

**CONJUNCTIVE KEYWORD SEARCH WITH KEY WRAPPING
AND SPONGE RE ENCRYPTION FUNCTION FOR E-HEALTH
CLOUDS**

*A project report submitted in partial fulfillment of the requirements for the
award of the Degree of
BACHELOR OF TECHNOLOGY*

In

COMPUTER SCIENCE AND ENGINEERING

Submitted by:

K.ANITHA

Reg no:14811A0533

Y.RAHULKALKI

Reg no:14811A0555

D.E.MANIKANTA PRABHUVU

Regd No: 14811A0517

S.ANIL KUMAR

Reg no:14811A0562

SM.NAINA MOHAMMED

Reg no:14811A0565

Under the esteemed guidance of

V.TRINADHA M.Tech.,

Assistant Professor.

Department of Computer Science and Engineering



AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)

(Accredited by NAAC, UGC & NBA, AICTE)

MAKAVARAPALEM, NARSIPATNAM,

VISAKHAPATNAM DIST

(2014-2018)

**AVANTHI INSTITUTE OF ENGINEERING AND
TECHNOLOGY**

(Accredited to NBA, Affiliated to JNTU Kakinada & Approved by
AICTE)

**TAMARAM, MAKAVARAPALEM, NARSIPATNAM-531113
VISAKHAPATNAM (DIST)**



**DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING
CERTIFICATE**

This is Certify that this project work entitled "CONJUNCTIVE KEYWORD SEARCH WITH KEY WRAPPING AND SPONGE RE ENCRYPTION FUNCTION FOR E-HEALTH CLOUDS" is submitted by K. ANITHA (14811A0533), D. E. MANIKANTA PRABHUVU (14811A0517), Y. RAHULKALK I (14811A0555), S. ANILKUMAR (14811A0562), S. NAINA MOHAMMAD (14811A0565) in partial fulfillment of the requirements for the award of BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING is a record of bonafied work carried out by them under my guidance and supervision during the academic year 2014-2018.

Project Guide

Head of the Department
Head of the Department

Computer Science and Engineering
Avanthi Institute of Engg. & Technology,
Tamaram, Makavarapalem (M),
Narsipatnam, Visakhapatnam-531113.

External Examinee

ABSTRACT

The Distributed healthcare data Keyword cloud computing system considerably facilitates secure and efficient patient treatment for medical consultation by sharing personal health information among the healthcare providers. This system should bring about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem proposed a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute based designated verifier signature, a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed healthcare data Keyword cloud computing system is proposed.

The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Confidentiality refers to the secrecy of the stored data so that only the client can read the contents of the stored data. To solve the problem of confidentiality, data encryption schemes can come in handy to provide the users with some control over the secrecy of their stored data.

This has been adopted by many recent researches which allow users to encrypt their data before outsourcing to the cloud. The searchable encryption scheme is a technology to incorporate security protection and favorable operability functions together, which can play an important role in the Maintaining of record system. In this paper, we introduce a novel cryptographic primitive named as key wrapping encryption technique using sponge function for secures data storage and also time based conjunctive keyword search for information Retrieval which and reduce the guessing attacks.