# CONTENTS

Acknowledgement  
Abstract  
List of Publications  
Table of Contents  
List of Figures  
List of Tables  
Abbreviations  

**CHAPTER 1: INTRODUCTION**  

1.1 Overview  
   1.1.1 Essential Characteristics  
   1.1.2 Cloud Services  
   1.1.3 Deployment Models  
1.2 Need for Cloud Data Outsourcing  
1.3 Data Management in Cloud Storage  
1.4 Confidentiality of Outsourced Data  
1.5 Cloud Computing System Architecture  
1.6 Need for Data Security in Cloud Storage  
1.7 Security Requirements for Cloud Storage  
   1.7.1 Authentication  
   1.7.2 Authorization  
   1.7.3 Confidentiality  
   1.7.4 Integrity  
   1.7.5 Non-Repudiation  
1.8 Motivations  
1.9 Scope of the Research Work  
1.10 Definition of the Problem  
1.11 Significance of the Proposed Research Work  
1.12 Aim and Objectives  
1.13 Organization of the Thesis  
1.14 Chapter Summary  

**CHAPTER 2: REVIEW OF LITERATURE**  

2.1 Introduction  
2.2 Security Issues and Solutions
2.3 Cryptography Technique for Cloud Storage

2.3.1 Types of Attacks on Cryptography Techniques

2.3.1.1 Ciphertext-Only Attack

2.3.1.2 Known-Plaintext Attack

2.3.1.3 Chosen-Plaintext Attack

2.3.1.4 Chosen-Ciphertext Attack

2.3.1.5 Brute Force Attack

2.3.1.6 Dictionary Attack

2.4 Existing Cloud Security Frameworks

2.5 Data Protection Techniques

2.6 Related Works on Data Encryption

2.6.1 Symmetric Encryption Used for Cloud

2.7 Related works on Data Obfuscation

2.7.1 Masking

2.7.2 Substitution

2.7.3 Shuffling Records

2.7.4 Number and Date Variance

2.7.5 Gibberish Generation

2.7.6 Data Generation

2.8 Chapter Summary

CHAPTER 3: AROMO Security FRAMEWORK TO ENSURE
CONFIDENTIALITY OF OUTSOURCED DATA

3.1 Introduction

3.2 Objectives

3.3 Methodology

3.4 AROMO Framework

3.4.1 SEcurity as a Service (SEaaS)

3.4.2 Key Generation and Management as a Service (KGMaaS)

3.4.3 STorage as a Service (STaaS)

3.5 Framework Operations

3.5.1 Measure of the Security Level of Proposed SSAs

3.6 Block Cipher Cryptography Class

3.6.1 ABC Hackman Tool

3.7 Execution of SSAs in SEaaS
6.4 Proposed AROMONcrypt SSA
   6.4.1 AROMONcrypt Execution Procedure
6.5 Simulation Results
6.6 Result Analysis of AROMONcrypt SSA
6.7 Research Findings and Interpretations
6.8 Chapter Summary

CHAPTER 7: CONCLUSION
7.1 Overview
7.2 Importance of Proposed Work
   7.2.1 SEaaS
      7.2.1.1 AROcrypt SSA
      7.2.1.2 MONcrypt SSA
      7.2.1.3 AROMONcrypt SSA
   7.2.2 KGMaaS
   7.2.3 STaaS
7.3 Measure of Security Level for Proposed SSAs
7.4 Research Findings and Interpretations
7.5 Applications of Research Findings
7.6 Salient Features of Proposed Work
7.7 Limitations and Future Directions

REFERENCES

APPENDICES
(i) Papers Published in the International Journals
(ii) Deployment of Cloud Server in Amazon
(iii) Connect EC2 server to User’s Machine
(iv) Simulation of ABC Hackman Tool to Analysis the SSAs
(v) Base64 Index Table
(vi) Scopus Index of the Research Scholar’s Publications and Citations
(vii) Google Scholar’s Index of the Research Scholar’s Publications and Citations
(viii) Academia.edu Index of the Research Scholar’s Publications and Citations