DECLARATION

I, **M SREEKANTH (RegNo.38110326), KUNAPAREDDY PREM KUMAR JI (Reg No. 38110280)** hereby declare that the professional Training Report on **"ENHANCING THE DATA AND SECURITY IN HEALTH CARE SYSTEM"** done by me under the guidance of **MS.T.ANANDHI M.E.,(PH.D).,** at Sathyabama Institute of Science and technology is submitted in partial fulfillment of the requirements of the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: **SIGNATURE OF THE CANDIDATE**

ACKNOWLEDGEMENT

We are pleased to acknowledge our sincere thanks to Board of management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

We convey our thanks to **Dr. T. SASIKALA M.E., Ph.D., Dean of the Department, Department of Computer Science and Engineering** for providing us the necessary support and details at the right time during the progressive reviews.

We convey our thanks to **Dr. L. LAKSHMANAN., M.E., Ph.D., Head of the Department, Department of Computer Science and Engineering** for providing us the necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **MS.T.ANANDHI M.E.,(PH.D).,** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

We wish to express our thanks to all Teaching and Non-teaching staff members of the Department of **COMPUTER SCIENCE AND ENGINEERING** who were helpful in many ways for the completion of the project.

ABSTARCT:

- Your health care provider may be moving from paper records to electronic health records (EHRs) or may be using EHRs already.
- EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information.
- This project focuses on developing secure cloud framework for evolving and accessing trusted computing services in all levels of public cloud deployment model.
- Thus, eliminates both internal and external security threats.
- These results in achieving data confidentiality, data integrity, authentication and authorization, eliminating both active and passive attacks from cloud network environment.
- To develop a secure cloud framework for accessing trusted computing and storage services in all levels of public cloud deployment model.

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 OUTLINE OF THE PROJECT

With the explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Therefore, more and more organizations and individuals would like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud. In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed. In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications, such as Google Drive, Dropbox and iCloud. Data sharing as one of the most common features in cloud storage, allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information. For instance, the Electronic Health Records stored and shared in the cloud usually contain patients' sensitive information (patient's name, telephone number and ID number, etc.) and the hospital's sensitive information (hospital's name, etc.). If these EHRs are directly uploaded to the cloud to be shared for research purposes, the sensitive information of patient and hospital will be inevitably exposed to the cloud and the researchers. Besides, the integrity of the EHRs needs to be guaranteed due to the existence of human errors and software/hardware failures in the cloud. Therefore, it is important to accomplish remote data integrity auditing on the condition

that the sensitive information of shared data is protected. A potential method of solving this problem is to encrypt the whole shared file before sending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. This method can realize the sensitive information hiding since only the data owner can decrypt this file. However, it will make the whole shared file unable to be used by others. For example, encrypting the EHRs of infectious disease patients can protect the privacy of patient and hospital, but these encrypted EHRs cannot be effectively utilized by researchers any more. Distributing the decryption key to the researchers seems to be a possible solution to the above problem. However, it is infeasible to adopt this method in real scenarios due to the following reasons. Firstly, distributing decryption key needs secure channels, which is hard to be satisfied in some instances. Furthermore, it seems very difficult for a user to know which researchers will use his/her EHRs in the near future when he/she uploads the EHRs to the cloud. As a result, it is impractical to hide sensitive information by encrypting the whole shared file. Thus, how to realize data sharing with sensitive information hiding in remote data integrity auditing is very important and valuable. Unfortunately, this problem has remained unexplored in previous researches.

1.2 EXISTING SYSTEM

- Cloud computing security based on set of control-based technologies.
- Data level security for handling data in a secure manner.
- Platform level security for providing secure platform to process the data. Secure framework for proving trusted environment to the

user, but it lacks in high level security and different levels of security, less focus on insider threat, active and passive attacks.

DISADVANTAGES

- Data confidentiality is less.
- Authentication and authorization is less.

1.3 PROPOSED SYSTEM:

- Your health care provider may be moving from paper records to electronic health records (EHRs) or may be using EHRs already.
- EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information.
- This project focuses on developing secure cloud framework for evolving and accessing trusted computing services in all levels of public cloud deployment model.
- Thus, eliminates both internal and external security threats.
- These results in achieving data confidentiality, data integrity, authentication and authorization, eliminating both active and passive attacks from cloud network environment.
- To develop a secure cloud framework for accessing trusted computing and storage services in all levels of public cloud deployment model.

ADVANTAGES OF PROPOSED SYSTEM

- Provides data integrity
- Data confidentiality

CHAPTER-2

AIM AND SCOPE

2.1 AIM OF THE PROJECT

To develop a secure cloud framework for accessing trusted computing and storage services in all levels of public cloud deployment model.

2.2 SCOPE OF THE PROJECT

Achieves high level security to provide trustable computing and storage services. Provides data integrity, data confidentiality, authentication and authorization. Eliminates both internal and external security threats. Avoids both active and passive attacks in cloud network environment. Achieves different levels of security in cloud framework.

2.3 SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

System : Pentium Dual Core.

Hard Disk : 120 GB.

Monitor : 15”LED

Input Devices : Keyboard, Mouse

Ram : 1GB.

SOFTWARE REQUIREMENTS:

Operating system : Windows 7.

Coding Language : Java

Toolkit : Netbeans

DATABASE : MySQL