AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER AND SYSTEMS ENGINEERING DEPARTMENT

A Security Framework for Cloud Computing Environments

A Thesis Submitted in Partial Fulfillment of the Requirements
of the Degree of Master of Science in Electrical Engineering
(Computer and Systems Engineering)

Submitted By

Mohammed Mahmoud Said Dawoud
B.Sc, in Electrical Engineering 2010
Computer and Systems Engineering Department
Faculty of Engineering, Ain Shams University

Supervised By

Dr. Gamal A. Ebrahim
Computer and Systems Engineering Department
Faculty of Engineering, Ain Shams University

Dr. Sameh A. Youssef
Computer and Systems Engineering Department
Faculty of Engineering, Ain Shams University

Cairo 2017

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER AND SYSTEMS ENGINEERING DEPARTMENT

Name: **Mohammed Mahmoud Said Dawoud**

Thesis Title: **A Security Framework for Cloud Computing Environments**

Degree: **Master in Electrical Engineering (Computer and Systems Engineering)**

EXAMINERS' COMMITTEE

Name, Title, and Affiliation **Signature**

1. **Prof. Dr. Elsayed E. Hemayed** ………….
   Professor at Computer Engineering Department
   Faculty of Engineering
   Cairo University

2. **Prof. Dr. Hoda Korashy Mohamed** ………….
   Emeritus Professor at Computer and Systems Engineering Department
   Faculty of Engineering
   Ain Shams University

3. **Dr. Gamal Abdel Shafy Ebrahim** ……………
   Associate Professor at Computer and Systems Engineering Department
   Faculty of Engineering,
   Ain Shams University

Date: 1 / 4 / 2017

STATEMENT

This thesis is submitted as a partial fulfillment of Master of Science degree in Electrical Engineering (Computer and Systems Engineering), Faculty of Engineering, Ain Shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or qualification at any other scientific entity.

Signature

Student Name
Mohammed Mahmoud Said Dawoud

Researcher Data

Name: **Mohammed Mahmoud Said Dawoud**

Date of birth: **18/10/1988**

Place of birth: **Cairo – Egypt**

Academic Degree: **Master of Science Degree**

Field of specialization: **Computer and Systems Engineering**

University issued the degree: **Ain Shams University**

Current job: **Computer Engineer**

Thesis Summary

Name: **Mohammed Mahmoud Said Dawoud**

Thesis: **A Security Framework for Cloud Computing Environments**

Degree: **Master of Science in Electrical Engineering (Computer and Systems Engineering)**

Cloud computing is a promising technology that provides dynamic allocation of computing resources from a resource pool. Also, it has useful characteristics such as power saving and low running cost. On the other hand, the security risks of cloud computing are a major concern that slows down its market growth. There are many frameworks for handling security risks of cloud computing, most of them trust cloud service provider and do not focus on the new types of security risks that might face the cloud. In this thesis, a new security framework for cloud computing is introduced that mainly tries to tackle these problems. The introduced framework does not trust the cloud service provider. Most current frameworks cannot detect the attacks that may come from cloud service provider side or due to vulnerabilities or attacks at the cloud service provider system. Mainly because they consider the cloud service provider as trusted entity. Hence, a framework is needed that can deal with these issues and transfer the trust away from the cloud service provider to another trustworthy party. The introduced framework in this thesis keeps the sensitive data encrypted and a trusted authority is the only one that is able to decrypt and process the sensitive data.

Keywords

Cloud Computing; Cloud Computing Security; Cloud Service Provider; Security Framework; Trusted Computing; Trusted Cloud; Cloud Security Framework; Cloud Trusted Authority; Secured Datacenter.

ACKNOWLEDGEMENT

I am most grateful to my supervisor Dr. Gamal A. Ebrahim who supported me and guided me while working on this master thesis, whose input has proven invaluable to accomplish this thesis. This thesis would not have been done without his help and support.

Also, I would like to thank my co-supervisor Dr. Sameh A. Youssef for his help and support to do this research.

Finally, I would like to thank everyone who helped me and encouraged me to continue this research especially my family and my friends.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AES	Advanced Encryption Standard
AWS	Amazon Web Services
BPMN	Business Process Modeling Notation
CIA	Confidentiality, Integrity, and Availability
CORS	Cross Origin Resource Sharing
CSP	Cloud Service Provider
CSRF	Cross Site Request Forgery
CSTA	Cloud Security Trusted Authority
DIV	Dynamic Integrity Validation
HTTPS	Hyper Text Transfer Secure
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
JWT	JSON Web Token
LAN	Local Area Network
NIST	National Institute of Standards and Technology
ORAM	Oblivious Random Access Memory
PaaS	Platform as a Service
ROI	Return On Investment
RSA	Rivest, Shamir, and Adelman
SaaS	Software as a Service
SDN	Software Defined Network
SICE	Strongly Isolated Computing Environment
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SSL	Secured Socket Layer
SSO	Single Sign On
TPM	Trusted Platform Module
TTP	Trusted Third Party
VM	Virtual Machine
VMM	Virtual Machine Monitor

CHAPTER 1

Introduction

Cloud computing can be considered as the future of information technology infrastructure. It represents a major paradigm shift in this direction. Additionally, it provides on-demand allocation of computing resources [1]. These computing resources are allocated and released dynamically. Dynamic allocation has many benefits such as fast resource allocation, efficient resource management, energy saving, and lower cost [1]. Moreover, cloud computing environment has several new features due to its nature such as multi-tenancy, virtualization, and outsourcing of computing resources. These new features allow sharing of computing resources among cloud users [2]. Hence, resource sharing in cloud computing should be handled in a secured way to keep the security and privacy of data away from being violated [3].

Conversely, cloud computing environment has some issues concerning data privacy and security. Consequently, one of the most important reasons that slows down the growth of cloud computing market is the data security risks at cloud computing environment [4]. Several security issues face cloud computing environments such as how to secure the data at the cloud, how keeping the data trusted at a data center that belongs to someone the user does not know, and what are the risks that the data might face in this new environment.

Some of the issues which face the cloud computing and slow down its market growth are being solved. One of these issues is the calculation of billing values and the consumption values of computing resources due to the fact that the allocation of computing resources is dynamic [5]. Additionally, the computing resources are allocated and released freely and dynamically based on the actual needs for these resources. Hence, the dynamic allocation complicates the calculation of the accurate consumption values for the computing resources.

Solutions and suggestions have been proposed to treat some of these issues and the research is still trying to develop and improve the proposed solutions. Security in cloud computing is one of the most sensitive challenges that face the cloud computing. Normally, businesses may not pay much attention for the financial cost as much as they do for the data security and privacy at the cloud. Concerning to this challenge, many studies and security frameworks have been introduced to solve such a challenge. However, gaps may be found at the current introduced security frameworks. Additionally, cloud user still has security concerns of the cloud computing security risks and gaps. New security frameworks are still being proposed to tackle the security issues in cloud computing.

On the other hand, current security frameworks are more focused on traditional security concerns such as physical and system security. New aspects of security such as human-factors security, asset management, and security policy management need more elaboration [6]. These new security aspects are not present in the traditional data centers' security aspects. However, they are present in the cloud computing environment.