

**UNIVERSITY OF SCIENCE AND TECHNOLOGY**  
**COLLEGE OF GRADUATE STUDIES AND**  
**ACADEMIC ADVANCEMENT**

**Secure Searching in Cloud**

A Thesis

Submitted to the College of Graduate studies and Academic  
Advancements in Partial Fulfillment of the Requirement for the  
Degree of Master of Science in Information Technology

**Prepared By:**

Ahmed AbdElmoneim Ahmed Mahmoud

**Supervisor By:**

Prof. Nouredien Abdelrahman

Dec2016

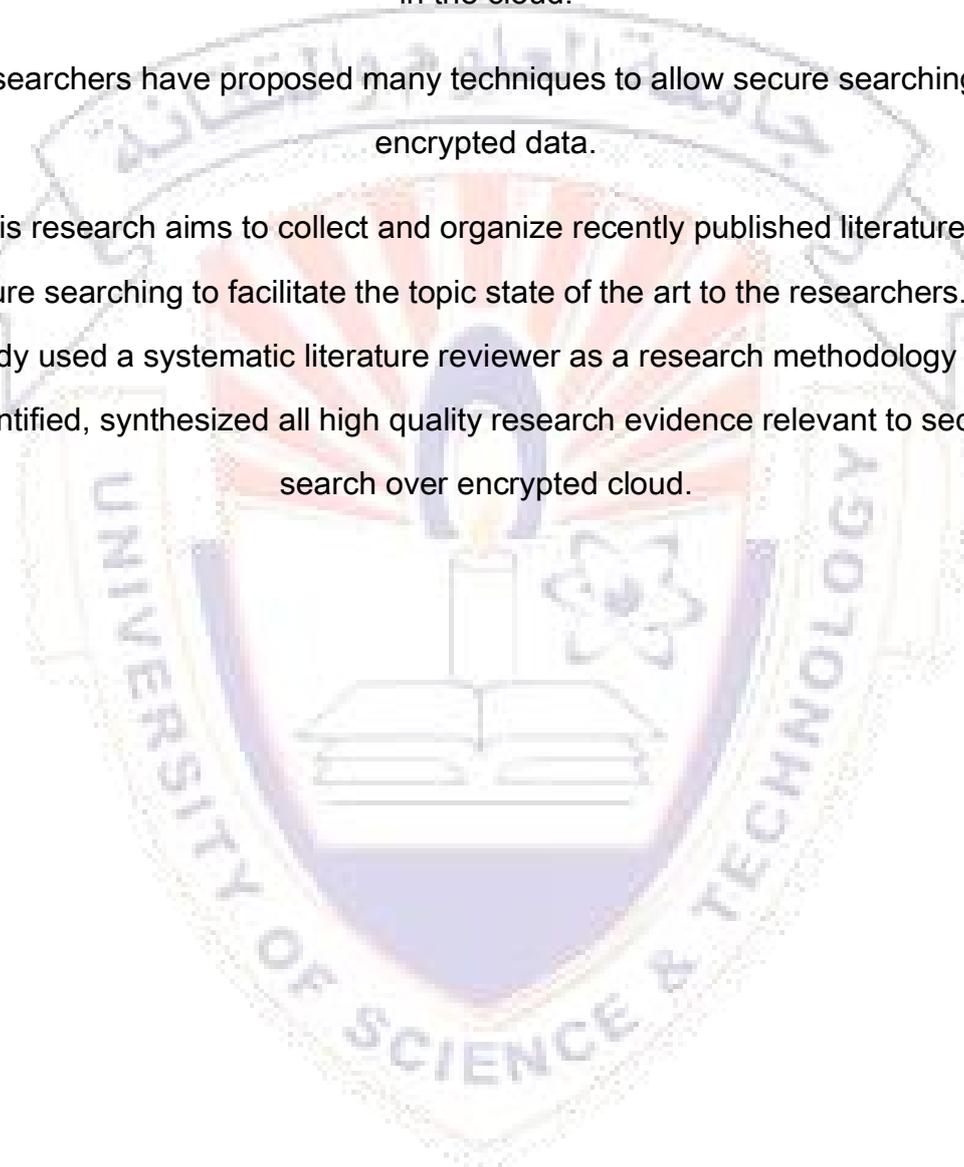
## Abstract

Nowadays, cloud computing became an interested field, many organizations and consumers transferred their business to the cloud.

One of the major cloud concerns is searching enterprise encrypted data store in the cloud.

