A

Major Project Report

On

SECURE KEYWORD SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING

Submitted to

Jawaharlal Nehru Technological University, Hyderabad

In partial fulfillment of the requirements for the award of Degree of

Bachelor of Technology

in

Computer Science & Engineering

by

PITTALA. GOUTHAMI	(196Y1A0583)
PATHIPAKA. RAKSHITHA	(196Y1A0580)
RUDROJU. AKSHAYA	(196Y1A0587)

Under the guidance of

MR. M. RUCHINANDAN
Asst. Professor

Department of Computer Science &Engineering

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN
(Approved by AICTE, New Delhi, Affiliated to JNTU, Hyderabad)
Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371(T.S.), Website : www.sritw.org

2022-2023

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371(T.S.), Website : www.sritw.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled "**SECURE KEYWORD SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING**" is submitted by **PITTALA. GOUTHAMI (196Y1A0583), PATHIPAKA. RAKSHITHA (196Y1A0580)** and **RUDROJU. AKSHAYA (196Y1A0587)** in the partial fulfillment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering during academic year 2022-23.

Mr. M. RUCHINANDAN
Project Guide

Dr. E. SUDARSHAN
Head of the Department

EXTERNAL EXAMINER

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

S.R.I.T. FOR WOMEN ★ WARANGAL ★

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data.

The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this project, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

S.R.I.T. FOR WOMEN WARANGAL

Principal
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (TS)