VISVESVARAYA TECHNOLOGICAL UNIVERSITY
JNANA SANGAMA CAMPUS, BELAGAVI-590010

A PROJECT REPORT

On

"PRIVACY PRESERVING AND DATA ANALYSIS IN MEDICAL HEALTH RECORDS"

Submitted by

KAVYA K	4AL13IS012
KRUPA KC	4AL13IS016
UDYAVAR PRATEEKSHA JAYANTH	4AL13IS035
VISHRUTH	4AL13IS037

In partial fulfillment of the requirements for the degree of

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

Under the Guidance of

Ms. SAHANA SHETTY
ASSISTANT PROFFESOR

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOODBIDRI-574225, KARNATAKA

2016 – 2017

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

CERTIFICATE

*This is to certify that the Project entitled "**PRIVACY PRESERVING AND DATA ANALYSIS IN MEDICAL HEALTH RECORDS**" has been successfully completed by*

KAVYA K	**4AL13IS012**
KRUPA KC	**4AL13IS016**
UDYAVAR PRATEEKSHA JAYANTH	**4AL13IS035**
VISHRUTH	**4AL13IS037**

*the bonafide students of Department of Information Science & Engineering, Alva's Institute of Engineering and Technology in partial fulfillment for the award of BACHELOR OF ENGINEERING in **DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING** of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the year 2016–2017. 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.*

Ms. Sahana Shetty **Project Guide** **Assistant Professor**	**Mr. Jayanthkumar A. Rathod** **Associate Professor** **Head of the Department**	**Dr.Peter Fernandes** **Principal**

Dept. Of Information Science & Engineering
Alva's Institute of Engg. & Technology
Mijar, MOODBIDRI - 574 225

EXTERNAL VIVA

Name of the Examiners	**Signature with Date**
1.	
2.	

ABSTRACT

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

A novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, Attribute-based encryption (ABE) techniques are used to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, the focus is on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. The proposed scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of the proposed scheme.

Different organization to be considered equally in that case Distributed ABE needs to design the system. An authority can revoke a user or user's attributes immediately by re-encrypting the cipher texts and updating users' secret keys. The algorithm can be made more efficient and also the user interface can be improved on. As new user requirements emerge new ideas of implementation can be worked on. Though the software meets all minimum constraints, there still remains a scope for improvement.