"Data Security in Cloud Computing: A Study"

A dissertation submitted for fulfillment for award of the degree of

MASTER OF ENGINEERING

In

COMPUTER SCIENCE & ENGINEERING

Submitted by

SHUBHRADEB MONDAL

Roll No: 30011217004

Reg. No: 173000410020 of 2017-2018

Under the Supervision of

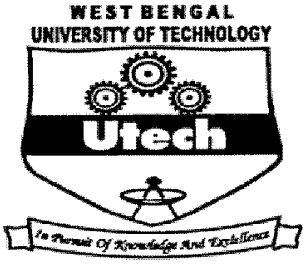
Dr. Koushik Majumder (Assistant Professor)

Mr. Subhanjan Sarkar (Assistant Professor)

Mr. Mihir Sing (Assistant Professor)

Mr. Santanu Chatterjee (Assistant Professor)

Department of Computer Science & Engineering (CSE)



MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL

HARINGHATA, NADIA, WEST BENGAL, 741249

Certificate of Originality

I hereby declare that this submission is of my own work and to the best of my knowledge it contains no materials previously published or written by other person, nor material which to a substantial extent has been accepted for the award of any other degree at Maulana Abul kalam Azad University of Technology, West Bengal or any other educational institution, except where due acknowledgment is made in the thesis.

Also declare the intellectual content of this thesis is the product of my own work, except to the extent that assistance from the others in the project design and conception or in style, presentation and linguistic expression is acknowledged.

I have tried my best to stick to accuracy and perfection; there may be some inadvertent error in this dissertation for which I solely owe responsibility.

……..……

Date & Signature:

SHUBHRADEB MONDAL
Reg. No. -- 173000410004 of 2017- 18
Roll No. – 30011217020

Acknowledgement

This project report on "**Data Security in Cloud Computing: A Study"** is an academic activity on the requirement of partial fulfillment of the degree of Master of Engineering.

I want to thank my respected teachers whose close guidance helped me a lot to complete this project.

I would like to thank Dr. Santanu Phadikar, Head of the Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal for providing me with all the necessary facilities to make my project work.

I shall be thankful to Dr. Koushik Majumder, Mr. Subhanjan Sarkar, Mr. Mihir Sing and Mr. Santanu Chatterjee as my project guide for constantly supporting and guiding me during the course of my work. His words of encouragement motivated me to achieve my goal and impetus to excel.

I want to thank all the faculty members of the institute who helped me for doing the project work.

Last but not the least I thank all my friends for their cooperation and encouragement that they have bestowed on us.

Shubhradeb Mondal Date
M. Tech. (Computer Science & Engineering)
Maulana Abul Kalam Azad University of Technology, West Bengal

Abstract

Cloud computing is a developing area in distributed computing and parallel processing or virtualizations. Cloud computing is a growing technology. It is a computer technology based on internet applications and the user benefits is the high quality data and application software service. Cloud computing use a resource pole and that store in a large volume computing resource in a distributed computing manner that require a significant processing power. Internet user may able to store the data store that they require and also be able to process there information as the requirement.
The cloud computing security issue mainly related to virtualization, data base, resource searing, load balancing and computation network and many organization till like the data searing in centralized data center is not secure because of virtualization vulnerability, access control issue, integrity and confidentiality.

When the data even stored to the third party vendor is not secured also. The service provider has accessibility of data. Homomorphic encryption technique is the trusted way to make more secure the data to protect from internal abuse of data in cloud storage from cloud service provider. In the case of Homomorphic encryption technique the only the user have the access key to both of encryption, decryption of data which provide the security from unauthorized access from the both of internal and external access of data. Filly Homomorphic encryption technique is representing special types of encryption which allows several computational experiments over the cipher texts and tern encrypted result. Filly Homomorphic encryption technique allows multiple times encryption operations with several encryptions techniques. Only data owner have the permission, client to apply Homomorphic encryption technique with their keys, And the decryption result is just as equal to a conducting operation over a plaintext is. Sometimes client is a group member of any particular organization and need to store their data. But due to some location change they need to transfer their data needs to one server to another server. In this case multi-cloud storage data process can handle the situations.

Certificate

This is to certify that the dissertation entitled. This project report on "**Data Security in Cloud Computing: A Study"** which was submitted by Shubhradeb Mondal (Registration No. – 173000410020 of 2017-2018 and Roll No.- 30011217004) in fulfillment of the requirement for the award of degree **Master of Engineering** in **Computer Science & Engineering** Department of Maulana Abul Kalam Azad University of Technology, West Bengal. The project work was carried out by him under our supervision and has been duly completed within the given period of time to the satisfaction of the CSE department, West Bengal University of Technology.

Dr. Koushik Majumder
Assistant Professor
Department of CSE
M.A.K.A.U.T, WB.

Mr. Subhanjan Sarkar
Assistant Professor
Department of CSE
M.A.K.A.U.T, WB.

Mr. Mihir Sing
Assistant Professor
Department of CSE
M.A.K.A.U.T, WB.

Mr. Santanu Chatterjee
Assistant Professor
Department of CSE M.A.K.A.U.T, WB.

Dr. Santanu Phadikar
(Head of the Department)
Department of CSE& SE
M.A.K.A.U.T, WB.

Signature of External

INDEX

Contents **page number**

Chapter Number	Diagram
Chapter 1	
Chapter 2	Figure 2.1 cloud computing basic model Figure 2.2 service models Figure 2.3 Public cloud Figure 2.4 Private cloud Figure 2.5 Hybrid Cloud Figure 2.6 Community cloud Figure 2.7 Cloud architecture Figure 2.8: Data Life Cycle Model in Cloud
Chapter 3	Fig3.1: maintenance security issues Fig3.2: security control form Fig3.3: Framework of security control Fig 3.4: homomorphic encryption scheme Fig3.5: fully homomorphic encryption diagram Fig3.6: VM image integrity and optimization process Fig 3.7: process flow of data encryption Fig3.8: diagrammatically represent of overall system Fig 3.9: proposed model diagram
Chapter 4	Fig 4.1: homomorphic encryption scheme Fig4.2: symmetric, asymmetric encryption and Homomorphic encryption Fig 4.3: Different Homomorphic Encryption techniques Fig 4.4: system model Fig 4.5: Storage model for data Encryption, decryption Fig 4.6 FHE with the help of Data user directly before store over cloud Fig 4.7: client side architecture Fig 4.8: Transferring data from one cloud to another cloud Fig 4.9: Data access with location change and transfer one service provider to another Fig 4.10: applying homomorphic encryption on user side.