

BONAFIDE CERTIFICATE

This is to certify that the final year project entitled “**HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing**” is a bonafide work done by **Anil Tirkey, Reg. No. 3521010016**, in partial fulfillment of the requirements for the award of the degree of **MASTER OF COMPUTER APPLICATIONS**. Who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported here is does not from any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Signature of Staff In-Charge
(Mr. K. SENTHIL KUMAR)

Head of the Department
(Dr. A. SUBBARAYAN)

Signature of external Guide

Signature of Examiner(s)

Name:

1.

2.

Date:

ACKNOWLEDGEMENT

I would like to thank God the almighty for showering his numerous blessings on me to complete this Term paper successfully.

It is my honor-bound duty to thank **Dr. T.R. PACHAMUTHU, B.Sc., M.I.E.**, Founder and Chancellor, **Prof. P. SATHIYANARAYANAN**, president, **Dr. M. PONNAVAIKKO**, vice- chancellor, **Dr. C. MUTHAMIZHCHELVAN**, Director (E&T), SRM University for their endeavor to provide all the facilities required and the interest they showed in the welfare of the staff.

I render my sincere thanks to Head of the Department of Computer Science & Engineering, **Dr. A.SUBBARAYAN**, Head of the Department of computer Applications, SRM University whose constant support and advice made a world of difference to me.

I am profoundly indebted to my project coordinator **Mrs. S. Kavitha, M.C.A., M. Phil**, Asst. Prof (Sr. G) **SRM University, Kattankulathur** for her innumerable acts of timely advice, encouragements and her guidance throughout the project.

I express my deep sense of heartfelt and immense gratitude to **Mr. K. SENTHIL KUMAR, MCA, M. Phil. (M.S.)**, Asst. Professor (Sr. G), for guiding me throughout my career.

I express my sincere thankfulness to all the teachers and staff of our department. Last but not least; I would like to express my sincere gratitude to my family members, colleagues and friends for their continuous support.

ABSTRACT

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme by Bethencourt et al. and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	BONAFIDE CERTIFICATE ACKNOWLEDGEMENT ABSTRACT TABLE OF CONTENTS LIST OF FIGURES LIST OF SYMBOLS LIST OF ABBREVIATIONS LIST OF TABLES	i ii iii iv viii xi xiii xiii
1.	INTRODUCTION 1.1 PROJECT INTRODUCTION 1.2 OVERVIEW	1 3
2.	SYSTEM ANALYSIS 2.1 EXISTING SYSTEM 2.2 DISADVANTAGES OF EXISTING SYSTEM 2.3 LITERATURE SURVEY 2.4 PROPOSED SYTEM 2.5 FEASIBILITY STUDY	4 4 5 8 9
3.	MODULES	

	3.1 MODULES NAME	11
	3.2 MODULE DESCRIPTION	11
4.	SYSTEM REQUIREMENTS 4.1 HARDWARE REQUIREMENTS 4.2 SOFTWARE REQUIREMENTS 4.3 FUNCTIONAL REQUIREMENTS 4.4 NON FUNCTIONAL REQUIREMENTS	13 13 14 14
5.	DATABASE DESIGN 5.1 INTRODUCTION 5.2 USER/REGISTRATION 5.3 STORAGE 5.4 FILE UPLOAD	15 15 16 16
6.	SYSTEM DESIGN 6.1 DATA FLOW DIAGRAM 6.2 SEQUENCE DIAGRAM 6.3 ACTIVITY DIAGRAM 6.4 USE-CASE DIAGRAM 6.5 CLASS DIAGRAM 6.6 SYSTEM ARCHITECTURE	17 20 21 22 23 24
7.	INPUT/OUTPUT DESIGN 7.1 INPUT DESIGN	25 26

	7.2 OUTPUT DESIGN	
8.	SOFTWARE ENVIRONMENT 8.1 JAVA TECHNOLOGY 8.2 THE JAVA PROGRAMMING LANGUAGE 8.3 JAVA PLATFORM 8.4 WHAT CAN JAVA TECHNOLOGY DO? 8.5 HOW WILL JAVA TECHNOLOGY CHANGE MY LIFE? 8.6 ODBC 8.7 JDBC 8.8 JDBC GOALS 8.9 SQL LEVEL API 8.10 NETWORKING 8.11 JFREE CHART	27 27 29 30 31 32 34 34 35 37 41
9.	IMPLEMENTATION 9.1 INTRODUCTION 9.2 SOURCE CODE	41 41
10.	SNAPSHOTS 10.1 GENERAL 10.2 HOME PAGE 10.3 LOGIN PAGE 10.4 REGISTRATION PAGE 10.5 FILE UPLOAD	60 60 61 62 63 64

