

A
Major Project Report
on
**MULTI-AUTHORITY ATTRIBUTE-BASED
KEYWORD SEARCH OVER ENCRYPTED CLOUD
DATA**

Submitted to
Jawaharlal Nehru Technological University, Hyderabad
in partial fulfilment of the requirements for the award of Degree of
Bachelor of Technology

in
Computer Science & Engineering
by

P. SRILAXMI PRASANNA	(196Y1A0579)
S. SUPRATHIKA	(196Y1A0589)
P. DIVYA DARSHINI	(206Y5A0506)
V. AKSHITA	(206Y5A0510)

Under the guidance
of

Mr. M. RANJITH KUMAR
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

Rajan

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 "MULTI-AUTHORITY ATTRIBUTE-BASED KEYWORD SEARCH OVER ENCRYPTED CLOUD DATA" is submitted by *P. Srilaxmi Prasanna (196Y1A0579)*, *S. Suprathika (196Y1A0589)*, *P. Divyadarshini (206Y5A0506)* and *V. Akshita (206Y5A0510)* in the partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering during academic year 2022-2023


Mr. M. RANJITH KUMAR
Project Guide


External Examiner


Dr. E. SUDARSHAN
Head of the Department


PRINCIPAL



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

ABSTRACT

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.



Rijan

Principal

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