UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Authentication Techniques For Cloud Computing Security

A Thesis

Submitted to the College of Graduate Studies and Academic Advancements

in PartialFulfillment of the Requirement for the Degree of Master of Science inInformation Technology

Prepared By:

Sana Gasim Ibrahim

Supervisor By:

Prof. NoureldienAbdelrhmanNoureldien

Jan 2017

Abstract

Cloud computing has emerged as a promising technique that greatly changes the modern Information technology industry, it depends on sharing resources that were never shared before, demanding a new set of security challenges. There are a variety of information security risks that need to be carefully considered, Risks will vary depending on the sensitivity of the data to be stored or processed. The authentication is one of the most important security issues in the cloud. It is very important for both the cloud provider and the user to have mutual trust such that the cloud provider can be assured that the user is not some malicious hacker and the user can be assured of data consistency, data storage and the instance he/she is running is not malicious.

Authentication is a key technology for information security, which is a mechanism to establish proof of identities to get access to information in the system. Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks.

In this research, we survey the proposed cloud authentication methods and provide an organized, systematic and classified literature that can aid researchers who are interested in this research field.

المستخلص

برزت الحوسبة السحابية في السنوات القليله الماضية بإعتبارها تقنية واعدة وقد ساهمت في تغيير صناعة تكنولوجيا المعلومات الحديثة بصورة واسعة، فهي تعتمد على تشارك الموارد التي لم يتم مشاركتها من قبل، مما فرض مجموعة جديدة من التحديات الأمنية .وهناك مجموعات متنوعة من المخاطر الأمنية المتعلقة بالمعلومات و التي تحتاج إلى النظر فيها بعناية، وتلك المخاطر تختلف تبعا لحساسية البيانات المراد تخزينها أو معالجتها. التحقق واحدة من اهم قضايا الأمن في السحابة , وهي من القضايا المهمة جدا لكلل من مزود السحابة والمستخدم ان تكون لديهم ثقة متبادلة بحيث مزود السحابة يجب أن يتأكد من المستخدم ليس بعض من القراصنة الخبيثة والمستخدم يجب أن يطمئن من أتساق البيانات ،تخزين البيانات ,التحقق هي التكنولوجيا الرئيسية لأمن المعلومات، وهي آلية لإقامة الدليل على الهويات للوصول للمعلومات في النظام .التحقق من خلال كلمة المرور التقليدية لا توفر الأمن الكافي على البيانات في بيئة الحوسبة السحابية ضد غالبية وسائل الهجمات الحديثة.

في هذا البحث تم تقديم دراسة مسحيه لطرق التوثيق في السحابه، وتم تقديمها بشكل منظم متسق ومصنف لتفيد الباحثيين المهتمين في هذا المجال.

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 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 indistinguishable from others like it, which consumers make the decision to purchase it based on price [1].

Cloud computing, a rapidly developing information technology, has aroused the concern of the whole world. Cloud computing is Internet-based computing, whereby shared resources, software, and information, are provided to computers and devices on-demand.

Cloud computing is a combination of various computing entities, globally separated, but electronically connected. As the geography of computation is moving towards corporate server rooms, it brings more issues including security, such as virtualization security, distributed computing, application security, identity management, access control, and authentication. Strong user authentication is the paramount requirement for cloud computing that restricts illegal access of cloud server**.**

1.2 Problem Statement

Users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and safely.

The information must be available to all users who are legitimate to use it at any time they want. So, users should be equipped with certain security means so that they can make sure that their data is safe.

As a solution to this problem, many researchers have tried to implement different types of authentication to make the cloud more secure. There are several ways to implement authentication. How these authentication services are provided to cloud users is a major concern for security community.

1.3 Research Objectives and Research Questions

The objective of this research is to provide insight on the problem of authentication of a user who stores and modifies his information in the cloud. Our target is to identify and analyze the problem and to survey the secure user authentication techniques in cloud computing environment, In order to provide a clear, consistent, organized literature review of cloud authentication techniques for the coming researchers.

The questions of this research are:

1. How to identify and authenticate users who store and modify their data in the cloud?
2. How can we protect the identity of the user from the cloud during authentication?
3. What are the schemes that have been proposed for user authentication?
4. How can we classify the proposed schemes for user authentication?

1.4 Motivation

With Cloud Computing, as with many new technologies and services, information security and data protection issues are intensely debated and examined far more critically than is the cases with offering that have been around for a while. Many surveys and studies reveal that potential customers have concerns about information security and data protection which stands in the way of a wider deployment.

User authentication is an essential security need. How researchers deal with this security issue in the cloud computing environment motivates this research.

1.5 Research Methodology

The information for this thesis was basically collected from the researcher's 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 Limitation

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 authentication, the main schemes of user authentication.

1.7 Thesis Structure

This thesis consists of fives chapters as follows: Chapter 2 explains and understand what cloud computing is, what components comprise a cloud solution, essential characteristics, cloud computing service model, deployment models, advantages and disadvantage of cloud computing, and takes a closer look at the security concerns and issues with cloud computing vulnerabilities and explaining the risk and top threats of cloud computing.

Chapter 3 shows research methodologies that have been used in this research. Chapter 4 surveys and classifies the existing user authentication techniques which take different criteria to authenticate the users in cloud. Chapter 5 contains the conclusion and the future work that should be done in the cloud authentication discipline.