Ain Shams University

Faculty of Computer and Information Sciences

Computer Science Department

Thesis Title

Identity-Based Management in the Cloud Computing

This thesis submitted to the Department of Computer Sciences, Faculty of Computer and Information Sciences, Ain Shams University, in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science

By

Hazem A. Elbaz

Researcher in Computer Science and Information Sciences

Under Supervision of

Prof. Dr. Taymoor M. Nazmy

Department of Computer Science

Faculty of Computer Science and Information Systems

Ain Shams University

Prof. Dr. Mohamed H. Abd-Elaziz

Department of Information Systems

Faculty of Computer Science and Information Systems

Ain Shams University

Cairo 2015

Abstract

The key management in cloud computing security became an incentive research area, where resource collaboration and coordination become so prevalent in cloud computing. Most researches focus on the authentication for two reasons; it is an essential security aspect and is the first line of defense in cloud computing environments. The main cloud computing authentication objectives are security and efficiency. This thesis examines the application of hierarchal identity-based authenticated key agreement in designing security key management for cloud computing.

The most common key management in the cloud computing solution goes to the Hierarchical Identity-Based Cryptography (HIBC), which focused on encryption and signature for access control cloud computing environment. Nevertheless, authentication methods did not have the same interest. Many of the authentication methods used with cloud computing environment are not efficient for large scale multiple domains. Moreover, it is only used for access control but did not support mutual authentication.

In this thesis, we propose a Hierarchal Identity-Based Authenticated Key Agreement protocol (HIB-AKA). Our proposed protocol exploits new interesting properties of Hierarchical Identity-Based Cryptography (HIBC) to replicate security services provided by the Cloud Security Infrastructure (CSI). The CSI is based on

Public Key Infrastructure (PKI) that supports standard X.509 certificates and proxy certificates. Since our proposed protocol is certificate-free and has small key sizes, it offers a more lightweight approach to key management than the CSI. Our protocol presents a new technique of using a one-pass delegation protocol that makes use of HIBC properties. This combination of lightweight key management and efficient delegation protocol experimentally proved to be better in scalability than the existing PKI-based approach to cloud security.

Acknowledgments

First of all, Thanks for **Allah** the most gracious, the most merciful, who gave me the ability to finish this work.

It is my pleasure to thank my supervisors for their leadership. Primarily, I am deeply indebted to my mentor, Prof. Taymoor M. Nazmi, for his advices and fuelling my motivation and enthusiasm during this research. I also would like to express my gratitude to Prof. Mohamed Hashim for his continuous encouragement, useful notes; he offered not only guidance and leadership, but also personal advice.

I would like to thank my beloved wife, without her picking up the slack when I was unavailable for the family, there would have been no way I could have accomplished this. My sons had to suffer because their dad could not be there since he was "working." I hope they see that it was all worth the effort. In addition, my Father, my small family for sacrifices and patience.

Finally, I would like to thank my close friends, who provided me the balance that I needed to achieve this task, they gave me the strength to overcome the challenges that seemed insurmountable, and pointed me to a positive in that it is always possible to restart whenever things look dark. To them I dedicate this work and effort.

Contents

List of Figures

List of Tables

List of Publications

The following papers have been published:

1. Elbaz, Hazem A., Mohammed H. Abd-elaziz, and Taymoor Nazmy. "Trusting Identity Based Authentication on Hybrid Cloud Computing." *Cloud Computing*. Springer International Publishing, 2014. 179-188.

2. Elbaz, Hazem A., Mohammed H. Abd-elaziz, and Taymoor Nazmy. "A Secure Electronic Student Record using Hierarchal Identity-based Authentication over University Cloud Storage." *International Journal of Emerging Trends in Engineering and Development* Issue 4, Vol.6 (Oct. -Nov. 2014)

3. Elbaz, Hazem A., Mohammed H. Abd-elaziz, and Taymoor Nazmy. "Analysis and Verification of a Key Agreement Protocol over Cloud Computing Using Scyther Tool." *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* 3.6 (2015).

4. Elbaz, Hazem A., Mohammed H. Abd-elaziz, and Taymoor Nazmy. "Provably secure and efficient hierarchal identity-based authenticated key agreement." *International Journal of Distributed and Cloud Computing (IJDCC)* under processing.

