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.

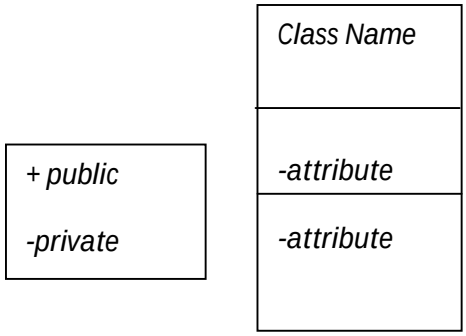
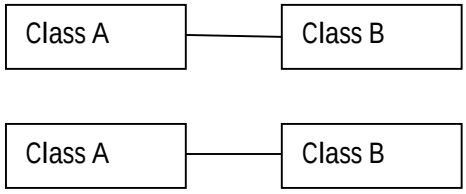
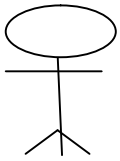
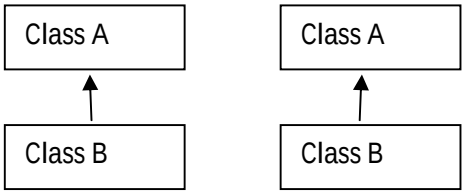
ABSTRACT

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.

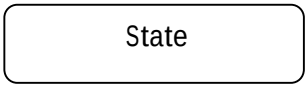
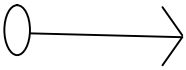
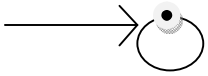
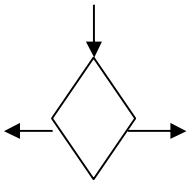
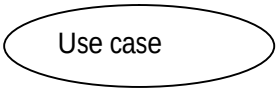
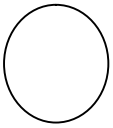
TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYSMBOLS

S.NO	NOTATION NAME	NOTATION	DESCRIPTION
1.	Class		Represents a collection of similar entities grouped together.
2.	Association		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		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 ABBREVATION

S.NO	ABBREVATION	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