

A Major Project Report On

**A STRONG TWO FACTOR MUTUAL AUTHENTICATION
SCHEME FOR CLOUD COMPUTING**

Submitted in partial fulfilment of the requirements
for the award of the degree of

**MASTER OF TECHNOLOGY
IN
SOFTWARE ENGINEERING**

By

Neha Sharma

(Roll No. 2K13/SWE/09)

Under the guidance of

Mr. Manoj Kumar

Associate Professor

Department of Computer Engineering
Delhi Technological University, Delhi



**Department of Computer Engineering
Delhi Technological University, Delhi**

2013-2015



DELHI TECHNOLOGICAL UNIVERSITY
CERTIFICATE

This is to certify that the project report entitled “**A STRONG TWO FACTOR MUTUAL AUTHENTICATION SCHEME FOR CLOUD COMPUTING**” is a bona fide record of work carried out by Neha Sharma (2K13/SWE/09) under my guidance and supervision, during the academic session 2013-2015 in partial fulfilment of the requirement for the degree of Master of Technology in Software Engineering from Delhi Technological University, Delhi.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Mr. Manoj Kumar

Associate Professor

Department of Computer Engineering

Delhi Technological University

Delhi



DELHI TECHNOLOGICAL UNIVERSITY

ACKNOWLEDGEMENTS

I feel immense pleasure to express my heartfelt gratitude to **Mr. Manoj Kumar** for his constant and consistent inspiring guidance and utmost co-operation at every stage which culminated in successful completion of my research work.

I also would like to thank the faculty of Computer Engineering Department, DTU for their kind advice and help from time to time.

I owe my profound gratitude to my family which has been a constant source of inspiration and support.

Neha Sharma

Roll No. 2K13/SWE/09

TABLE OF CONTENTS

Certificate	i
Acknowledgement	ii
Table of Contents	iii-v
List of Figures	vi
List of Tables	vii
Abstract	viii
Chapter 1: Introduction	1-3
1.1 Motivation	1
1.2 Problem Statement	2
1.3 Aim of Thesis	2
1.4 Organisation of Thesis	3
Chapter 2: Literature Review	4-8
Chapter 3: Research Background	9-17
3.1 Cloud Computing	9
3.2 Cloud Deployment Model	10
3.2.1 Public Cloud	10
3.2.2 Private Cloud	10
3.2.3 Hybrid Cloud	11
3.2.4 Community Cloud	11
3.3 Cloud Service Model	12
3.3.1 Software as a Service	12
3.3.2 Infrastructure as a Service	12
3.3.3 Platform as a Service	12
3.4 Characteristics of Cloud Computing	13

3.5 Cloud Computing Security.....	15
3.6 Authentication.....	16
3.6.1 Two Factor Authentication.....	16
Chapter 4: The Factors.....	18-19
4.1 Factors Used.....	18
4.1.1 Alphanumeric Password.....	18
4.1.2 Stego-Image.....	18
4.1.3 One Time Password (OTP).....	19
4.1.4 Digital Signature.....	19
Chapter 5: The Proposed Scheme.....	20-39
5.1 The Entities	20
5.2 The Scheme.....	20
5.2.1 Notations Used.....	20
5.2.2 The Assumptions.....	20
5.2.3 The Detailed scheme.....	21
5.2.3.1 Registration Phase.....	22
5.2.3.2 Log-In Phase.....	26
5.2.3.3 Change Credentials.....	32
5.2.3.3.1 Change Password.....	33
5.2.3.3.2 Change STEGO_IMG File.....	33
5.2.3.3.3 Change Email-id.....	34
5.2.3.3.4 Change Mobile Number.....	35
5.2.3.4 Forget/Lost Credentials Phase.....	35
5.2.3.4.1 Forgot Password.....	35
5.2.3.4.2 Lost STEGO_IMG File.....	36
5.2.3.4.3 Both credentials Lost.....	38
Chapter 6: Implementation and Results	40-65
6.1 The Graphical User Interface (GUI).....	40
6.1.1 Registration Phase.....	40
6.1.2 Log-in Phase.....	52

6.1.3 Change Credentials.....	63
6.1.4 Lost Credentials.....	64
Chapter 7: Security Analysis.....	66-70
Chapter 8: Conclusions and Future Work	71-72
References	73-75

LIST OF FIGURES

Figure 1: Overview of Cloud Computing	9
Figure 2: Cloud Deployment Models.....	11
Figure 3: Cloud Service Model.....	13
Figure 4: Cloud Key Characteristics.....	14
Figure 5: Categories of Authentication Factors.....	16
Figure 6: Basic Architecture of Proposed Model	22
Figure 7: Registration Phase.....	25
Figure 8: Log-In Phase (Mutual Authentication).....	30
Figure 9: Log-In Phase (Updating Database)	32
Figure 10: GUI of Proposed Scheme	40
Figure 11: UI for Registration.....	41
Figure 12: Example of Error Message Box	42
Figure 13: STEGO_IMG.....	47
Figure 14: Save Dialog Box for STEGO_IMG	48
Figure 15: Message Box on Successful Registration	52
Figure 16: UI for Log-In.....	52
Figure 17: Mobile Phone receiving OTP.....	60
Figure 18: OTP Input Box.....	61
Figure 19: Cloud Services Home Page	63
Figure 20: Message Box on Unsuccessful Log-In.....	63
Figure 21(1): Input Box for Re-entering Password to Change Mail-id.....	64
Figure 21(2): Input Box for Entering New Mail-id to Change Mail-id.....	64
Figure 22: Input Box to Enter Username.....	65
Figure 23: UI for Setting New Password.....	65

LIST OF TABLES

Table 1: Description of notations	21
---	----

ABSTRACT

Cloud computing is an emerging technology. Along with many benefits, it brings new challenges. Among many issues of cloud computing, security is one of them. Security issues in cloud computing evolves along with the technology and considered as most critical one.

Security issues, such as identity management, virtualization security, application security, access control and authentication, are considered as one of the major cause of hindrance in widespread adoption of cloud computing. Security mechanisms being followed are insufficient to ensure confidentiality, integrity, availability and non-repudiation etc. A strong mutual authentication scheme is the vital requirement of cloud computing. This research work proposes a strong two factor mutual authentication scheme. The proposed scheme makes use of factors from two categories i.e. knowledge factor and possession factor. Use of multiple factors i.e. alphanumeric password, Stego-image, one time password and digital signature from two categories makes the scheme stronger. The proposed protocol provides identity management, mutual authentication and session key agreement between user and service provider. The scheme provides facilities for changing credentials such as password, Stego-image file etc. The scheme also provides facility to get new credentials if the user loses/forgets any credential. Security analysis illustrates that our scheme resists common security attacks. Our scheme is well suited for cloud computing environment because of its strong security features.