

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

BELGAUM 590014



KSCST sponsored

PROJECT REPORT

ON

**“ENSURING DATA SECURITY IN CLOUD
COMPUTING”**

Submitted in partial fulfillment of the requirements for the
degree of

**BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE AND ENGINEERING**

Submitted by:

Mr. DHAWAL JAIN

4SU08IS020

Mr. NARAYANA N

4SU08IS031

Mr. SHISHIR SIDDHARTHA

4SU08IS040

Mr. RAJATH M C

4SU07IS033

Under the Guidance of:

Mr. PRASAD B.S., B.E. M.Tech.

Lecturer

Department of Information Science and Engineering
SDM Institute of Technology, Ujire



DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

SDM INSTITUTE OF TECHNOLOGY, UJIRE-574240

(Approved by AICTE, Affiliated to VTU, Belgaum)

2011-2012

ABSTRACT

Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks .