VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI

A PROJECT REPORT ON

"SECURE DATA SHARING IN CLOUD FOR MEDICAL DATA"

Submitted in partial fulfillment for the award of Degree of,

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE &ENGINEERING

By

PRIYANKA S P	**4AL15CS072**
RANJITH	**4AL15CS079**
SHRIDEVI PRABHU B S	**4AL15CS089**
NALINI	**4AL16CS401**

Under the Guidance of

Mr. Vasudev S Shahapur

Associate Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOODBIDRI-574225, KARNATAKA

2018 – 2019

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225, KARNATAKA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"SECURE DATA SHARING IN CLOUD FOR MEDICAL DATA"** has been successfully completed by

PRIYANKA S P	**4AL15CS072**
RANJITH	**4AL15CS079**
SHRIDEVI PRABHU B S	**4AL15CS089**
NALINI	**4AL16CS401**

the bonafide students of **DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY** of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the year 2018–2019. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the Bachelor of Engineering Degree.

Mr. Vasudev S Shahapur	**Dr. Manjunath Kotari**	**Dr. Peter Fernandes**
Project Guide	**Head of the department**	**PRINCIPAL**
		Alva's Institute of Engg. & Technology,
		Mijar, MOODBIDRI - 574 225, D.K

External Viva

Name of the Examiners   **Signature with Date**

1. MAHESH B.L.

2. Dr. L M Nirur Bru

ABSTRACT

There is a significant increase in the amount of data loss in corporate servers in the cloud environments. This includes password compromise in the cloud and account hijacking, thus leading to severe vulnerabilities of the cloud service. Current authentication methods require the users to use their credentials to gain access to cloud service. However once the credential is compromised, the attacker will gain access to the cloud service easily. This paper proposes a novel scheme that does not require the user to present his password, and yet is able to prove his ownership of access to the cloud service using a variant of zero-knowledge proof. A challenge-response protocol is devised to authenticate the user, requiring the user to compute a one-time pad (OTP) to authenticate himself to the server without revealing password to the server.