

A  
Major Project Report  
on  
**IDENTITY-BASED ENCRYPTION TRANSFORMATION FOR  
FLEXIBLE SHARING OF ENCRYPTED DATA IN PUBLIC CLOUD**

*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*

NALUBALA HARIPRIYA  
PITTA SAI SRI  
TADURI PREETHI  
PANCHAGIRI MANISHA

(196Y1A0571)  
(196Y1A0582)  
(196Y1A05A0)  
(196Y1A0578)

Under the guidance  
of

**Mrs. A. KALYANI**

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](http://www.sritw.org)

**2022-2023**

*Rajani*



**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](http://www.sritw.org)

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



### CERTIFICATE

This is to certify that the project entitled “**IDENTITY-BASED ENCRPTION TRANSFORMATION FOR FLEXIBLE SHARING OF ENCRYPTED IN PUBLIC CLOUD**” is submitted by *N. Haripriya (196Y1A0571)*, *P. Sai Sri (196Y1A0582)*, *T. Preethi (196Y1A05A0)* and *P. Manisha (196Y1A0578)* 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.

**Mrs. A. KALYANI**  
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.)

## ABSTRACT

With the rapid development of cloud computing, an increasing number of individuals and organizations are sharing data in the public cloud. To protect the privacy of data stored in the cloud, a data owner usually encrypts his data in such a way that certain designated data users can decrypt the data. This raises a serious problem when the encrypted data needs to be shared to more people beyond those initially designated by the data owner. To address this problem, we introduce and formalize an Identity-Based Encryption Transformation (IBET) model by seamlessly integrating two well-established encryption mechanisms, namely Identity-Based Encryption (IBE) and Identity-Based Broadcast Encryption (IBBE). In IBET, data users are identified and authorized for data access based on their recognizable identities, which avoids complicated certificate management in usual secure distributed systems. More importantly, IBET provides a transformation mechanism that converts an IBE ciphertext into an IBBE ciphertext so that a new group of users not specified during the IBE encryption can access the underlying data. We design a concrete IBET scheme based on bilinear groups and prove its security against powerful attacks. Thorough theoretical and experimental analyses demonstrate the high efficiency and practicability of the proposed scheme.



*Rijan*

**Principal**

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



*Rijan*

**Principal**

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