SAPTHAGIRI COLLEGE OF ENGINEERING

14/5, Chikkasandra, Hesaraghatta Main Road, Bangalore-560057

Department of Computer Science and Engineering

Certificate

SAPTHAGIRI
College of Engineering

Certified that the project work entitled "**Two Party Key Issuing Protocols for Improving Attribute-Based Data Sharing Scheme Revisited in Cloud**" carried out by **Preethi P(1SG13CS075), Ranjitha K T(1SG13CS084), Anithalakshmi C (1SG14CS402), Ramya J(1SG14CS417),** bonafide students of this institute, in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering of Visvesvaraya Technological University, Belgaum** during the academic year **2016-17.** It i certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the repor deposited in the department library. The project progress report has been approved as it satisfies the academi requirements in respect of Project work prescribed for the said degree.

22/6/17

Signature of the Guide

Prof. Veena K.R

Assisant Professor

22.6.17

Signature of the HOD

for **Dr. Prashanth C.M**

Professor & Head

Signature of the Principal

Dr. Aswatha Kumar M

Principal

Dr. Aswatha Kumar. M
Principal
Sapthagiri College of Engineering
No. 14/5, Chikkasandra,
Hesaraghtta Main Road,
Bangalore-560 057

Name of the Examiners

1………………………

2………………………

Signature with date

………………………

………………………

ABSTRACT

Cipher text-policy attribute-based encryption (CP-ABE) is a very promising encryption technique for secure data sharing in the context of cloud computing. Data owner is allowed to fully control the access policy associated with his data which to be shared. However, CP-ABE is limited to a potential security risk that is known as key escrow problem, whereby the secret keys of users have to be issued by a trusted key authority. Most of the existing CP-ABE schemes cannot support attribute with arbitrary state. Attribute-based data sharing scheme is revisited in order to solve the key escrow issue, so that the resulting scheme is friendlier to cloud computing applications. An improved two-party key issuing protocol is proposed that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. The performance analysis and the security proof show that the proposed scheme is able to achieve efficient and secure data sharing in cloud computing compromise the data for commercial benefits.