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

Dr. D. MURUGANANDAM, M.Tech, Ph.D.,
Assistant Professor

HEAD OF DEPARTMENT
Computer Science & Engineering
University College of Engineering
Panruti – 607106

SIGNATURE

Dr. J.PARANTHAMAN,M.E., Ph.D.,
Assistant Professor

SUPERVISOR
Computer Science & Engineering
University College of Engineering
Panruti – 607106

EXAMINATION HELD ON _____

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 .

TABLE OF CONTENTS

LIST OF FIGURES