List of Abbreviations

Abbreviation	Description
AKA	Authentication Key Agreement
API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
BDHP	Bilinear Diffie Hellman Problem
CDHP	Computational Diffie Hellman Problem
CRM	Customer Relationship Management
CIS	Cloud Security Infrastructure
CSP	Cloud Service Provider
DDHP	Decisional Diffie Hellman Problem
DDoS	Distributed Denial of Service
DLP	Discrete Logarithm Problem
DN	Distinguished Name
DoS	Denial of Service
EC2	Elastic Compute Cloud
ENIAC	Electronic Numerical Integrator And Computer
ERP	Enterprise Resource Planning
ESR	Electronic Student Record
FR attack	Frey-R¨uck attacks
GDH	Gap Diffie Hellman

GMP Library	A free library for arbitrary-precision arithmetic, operating on signed integers, rational numbers, and floating point numbers.
GNFS	General Number Field Sieve
HIB-AKA	Hierarchal Identity Based Authenticated Key Agreement
HIBC	Hierarchal Identity Based Cryptography
HIBE	Hierarchal Identity Based Encryption
IaaS	Infrastructure as a Service
IACAC	Identity Authentication and Capability based Access Control
IBAKE	Identity Based Authentication Key Exchange
IBC	Identity Based Cryptography
IBE	Identity Based Encryption
IBS	Identity Based Signature
IdP	Identity Provider
IoT	Internet of Things
KGC	Key Generator Center
LAN	Local Area Networks
MD5	Message Digest Algorithm 5
MOV attack	Menezes, Okamoto, Vanstone Attack
NIST	National Institute of Standards and Technology
OAuth	Open Authentication
OTP	One Time Password
PaaS	Platform as a Service
PKI	Public Key Infrastructure
PBC	Pairing Based Cryptography
PKG	Private Key Generator

QoS	Quality of Services
S3	Simple Storage Service
SaaS	Software as Services
SAML	Security Assertion Markup Language
SAN	Storage Area Networks
SPDL	Security Protocol Description Language
SSO	Single Sign On
URL	Uniform Resource Identifier
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Networks
XML	eXtensible Markup Language

Chapter 1

Introduction

1.1 Overview

Cloud computing is a computing model; in this model, resources (i.e servers, networks, applications and other elements) are retrieved from the internet through web-based tools and applications rather than a direct connection to a server. The cloud model differs from traditional outsourcers in that customers do not hand over their own IT resources to be managed. However, the cloud computing structure allows access to information as long as an electronic device has access to the web.

Therefore, IT resources are plugged into the "cloud" for infrastructure services, platform (operating system) services, or software services (such as SaaS apps), treating the "cloud" much as they would an internal data center or computer providing the same functions.

While cloud environments offer flexibility, scalability, there have been commensurate concerns about security. As more data moves from centrally located server storage to the cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at

risk if appropriate measures are not put in place prior to selecting a cloud provider or implementing your own cloud and migrating to cloud services.

With such a broad scope, how can cloud environments sufficiently evaluate all relevant risks to ensure that their cloud operations are secure? While traditional security challenges such as loss of data, physical damage to infrastructure and compliance risk are well known, the appearance of such threats in a cloud environment can be remarkably different.

One of the first steps towards securing cloud environment is to review and update existing IT policies to clearly define guidelines to which all cloud-based operations must observe. Such policies implement formal controls and processes with the specific aim of protecting data and systems in addition to fulfilling regulatory compliance obligations.

Cloud security policies should be applied to both internal and third party managed cloud environments. Whether building private or utilizing public cloud infrastructure within the organization, the responsibility for cloud security is shared between your organization and any cloud service providers you engage with. When showing carefulness on cloud service providers carefully review their published security policies and ensure that it aligns with your own corporate policies.

A fundamental security concept employed in many cloud installations is known as the defense-in-depth strategy. This involves using layers of security technologies to protect data and infrastructure against threats in multiple ways. In the event of a security failure at one level, this approach provides a certain level of redundancy and containment to create a robust security net. Security is more effective when layered at each level of the cloud stack.