A TRACEBLE ATTRIBUTE WITH OUT SOURCED DECRYPTION IN CLOUD STORAGE

A project report submitted in partial fulfillment of the requirements
for the award of the Degree of

BACHELOR OF TECHNOLOGYIN
COMPUTER SCIENCE & ENGINEERING

Submitted by

M.YAMINI NAGADEVI(17815A0502)

S.RAVI KARUN KUMAR(16811A0579)

V.PRIYA MAHA LAXMI(16811A0584)

V.GAYATRI(16811A0587)

S.BADIRUDDIN(16811A0581)

Under the esteemed guidanceof

Mr. M.CHIRANJEEVI(M.Tech)
Assistant Professor

Department of Computer Science & Engineering

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(Affiliated to JNTU Kakinada & Approved by AICTE)
TAMARAM, MAKAVARAPALEM, NARSIPATNAM-531113
VISAKHAPATNAM (DIST)
(2016-2020)

AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Affiliated to JNTU Kakinada & Approved by AICTE)

TAMARAM, MAKAVARAPALEM,
NARSIPATNAM-531113VISAKHAPATNAM (DIST)

CERTIFICATE

This is to certify that the Project Report entitled **"A TRACEBLE ATTRIBUTE WITH OUT SOURCED DECRYPTION IN CLOUD STORAGE"** M.YAMININAGADEVI(17815A0502), S.RAVIKARUNKUMAR(16811A0579),V.PRIYAMAHALAXMI(16811A0584),V.GAYATRI(16811A0587),S.BADIRUDDIN(16811A0581)In partial fulfilment of the requirements for the degree of B.Tech (C.S.E) in Department of Computer Science & Engineering, at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY affiliated by Jawaharlal Nehru Technological University Kakinada ,is a record of bonafide work carried out by them under my guidance and supervision.

The results embodied in this thesis have not been submitted to any university orinstitute for the award or any degree of diploma.

M.CHIRANJEEVI P.M.Manohar
Project Guide Head of the Department

External Examiner

ABSTRACT

The attribute-based encryption (ABE) is the most promising way to ensure data security and to realize one-to-many fine-grained data sharing simultaneously. However, it cannot be well applied in the cloud-assisted IoT due to the complexity of its decryption and the decryption key leakage problem. To prevent the abuse of decryption rights, we propose a multiauthority ABE scheme with white-box traceability in this paper. Moreover, our scheme greatly lightens the overhead on devices by outsourcing the most decryption work to the cloud server. Besides, fully hidden policy is implemented to protect the privacy of the access policy. Our scheme is proved to be selectively secure against replayable chosen ciphertext attack under the random oracle model. Some theory analysis and simulation are described in the end.