

A  
Major Project Report II  
On

**A Novel Cryptography Based Security In Cloud Computing**

Submitted in Partial Fulfillment of the Requirement  
For the Award of the Degree of

**Master of Technology**

*In*

**Software Engineering**

*By*

**Raju Kumar**  
University Roll No. 2K13/SWE/14

*Under the Esteemed Guidance of*

**Dr. S. K. Saxena**  
Computer Science & Engineering Department, DTU



**2013-2015**

**COMPUTER SCIENCE & ENGINEERING DEPARTMENT**

**DELHI TECHNOLOGICAL UNIVERSITY**

**DELHI - 110042, INDIA**

## **DECLARATION**

I hereby declare that the Major Project-II work entitled “**A Novel Cryptography Based Security In Cloud Computing**” which is being submitted to the Delhi Technological University, in partial fulfillment of requirements for the award of degree of Master of Technology (SWE) in the Department of Computer Science & Engineering, is a bonafidereport of the Major Project-II carried out by me. The material contained in this report has not been submitted to any University or Institution for the award of any degree.

**Raju Kumar**  
Roll no:- 2K13/SWE/14  
M.Tech.(Software Engineering)  
Email:-yadvraju03@yahoo.com

# CERTIFICATE

This is certify that the Major Project-II Report entitled “**A Novel Cryptography Based Security In Cloud Computing**” is the work of Raju Kumar (Roll no. 2K13/SWE/14). This project was completed under my supervision and form a part of Master of Technology (Software Engineering) course curriculum in the Department of Computer Science & Engineering, Delhi Technological University, Delhi.

Date:

**( Dr. S. K. Saxena)**

Project Guide

Dept. of Computer Science & Engineering

Delhi Technological University

# ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor **Dr. S.K.Saxena** for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to **Dr. O.P.Verma**, HOD, Computer Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Date:

**Raju Kumar**

**University Roll no: 2K13/SWE/14**

**M.Tech (Software Engineering)**

**Department of Computer Science &  
Engineering**

**Delhi Technological University, Delhi – 110042**

## **ABSTRACT**

Cloud computing is in demand nowadays because of its reliability. It provide us better platform for sharing data, messages, hardware, software and so on without fear of losing data. The number of users in cloud environment and number of threats on their cloud data are also increasing. In cloud computing, most of the researchers focused mainly on three areas, namely security at client's side, security at network and security at server's side. In this research I have focused both on security aspect of outsourced data and minimization of the duplication data, which also impacts the security of cloud. I have proposed an effective cryptography based security model which is more effective and secure than existing models in terms of performance and reliability. I have used a novel cryptography technique at client side before transmitting the data for increasing the trust of data owner as well as providing the security. I have also used a hashing function for checking the duplication of data so as to minimize space and bandwidth needed to store and upload the duplicate file.

**Keywords:** Cloud Computing, Network Security, Hashing, Cryptography.

# **CONTENTS**

**Declaration**

**Certificate**

**Acknowledgment**

**Abstract**

**Contents**

**List of Figures**

**List of Tables**

## **Chapter 1**

### **INTRODUCTION**

1.1 An Overview	01
1.2 General Concept	02
1.3 Motivation	03
1.4 Related Work	03
1.5 Problem Statement	05
1.6 Scope of Work	05
1.7 Organization of Thesis	06

## **Chapter 2**

### **CLOUD COMPUTING OVERVIEW**

2.1 Cloud Definitions	07
2.2 History of Cloud	08
2.3 Cloud Models	09
2.3.1 Deployment Models	09
2.3.2 Service models	12

2.4 Advantage of Cloud Computing	14
2.5 Issue in Cloud	15

### **Chapter 3**

#### **CRYPTOGRAPHY & NETWORK SECURITY OVERVIEW**

3.1 Security Goals	19
3.1.1 Confidentiality	19
3.1.2 Integrity	19
3.1.3 Availability	19
3.2 Attacks	19
3.2.1 Inside Attack	19
3.2.1 Outside Attack	19
3.3 Attacks Threatening Confidentiality	20
3.3.1 Snooping	20
3.3.2 Traffic Analysis	20
3.4 Attacks Threatening Integrity	20
3.4.1 Modification	20
3.4.2 Masquerading	20
3.4.3 Replaying	20
3.4.4 Repudiation	21
3.5 Attacks Threatening Availability	21
3.6 Cryptography	21
3.6.1 Symmetric-Key Cryptography	21
3.6.2 Asymmetric-Key Cryptography	22
3.6.3 Hashing	22
3.7 Security on Cloud	22

### **Chapter 4**

#### **PROPOSED METHODOLOGY**

4.1 Block Status Table	35
4.2 Proposed Symmetric Key Algorithm	35
4.2.1 Encryption	35
4.2.2 Decryption	36
4.3 Proposed Cryptographic Hash Function Algorithm	36
4.4 Proposed framework	37
4.5 Proposed Model	38

## **Chapter 5**

### **IMPLEMENTATION AND RESULT ANALYSIS**

5.1 Tools Used	39
5.2 Snapshots	40
5.3 Objectives	41
5.4 Advantages of Proposed Algorithm	41

<b>CONCLUSION AND FUTURE ENHANCEMENT</b>	<b>43</b>
--	-----------

### **REFERENCES**



# LIST OF FIGURES

Figure 1: Cloud computing	07
Figure 2: Cloud computing architecture	08
Figure 3: Public Cloud	10
Figure 4: Private cloud	10
Figure 5: Hybrid cloud	11
Figure 6: Community Cloud	11
Figure 7: Efficiency & cost related to Cloud service models	14
Figure 8:Block Diagram or Data Encryption and Decryption in Cloud System	37
Figure 9: Client Side Encryption	40
Figure 10: TTPA Table1	40
Figure 11: Decryption	41

# List of Tables

Table 1: Deployment models comparison

12