**LIGHTWEGITH VERFICATION FOR MULTI USER VERIFIABLE SEARCHABLE SYMMETRIC ENCRYPTION**

A PROJECT REPORT

**Submitted by**

**SRITHILLAIKKRASI.B(810015205083)**

**BHARATHI.S(810015205304)**

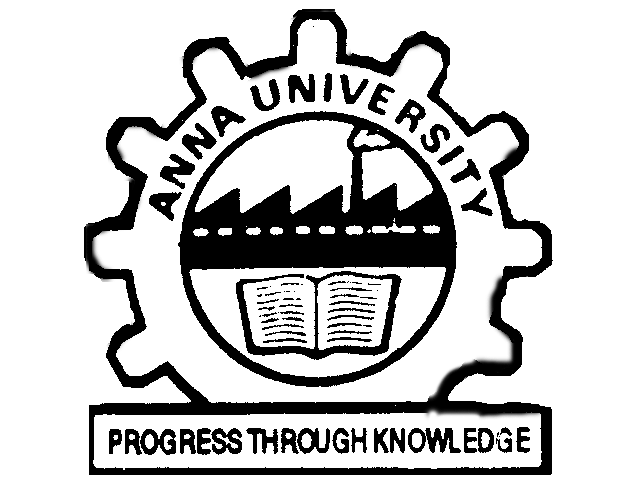
**in partial fulfilment for the aware of the degree**

**of**

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION TECHNOLOGY**

****

**UNIVERSITY COLLEGE OF ENGINEERING ,**

**BIT CAMPUS,TIRUCHIRAPALLI**

**ANNA UNIVERSITY :: CHENNAI 600 025**

**APRIL 2019**

**BONAFIDE CERTIFICATE**

Certificate that the project report **“ LIGHTWEGITH VERFICATION FOR MULTI USER VERIFIABLE SEARCHABLE SYMMETRIC ENCRYPTION ’’** is the bonafied work of **“ SRITHILLAIKKARASI . B (810015205083)** and **BHARATHI.S (810015205304)’’** who carried out the project work under my supervision.

**SIGNATURE SIGNATURE Dr.D.VENKATESAN Mr.C.SURESHKUMAR**

**HEAD OF THE DEPARTMENT SUPERVISOR Department of Information Department of Information Technology Technology** University College of Engineering, University college of Engineering Anna University-BIT Campus , Anna University-BIT Campus,Tiruchirappalli-620 024 . Tiruchirappalli-620 024.

**Submitted for project viva voce examination held on …………………….**

**Internal Examiner External Examiner**

**DECLARATION**

We hereby declare that the work entitled **“LIGHTWEGITH VERFICATION FOR MULTI USER VERIFIABLE SEARCHABLE SYMMETRIC ENCRYPTION’’** is submitted in partial fulfilment of the requirement for the award of the degree in B.TECH in University college of Engineering, BIT Campus, Anna University, Tiruchirappali. It is the record of our own work carried out during the academic year 2018-2019 under the supervisor and guidance of **Mr.C.SURESHKUMAR**, Teaching fellow, Department of Information Technology, University College of Engineering , BIT Campus, Anna University, Tiruchirappali. The extent and source of information are derived from the existing literature and have been indicated through the dissertation at the appropriate place.

**SRITHILLAIKKARASI .B**

**(810015205083)**

**BHARATHI.S**

**(8100150205304)**

**I certify that the declaration made above by the candidates is true**

**Signature of the Guide**

**Mr.C.SURESHKUMAR,**

Teaching Fellow,

Department of Information

Technology,

Universite college of Engineering,

Anna University-BIT Campus,

Tiruchirapalli-620 024.

**ACKNOWLEDGEMENT**

We would like to thank our honourable Dean **Dr.T.SENTHILKUMAR,** Professor for having provided us with all required facilities to complete our project without hurdles.

We would also like to express our sincere thanks to **Dr.D.VENKATESAN,** Head of the Department of Information Technology ,for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of this project work.

We would like to thank our project Coodinator **MRS. V.M.PRIYADHARSHINI,** Assistant Professor, Department of Information Technologyand **Mr.M.PRASANNAKUMAR,** Teaching Fellow, Department of computer science and engineering for his kind support.

We would like to thank and express our deep sense of gratitude to our project guide **Mr.C.SURESHKUMAR,** Teaching Fellow, Department of Information Technology for his valuable guidance throughout the project. We also extend our thanks to all other teaching and non teaching staff for their encouragement and support.

