality to performoperations on encrypted data without using the private key and without decrypting thatdata. After decrypting the result of this operation, it is the same as if we carried out thecalculation on the plain data. This major strength of homomorphic encryption allows thecloud service providers to perform operations on encrypted client data withoutcompromising on the client data privacy.

المستخلص

إن مفهوم الحوسبة السحابية بات أحد أهم الموضوعات المطروحة للنقاش في الصناعة خلال الفترة الماضية.

الحوسبة السحابية هى تكنولوجيا تعتمد على نقل المعالجة والإدارة ومساحة التخزين الخاصة بالحاسوبإلى جهاز خادميتم 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 ومبسطة تجعل من هذه الآلية آلية مرنة . لكن من المعلوم ان المرونة والتأمين كفتاء ميزان يجب الموازنة بينهما فقد أوجدت هذه الآلية مخاطر قد تفتك بأمن وخصوصية بيانات المستخدم.

جاءت هذه الدراسة لتقدم نظام مقترح يوفر التأمين والخصوصية للبيانات ، بإستخدام تقنيةالتشفير 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

LIST OF FIGURES

LIST OF TABLES