Researchers have proposed many techniques to allow secure searching on encrypted data.

This research aims to collect and organize recently published literature on secure searching to facilitate the topic state of the art to the researchers. The study used a systematic literature reviewer as a research methodology and identified, synthesized all high quality research evidence relevant to secure search over encrypted cloud.



## المستخلص

أصبحت الحوسبة السحابية حقل لكثير من الباحثين والمؤسسات في الوقت الحاضر، وبناءً على ذلك فقد نقلت العديد من المؤسسات والمستهلكين أعمالهم إلى الحوسبة السحابية.

إن إحدى الإهتمامات الرئيسية لمستخدمي السحابة هي التمكن من البحث في بيانات الخاصة بهم والمخزنة في السحابة.

لأن البيانات يتم تخزينها في السحابة مشفرة، فإن الباحثون إقترحوا العديد من التقنيات لإتاحة البحث بشكل آمن على البيانات المشفرة.

يهدف هذا البحث إلى جمع وتنظيم الكتابات المنشورة مؤخراً عن البحث الآمن في البيانات المخزنة في السحابة، واستخدمت الدراسة مراجع علمية ذات صلة في منهجية البحث، والأوراق

المنشورة عن البحث الآمن في البيانات المشفرة والمخزنة في السحابة

## 1.1 Introduction

In the early years between 1960 and 1961 John McCarthy, an American computer scientist and cognitive scientist, came up with the idea of computer or information utility. In 1961 at MIT Centennial John McCarthy pointed out “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry”. Cloud Computing (CC) has developed from McCarthy’s idea of utility computing which begins the commoditization process to a new service that is widely available and has become undistinguishable from others like it, which consumers make the decision to purchase it based on price [1].

Cloud Computing technology has become a popular alternative to traditional computing technologies. This technology provides a new concept of a pay-per-use utility model of computing resources based mainly on virtualization technology. Numerous benefits result from these features, such as cost-effectiveness, time saving, scalability, and green information technology environment.

Despite these benefits, cloud computing faces many challenges and security issues that hinder the utilization of cloud computing.

Advances in technology and lower costs for storage have allowed organizations to capture and save more information on could have been imagined decades ago. Cyber-criminals have begun to see the value of this information and use it for various motives. Organizations have a fiduciary responsibility to protect information and its associated infrastructure components used to store and transmit it as key assets. “Risk assessments are the first step in determining how to safeguard enterprise assets [2].

The fact that the data owner has to encrypt his data before outsourcing it in the cloud, leads to many accessibility problems to users who are authorized to access the data. Secure searching over encrypted data, is an example of these problems.

## **1.2 Problem Statement**

Almost all enterprises today share their data among their internal users and customers. In their local networks, enterprises have full potential on searching their databases. Moving towards cloud computing, enterprises must be confident on capabilities of searching provided by Cloud Service Providers (CSP).

Thus searching in cloud data is very important to enterprises to join cloud services.

One of the most important challenging issues is how to search securely on the encrypted cloud data.

## **1.3 Research Objectives**

The objective of this research is to provide insight on the problem of secure searching in cloud data. Our aim is to identify and analyze the problem and to determine the science behind various methods that have been proposed for secure search. So the questions of this research are:

- 1- How users can make secure search in cloud computing environment?
- 2- What schemes have been proposed for secure searching?
- 3- How can we classify the proposed secure searching schemes?

## **1.4 Motivations**

How secure searching on cloud encrypted data? Is the question that motivates this research a challenging?

## **1.5 Research Methodology**

The information for this thesis was basically collected from the papers published in journals, conference and digital libraries. The survey of literature is used to answer questions 1 and 2 of the research questions. Chapter three gives details of the research methodology.

## **1.6 Research Scope**

This research thesis is concerned only with studying methods dedicated to secure search of encrypted cloud data.

## **1.7 Research Contribution**

Thesis contributions are:

- i. Identification of the secure searching cloud data algorithms.
- ii. Determining and organizing the proposed cloud data schemes.
- iii. Classification of proposed schemes.

## **1.8 Research Structure**

The remained of this thesis is organized as follows:

Chapter tow contains important aspects of cloud computing, including its definition, characteristics, models of cloud services, pros and cons of using cloud computing.

The chapter also briefly stated the challenges and security issues that faces cloud computing. Chapter three presents the research methodology being used to conduct about cryptographic schemes a simple background this research. Chapter four gives

