

A Major Project Report On

**An Access Control Mechanism based on Authorization  
Certificates for Cloud Computing: Ensuring User's Anonymity**

Submitted in partial fulfilment of the requirements

for the award of the degree of

**MASTER OF TECHNOLOGY**

**IN**

**SOFTWARE ENGINEERING**

By

**Richa Arora**

(Roll No. 2K13/SWE/17)

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 “**An Access Control Mechanism based on Authorization Certificates for Cloud Computing: Ensuring User's Anonymity**” is a bona fide record of work carried out by Richa Arora (2K13/SWE/17) under my guidance and supervision, during the academic session 2013-2015 in partial fulfillment 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

### ACKNOWLEDGEMENT

With due regards, I hereby take this opportunity to acknowledge a lot of people who have supported me with their words and deeds in completion of my research work as part of this course of Master of Technology in Software Engineering.

To start with I would like to thank the almighty for being with me in each and every step of my life. Next, I thank my parents and family for their encouragement and persistent support.

I would like to express my deepest sense of gratitude and indebtedness to my guide and motivator, **Mr. Manoj Kumar**, Associate Professor, Department of Computer Engineering, Delhi Technological University for his valuable guidance and support in all the phases from conceptualization to final completion of the project.

I wish to convey my sincere gratitude to our Head of Department, and all the faculties and PhD. Scholars of Computer Engineering Department, Delhi Technological University who have enlightened me during my project.

Richa Arora

2K13/SWE/17

# TABLE OF CONTENTS

Certificate	ii
Acknowledgement	iii
List of Figures	vii
List of Tables	viii
Abstract	ix
Chapter 1. Introduction	1
1.1 Cloud Computing	1
1.2 Essential Features	2
1.2.1 On-demand Self-service	2
1.2.2 Broad Network Access	2
1.2.3 Resource Pooling	3
1.2.4 Rapid Elasticity	3
1.2.5 Measured Service	3
1.3 Cloud Deployment Models	3
1.3.1 Private Cloud	3
1.3.2 Community Cloud	4
1.3.3 Public Cloud	5
1.3.4 Hybrid Cloud	5
1.4 Cloud Service Model	5
1.4.1 IaaS	5
1.4.2 PaaS	6
1.4.3 SaaS	7
1.5 Security Challenges	7
1.5.1 Confidentiality	7
1.5.2 Integrity	7
1.5.3 Availability	8

1.5.4	Security Management	8
1.6	Access Control	8
1.7	Performance Evaluation	9
1.7.1	Security	9
1.7.2	Dynamic Data Sharing	9
1.7.3	Fine Grained Access Control	9
1.7.4	Accountability	9
1.7.5	Scalability	9
1.8	Motivation	10
1.9	Problem Statement	10
1.10	Scope of Work	11
1.11	Thesis Organization	12
Chapter 2.	Literature Survey	13
2.1	Distributing Decryption Key Directly	13
2.2	Key-policy Attribute based Encryption	14
2.3	Cipher text-policy Attribute based Encryption	16
2.4	Profile based Access Control	17
2.5	FADE	18
2.5.1	File Upload	18
2.5.2	File Download	19
2.6	MTBAC	20
2.7	Trust and Role Based	22
2.8	Access Control Matrix	23
2.9	Risk Based Access Control	24
2.10	Summary of the existing mechanisms	25
Chapter 3.	Security Architecture of Cloud Computing	27
Chapter 4.	Proposed Algorithm and Framework	32
4.1	Authorization Certificates	32
4.2	System Model	34
4.3	Proposed Algorithm	35

4.3.1	Set up	35
4.3.2	Request for Authorization Certificates	36
4.3.3	File Download	40
4.3.4	Access Right Revocation	43
Chapter 5.	Implementation and Results	45
Chapter 6.	Security Analysis	49
Chapter 7.	Conclusion	51
	References	52

## List of Figures

Fig. 1 :	Cloud Computing Model	2
Fig. 2 :	Cloud Deployment Models	4
Fig. 3 :	Cloud Service Models	6
Fig. 4 :	Example of Access Structure	15
Fig. 5 :	File Upload in FADE	19
Fig. 6 :	File Download in Fade	20
Fig. 7 :	Mutual trust structure	21
Fig. 8 :	Trust attributes	22
Fig. 9 :	Framework of role and trust based mechanism	23
Fig. 10 :	User's apprehension in cloud computing	28
Fig. 11 :	Reference architecture for cloud security	28
Fig. 12 :	NIST Security Reference Architecture	30
Fig. 13 :	System Model	35
Fig. 14 :	File Upload	36
Fig. 15 :	Data Flow among Entities	37
Fig. 16 :	Flow Chart for Requesting Certificate	39
Fig. 17 :	Flow Chart for File Downloading	42
Fig. 18 :	UI for uploading files and revoking access	45
Fig. 19 :	File chooser	46
Fig. 20 :	UI for Data sharers	47
Fig. 21 :	UI for requesting authorization certificates	47
Fig. 22 :	UI to access files	48

## **List of Tables**

Table 1 :	List of Profiles	17
Table 2 :	Example of ACM	24
Table 3 :	Access Control Techniques' Summarization	25
Table 4 :	Security Recommendations	31
Table 5 :	Format of certificate	33
Table 6 :	Access Control Matrix	33



## **ABSTRACT**

Access control is a mechanism used to grant or revoke access rights to or from the users. Data stored at remote server is highly confidential and must be protected from unauthorized users. Existing solutions are either too complex to implement or are not able to achieve all the required security parameters. Data is stored in cipher-text form in cloud; therefore there is a need for cipher-text based access control mechanism. The proposed algorithm uses authorization certificates to achieve access control. Data owners issue authorization certificates to the authorized users. Only the owner of certificate is given access to the data stored on remote server. Data owner can revoke access rights of data sharers any time without affecting the cipher-text. The proposed algorithm consumes minimal resources and is easy to implement.