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

# Automatic Revocation Schemes in cloud computing

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:**

Manahil Awad Sherfi

Supervisor By:

Prof. Dr. Nour eldien Abd Al-Rahman

Nov 2016

## Abstract

Cloud computing is gaining widespread acceptance due to the various benefits it offers, such as cost-effectiveness, time savings and efficient utilization of computing resources. However, security issues are among the major challenges holding back the widespread adoption of this new technology.

The nature of this technology requires the Data Owner to move their data to the cloud. Data Owner has to encrypt her data to preserve data integrity and confidentiality, and she must control accessibility by distributing decryption keys to authorized users, when user was revoked Data Owner must re-encrypt her data and re-distribute the new keys to the rest of users. Above solution is not effective; Data Owner must be online to complete these tasks. And it consumes network resources, in addition to unreliability of communication.

Data Owner can delegate user revocation to Cloud Service Provider (CSP), this enables CSP to revoke users without any command after initial setup. By this solution the revocation Process becomes Automatic and it reduce many computations from Data Owner. This delegation has to implement securely and without revealing information.

In this research we study, survey and classify proposed Automatic Revocation schemes, we also evaluate these schemes and provide an expectation of future work.

## المستخلص

تلقى الحوسبة السحابية قبولا واسع النطاق بسبب المزايا المختلفة التي تقدمها، مثل الفعالية من حيث التكلفة، وتوفير الوقت والاستخدام الفعال للموارد الحوسبة. ومع ذلك، فالمسائل الأمنية هي من بين التحديات الكبرى التي تؤخر اعتماد هذه التكنولوجيا الجديدة.

طبيعة هذه التكنولوجيا تتطلب من مالكي البيانات نقل بياناتهم إلى مقدمي خدمة الحوسبة السحابية ولابد ان يقوم مالك البيانات بتشفير بياناته للحفاظ على سلامة البيانات وسريتها، كما يجب أن يتحكم في الوصول لهذه البيانات عن طريق توزيع مفاتيح فك التشفير للمستخدمين الشرعيين. عندما يتم نزع صلاحية الوصول من المستخدم، على مالك البيانات ان يقوم بإعادة تشفير البيانات وإعادة توزيع مفاتيح جديدة لبقية المستخدمين. وهو حل غير فعال. حيث يتطلب ذلك وجود مالك البيانات متصلا عبر الإنترنت لإتمام هذه المهام ، كما ان هذه الطريقة تستهلك موارد الشبكة، بالإضافة إلى عدم موثوقية الاتصال.

يستطيع مالك البيانات تفويض مسؤولية إلغاء صلاحيات المستخدم لمزود الخدمة السحابية(CSP) ، وهذا يتيح لمزود الخدمة نزع صلاحيات المستخدمين دون أي أمر بعد الإعداد الأولي. عن طريق هذا التفويض تصبح عملية الإلغاء تلقائية و تقلل كثيرا من الاعباء على مالك البيانات. يجب ان ينفذ هذا التفويض بشكل آمن ودون الكشف عن معلومات.

في هذا البحث تم عمل دراسة و تصنيف لطرق تطبيق النزع الالي( Automatic Revocation) ، و تم تقييم هذه الطرق و تقديم توقعات للتطورات المستقبلية.

## 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 some day 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., such as multitenancy management, user's data isolation, and data sharing management and control… etc.
The fact that the data owner has to encrypt her data before outsourcing it in the cloud, leads to many accessibility problems to users who are authorized to access the data. Searching encrypted data, managing user's privileges and revocation of users are examples of these problems.

## 1.2 Problem Statement

When a Data Owner shares data among multiple users, she has to be able to control the user's access to that data. Fine-grained access control allows for efficient, easy to manage user's privileges and access control. Many encryption schemes have been proposed to achieve effective fine grained access control and they have been implemented in specific manners to provide automatic access control. One of the main user's access control operations performed by Data Owners is the user revocation.

User revocation can be done by the Data Owner, but this cause a plenty of efficiency and security problems. A better handling to user revocation is to delegate the process to a third party such as a CSP, which is known as automatic revocation.
Automatic revocation is achieved when Cloud Service Provider prevent data from a user without any command from Data Owner. The complexity of this solution lies in how to automate user revocation and at the same time preserve user privacy and data security. Data Owner must delegate the task of revocation to CSP without information revealing, and the CSP should handle user revocation without obtaining any information.
Many automatic revocation schemes have been developed and we classify them into two categories: Time based schemes and Task based schemes.

## 1.3 Research Objectives and Research Questions

The objective of this research is to provide insight on the problem of revocation of users who are sharing the same data or database. Our aim is to identify and analyze the problem and to investigate the automation of user revocation through studying various methods that have been proposed for automatic revocation. So the questions of this research are:
RQs:
*1- How to automate the user revocation?*
*2- What schemes have been proposed for automatic revocation?*
*3- How can we classify the proposed schemes of automatic user revocation?*
*4- What are the future research directions in revocation?*

## 1.4 Motivations

Almost all enterprises today share their data among their internal users and customers. In their local networks, enterprises have full potential on user's access control. Moving towards cloud computing, enterprises must be confident on security and access control mechanism provided by Cloud Service Providers (CSP).
One of the most important issues in the user's access control operations is the user revocation. The basic idea to perform user revocation in cloud is to use re-encryption. In this method after the expiration of user's right of accessing to the shared data, Data

Owner has to re-encrypt data with different key so as to deny the access of the revoked user.

Cloud is essentially a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. As a distributed system, the cloud will experience failures common to such systems, such as server crashes and network outages. As a result, re-encryption commands sent by the data owner may not propagate to all of the servers in a timely fashion, thus creating security risks.

When Data Owner delegates the responsibility of revocation to Cloud Service Provider (CSP), and CSP apply the revocation process based on specific instructions – without any command from Data Owner- this is called Automatic Revocation. So how automatic revocation can be implemented with users privacy preserved is a challenging question.

## 1.5 Research methodology

The information for this thesis was basically collected from the research papers such as journals, conference papers and other papers. So a scientific literature review methodology is applied. Our literature review methodology contains seven steps: searching, obtaining, assessing, reading, critical evaluation, recording, and writing. This methodology is explained in details in chapter 3.

## 1.6 Research Delimitations

This thesis will not discuss any technical descriptions about Cloud Computing nor discuss mathematics behind encryption algorithms. It will mainly present the concept of user revocation, the main steps in encryption schemes that used to achieve fine-grained access control with specific focus on automatic revocation schemes.

## 1.7 Thesis Contribution

The contribution of this is:

- Clarifying the concept of automatic revocation
- Identifying the currently proposed automatic revocation schemes.

- Classifying the proposed automatic user revocation schemes.
- Suggestion of future research directions.

## 1.8 Thesis Structure

The remaining contents of the thesis are organized as following:

Chapter 2 contains important aspects of cloud computing, including its definition, essential 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 3 presents the research methodologies being used to conduct this research. Chapter 4 gives the technical background needed to understand the proposed user revocation schemes, such as Proxy Re-Encryption (PRE), Attribute Base Encryption (ABE), and Homomorphic Encryption (HE). Chapter 5 surveys and classifies the currently proposed Automatic Revocation schemes. Finally chapter 6 discusses the future direction of research in automatic revocation.