

# Data Integrity Auditing without Private Key Storage for Secure Cloud Storage

*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

B.YUVA KIRAN SAI	Reg.No.16811A0507
A.SWATHI	Regd.No.16811A0502
B.LAVANYA	Regd.No.16811A0508
G.GANGADHAR	Redg.No.16811A0524

Under the guidance of

Mr. M.CHIRANJEEVI, M. Tech

*Assistant professor*

*Department of Computer Science and Engineering*



AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

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

(Accredited by NAAC, UGC & NBA, AICTE)

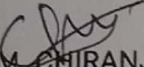
MAKAVARAPALEM, NARSIPATNAM,  
VISAKHAPATNAM-531113 (2016-2020)

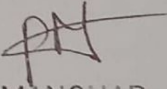
AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY  
(Approved by AICTE, New Delhi & Permanently affiliated to JNTU Kakinada)  
(Accredited by NAAC, UGC & NBA, AICTE)  
MAKAVARAPALEM, NARSIPATNAM,  
VISAKHAPATNAM-531113



## CERTIFICATE

This is to certify that the project entitled "Data Integrity Auditing without Private Key Storage for Secure Cloud Storage" in partial fulfillment for the of degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING, at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is an bonafied work carried out by B.YUVA KIRAN SAI (16811A0507), A.SWATHI (16811A0502), B.LAVANYA (16811A508), G.GANGADHAR (16811A0524) under the guidance and supervision during 2019-2020.

  
Mr. M. CHIRANJEEVI  
Project Guide

  
Mr. P. MANOHAR  
Head of the Department

External Examiner

## ABSTRACT

Using cloud storage services, users can store their data in the cloud to avoid the expenditure of local data storage and maintenance. To ensure the integrity of the data stored in the cloud, many data integrity auditing schemes have been proposed. In most, if not all, of the existing schemes, a user needs to employ his private key to generate the data authenticators for realizing the data integrity auditing. Thus, the user has to possess a hardware token (e.g., USB token, smart card) to store his private key and memorize a password to activate this private key. If this hardware token is lost or this password is forgotten, most of the current data integrity auditing schemes would be unable to work. In order to overcome this problem, we propose a new paradigm called data integrity auditing without private key storage and design such a scheme. In this scheme, we use biometric data (e.g., iris scan, fingerprint) as the user's fuzzy private key to avoid using the hardware token. Meanwhile, the scheme can still effectively complete the data integrity auditing. We utilize a linear sketch with coding and error correction processes to confirm the identity of the user. In addition, we design a new signature scheme which not only supports block less verifiability, but also is compatible with the linear sketch. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.