We thank our beloved parents and friends for their full support in the moral development of this project.

**ABSTRACT**

In a client storage system , the securely performed keyword queries and the files can be retrieved efficiently from server with data privacy . The server may return incorrect or incomplete result to a client where the server may be untrusted . so , the client does not maintain it entire dataset locally . SSE is that the cloud server does not learns about the information in the files or keyword during the searching process . In this paper , we present a multiuser verifiable searchable Symmetric encryption (MVSSE) schema that achieves all the desirable features of a verifiable SSE & allows multiple users to perform searching allows multiple users to perform searching MVSSE functionality works under the university composable security framework . The multi user verifiable SSE schema is UC secure . we also implement our schema to verify its high performance based some real dataset .

**TABLE OF CONTENTS**

**CHAPTER NO TITLE PAGE NO**

**ABSTRACT V**

**LIST OFFIGURES VIII**

**LIST OF ABBREVIATION IX**

**1 INTRODUCTION 1**

* 1. OVERVIEW 1
  2. INTRODUCTION TO AUDITING 2
  3. PROBLEM STATEMENT 5
  4. OBJECTIVE 6
  5. ORGANISATION OF REPORT 6

**2 LITERATURE SURVEY 7**

2.1 SUMMARY 11

**3 SYSTEM ANALYSIS 12**

3.1 EXISTING SYSTEM 12

3.1.1 DISADVANTAGE OF EXISTING SYSTEM 12

3.2 PROPOSED SYSTEM 12

3.2.1 SYSTEM ARCHITECTURE DESIGN 13

3.2.2 ADVANTAGE 13

3.2.3 PROPOSED SYSTEM BLOCK DIAGRAM 14

**4 IMPLEMENTATION 15**

4.1 MODULE 15

4.1.1 REGISTERATION 15

4.1.2 LOGIN 15

4.1.3 DATA PROVIDER 16

4.1.4 DATA USER 16

4.1.5 DATA SERVER 16

4.2 ALGORITHM **17**

4.2.1 SYMMETRIC ENCYPTION 17

**5 SOFTWARE ENVIRONMENT 20**

**6 SYSTEM DESIGN 38**

6.1 UML DIAGRAM 38

6.2 USE CASE DIAGRAM 40

6.3 CLASS DIAGRAM 41

6.4 SEQUENCE DIAGRAM 42

6.5 DEPLOYMENT DIAGRAM 43

6.6 DATA FLOW DIGRAM 44

**7 SYSTEM TESTING 45**

**8 CONCLUSION 48**

8.1 CONCLUSION 48

8.2 REFERENCES 49

**APPENDIX 1 : SCREENSHOTS AND SOURCECODE 51**

**SCREENSHOTS 51**

**SOURCECODE 5**

**LIST OF FIGURE**S

**S.NO TITLE PAGE NO**

1 CLOUD DATA STORAGE ARCHITECTURE 4

2 ARCHITECTURE FOR MULTI USER VERIFIABLE

SEARCHABLE SYMMETRIC ENCRYTION 13

3 WORKING OF COMPILER 21

4 EXECUTION OF JAVA PROGRAM 22

5 DEPICTS A PROGRAM RUN ON JAVA PLATFROM 23

6 DEPICTS WHAT IS INCLUDED IN JAVA 2 SDK 24

7 INTERPRETER OF THE PROBLEM 27

8 TCP/IP STACK 28

9 GENERAL J2ME ARCHITECTURE 34

**LIST OF ABBERIVATION**

CSP CLOUD SERVICE PROVIDER

TPA THIRD PARTY AUDITOR

SEPDP SECURE AND EFFICIENT PRIVACY PRESERVING

PROVABLE DATA POSSESSION SCHEME

BTC BITCIONS

MVSSE MULTI USER VERIFIABLE SEARCHABLE SYMMETRIC

ENCRYPTION

SSE SEARCHABLE SYMMETRIC ENCRYPTION

SE SEARCHABLE ENCRYPTION

IBKEM IDENTITY BASED KEY ENCAPSULATION

MECHANISM

RO RANDOM ORACLE

SPCHS SEARCHABLE PUBLIC KEY CIPHER TEXTS WITH

HIDDEN STRUCTURES

KS KEYWORD SERVER

SA-PEKS SERVER AIDED PUBLIC KEY ENCRPTION WITH

KEYWORD SEARCH

KGA KERWORD GUESSING ATTACK