	10.6 UPLOAD PROCESS	65
	10.7 CONSUMER LOGIN	66
	10.8 DOWNLOAD DATA	67
11.	SYSTEM TESTING 11.1 GENERAL 11.2 DEVELOPING METHODOLOGIES 11.3 TYPES OF TESTING	67 67 67
12.	FUTURE ASPECTS	70
13.	CONCLUSION	71
	REFERENCES	72

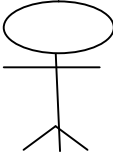

LIST OF FIGURES

FIGURE NO	NAME OF THE FIGURE	PAGE NO.
6.1	DFD ALL LEVEL	17
6.2	DFD LEVEL 1	18
6.3	DFD LEVEL 2	10
6.4	SEQUENCE DIAGRAM	20
6.5	ACTIVITY DIAGRAM	21
6.6	USE-CASE DIAGRAM	22
6.7	CLASS DIAGRAM	23


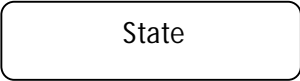
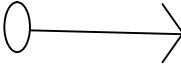
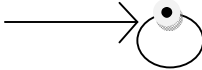

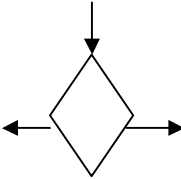
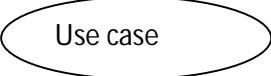
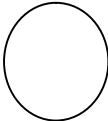
6.8	SYSTEM ARCHITECTURE DIAGRAM	24
8.1	JAVA PROGRAM EXECUTION PROCESS	28
8.2	JAVA VIRTUAL MACHINE	28
8.3	JAVA PLATFORM	29
8.4	JAVA2 SDK 1.3	31
8.5	JAVA COMPILATION AND INTERPRETATION	37
8.6	TCP/IP STACK	38
8.7	IP ADDRESS FORMAT	40
10.1	HOME PAGE	60
10.2	LOGIN PAGE	61

10.3	REGISTRATION PAGE	62
10.4	FILE UPLOAD	63
10.5	DATA UPLOAD PROCESS	64
10.6	CONSUMER LOGIN	65
10.7	DATA DOWNLOAD	66

LIST OF SYMSBOLS

S.NO	NOTATION NAME	NOTATION	DESCRIPTION
1.	Class	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <i>+ public</i> <i>-private</i> </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <i>Class Name</i> <i>-attribute</i> <i>-attribute</i> </div> </div>	Represents a collection of similar entities grouped together.
2.	Association	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class A</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class B</div> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class A</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class B</div> </div>	Associations represent static relationships between classes. Roles represent the way the two classes see each other.
3.	Actor		It aggregates several classes into single classes.
4.	Aggregation	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class A</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class B</div> <div style="width: 10px; height: 10px; background-color: black; margin: 0 auto 10px auto;"></div> </div> <div style="text-align: center;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class A</div> <div style="border: 1px solid black; padding: 5px; text-align: center;">Class B</div> <div style="width: 10px; height: 10px; background-color: black; margin: 0 auto 10px auto;"></div> </div> </div>	Interaction between the system and external environment
5.	Relation (extends)		Extends relationship is used when one use case is similar to another use case but

			does a bit more.
--	--	--	------------------

6.	Communication		Communication between various use cases.
7.	State		State of the process.
8.	Initial State		Initial state of the object
9.	Final state		final state of the object
10.	Control flow		Represents various control flow between the states.
11.	Decision box		Represents decision making process from a constraint
12.	Use case		Interaction between the system and external environment.
13.	Data Process/State		A circle in DFD represents a state or process which has been triggered due to some event or action.

LIST OF ABBREVIATION

S.NO	ABBREVIATION	EXPANSION
1.	DB	Database
2.	TARs	Tree-based Association Rules
3.	XML	Extensible Markup Language
4.	RTAR	Rooted Tree-based Association Rules
5.	ETAR	Extended Tree-based Association Rules
6.	GUI	Graphical User Interface
7.	CSP	Cloud Service Provider

LIST OF TABLES

TABLE NUMBER	TABLE NAME	PAGE NUMBER
5.1	USER/REGISTRATION	15
5.2	STORAGE	16
5.3	FILE UPLOAD	16