**VERIFIABLE SEARCHABLE ENCRYPTION FRAMEWORK**

# A PROJECT REPORT

## ***Submitted by***

KALAIDHARANI V (422619104020)

TAMIZHSELVAN D (422619104044)

## VARSHINI B (422619104046)

*In partial fulfillment for the award of the degree*

*Of*

**BACHELOR OF ENGINEERING**

# IN

**COMPUTER SCIENCE AND ENGINEERING**



**UNIVERSITY COLLEGE OF ENGINEERING, PANRUTI**

**ANNA UNIVERSITY: CHENNAI 600 025**

**MAY 2023**

**ANNA UNIVERSITY: CHENNAI 600 025**

# BONAFIDE CERTIFICATE

Certified that this project report **“VERIFIABLE SEARCHABLE ENCRYPTION FRAMEWORK”** is the bonafide work of **“KALAIDHARANI V (422619104020), TAMIZHSELVAN D (422619104044), VARSHINI B (422619104046)”** who carried out the project work under my supervision.

|  |  |
| --- | --- |
| **SIGNATURE** | **SIGNATURE** |
| **Dr. D. MURUGANANDAM, M.Tech, Ph.D.,**  **Assistant Professor** | **Dr. J.PARANTHAMAN,M.E., Ph.D.,**  **Assistant Professor** |
| **HEAD OF DEPARTMENT** | **SUPERVISOR** |
| Computer Science & Engineering University College of Engineering | Computer Science & Engineering University College of Engineering |
| Panruti – 607106    EXAMINATION HELD ON \_\_\_\_\_\_\_\_\_\_\_ | Panruti – 607106 |
| **INTERNAL EXAMINER** | **EXTERNAL EXAMINER** |

**DECLARATION**

We hereby declare that the work entitled “**VERIFIABLE SEARCHABLE ENCRYPTION FRAMEWORK**” is submitted in partial fulfillment for the award of the degree in Bachelor of Engineering in Computer Science & Engineering. University College of Engineering, Panruti is a record of our own work carried out by us during the academic year 2022-2023. Under the supervision and guidance of **Dr.J.Paranthaman M.E., Ph.D., Assistant Professor/CSE**, Department of Computer Science and Engineering, UNIVERSITY COLLEGE OF ENGINEERING PANRUTI. The extent and source of information are derived from the existing literature and have been indicated through dissertation at the appropriate places. The matter embodied in this work is original and has not been submitted for the award of any other degree or diploma, either in this or any other university.

|  |  |  |
| --- | --- | --- |
| **REGISTER NUMBER** | **NAME** | **SIGNATURE** |
| 422619104020 | Kalaidharani V |  |
| 422619104044 | Tamizhselvan D |  |
| 422619104046 | Varshini B |  |

I certify that the declaration made above by the candidate is true

**SIGNATURE**

**Dr. J.PARANTHAMAN,M.E., Ph.D.,**

**Assistant Professor**

**SUPERVISIOR**

Computer Science & Engineering

University College of Engineering

Panruti – 607106

# ABSTRACT

Searchable encryption (SE) allows cloud tenants to retrieve encrypted data while preserving data confidentiality securely. Many SE solutions have been designed to improve efficiency and security, but most of them are still susceptible to insider Keyword-Guessing Attacks (KGA), which implies that the internal attackers can guess the candidate keywords successfully in an off-line manner. Also in existing SE solutions, a semi-honest- but-curious cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly (e.g., to save storage space). To address these two challenging issues, we first construct the basic Verifiable SE Framework (VSEF), which can withstand the inside KGA and achieve verifiable searchability. Based on the basic VSEF, we then present the enhanced VSEF to support multi-keyword search, multi-key encryption and dynamic updates (e.g., data modification, data insertion, and data deletion) at the same time, which highlights the importance of practicability and scalability of SE in real- world application scenarios. We conduct extensive experiments using the Enron email dataset to demonstrate that the enhanced VSEF achieves high efficiency while resisting to the inside KGA and supporting the verifiability of search results .

iii

**TABLE OF CONTENTS**

iv

|  |  |  |
| --- | --- | --- |
| **CHAPTER**  **NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | iii |
|  | **LIST OF FIGURES** | vi |
| 1 | **INTRODUCTION** | 1 |
|  | 1.1 Contribution | 2 |
|  | 1.2 System Model | 3 |
|  | 1.3 Security Model | 5 |
|  | 1.4 Objectives | 5 |
|  | 1.5 Scope | 5 |
| 2 | **LITERATURE SURVEY** | 6 |
|  | 2.1 A search optimized blockchain-based verifiable searchable symmetric encryption framework | 6 |
|  | 2.2 Verifiable Attribute-Based Keyword Search Scheme over Encrypted Data for Personal Health Records in Cloud | 7 |
|  | 2.3 A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services | 8 |
|  | 2.4 Enabling verifiable multiple keywords search over encrypted cloud data | 9 |
|  | 2.5 An Efficient Public-Key Searchable Encryption Scheme Secure against Inside Keyword Guessing Attacks | 10 |
| 3 | **SYSTEM ANALYSIS** | 11 |
|  | 3.1 Existing System | 11 |
|  | 3.2 Disadvantages | 11 |
|  | 3.3 Proposed System | 12 |
|  | 3.4 Advantages | 12 |
| 4 | **SYSTEM REQUIREMENTS** | 13 |
|  | 4.1 Hardware Requirements | 13 |
|  | 4.2 Software Requirements | 13 |
| 5 | **SOFTWARE DESCRIPTION** | 14 |
|  | 5.1 Software:C# | 14 |
|  | 5.2 Mongo Database | 17 |
|  | 5.3 FTP Cloud | 20 |
| 6 | **SYSTEM DESIGN** | 23 |
|  | 6.1 System Architecture | 23 |
|  | 6.2 Sequence Diagram | 24 |
| 7 | **SYSTEM IMPLEMENTATION** | 26 |
|  | 7.1 Elliptical Curve Cryptography | 27 |
|  | 7.2 Secure Socket Layer | 27 |
| 8 | **SYSTEM TESTING** | 28 |
|  | 8.1 Unit Testing | 29 |
|  | 8.2 Functional Testing | 30 |
|  | 8.3 Integration Testing | 30 |
| 9 | **SYSTEM STUDY** | 31 |
| 10 | **SCREENSHOTS** | 60 |
| 11 | **CONCULSION AND FUTURE**  **ENCHANCEMENT** | 63 |
|  | **REFERENCES** | 65 |

v

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIG.NO.** | **TITLE** | **PAGE NO.** |
| 1 .1 | The System Model of VSEF | 4 |
| 6.1 | The System Architecture of VSEF | 23 |
| 6.2 | Data Uploading | 24 |
| 6.3 | Result Verification | 25 |
| 6.4 | Data Update | 25 |
| 7.1 | Simple Elliptical Curve | 27 |
| 7.2 | Secure Socket Layer | 27 |
| 10.1 | Dashboard | 60 |
| 10.2 | Login Page | 60 |
| 10.3 | File Uploading | 61 |
| 10.4 | Key Generation | 61 |
| 10.5 | File Downloading | 62 |

vi