

**Visvesvaraya Technological University
Belgaum, Karnataka- 590014**



A Project Report On
**Secure sharing and storage of Personal Health
Records in Cloud and reading current health data
using Sensor Networks**

Submitted in the partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF ENGINEERING
in
INFORMATION SCIENCE AND ENGINEERING

Submitted by

Prachi Lakhota(1DS10IS070)
Sankalp Kak(1DS10IS080)

Saurav Mawandia(1DS10IS081)
Tanvee Singh(1DS10IS107)

Under the Guidance of
Mrs.Padmashree.T
Asst. Professor, Dept. of ISE



2013-2014

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING
DAYANANDA SAGAR COLLEGE OF ENGINEERING
SHAVIGE MALLESHWARA HILLS, KUMARASWAMY LAYOUT, BANGALORE-78

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Shavige Malleshwara Hills, Kumaraswamy Layout
Bangalore-560078

Department of Information Science and Engineering



2013-2014

Certificate

This is to certify that the Project Work entitled ” **Secure sharing and storage of Personal Health Records in Cloud and reading current health data using Sensor Networks**” is a bonafide work carried out by **Prachi Lakhotia** (1DS10IS071), **Sankalp kak** (1DS10IS080), **Saurav Mawandia** (1DS10IS081) and **Tanvee Singh** (1DS10IS107) in partial fulfillment for the 8th semester of Bachelor of Engineering in Information Science & Engineering of the Visvesvaraya Technological University, Belgaum during the year 2013-2014. The Project Report has been approved as it satisfies the academics prescribed for the Bachelor of Engineering degree.

Signature of Guide
[Mrs.Padmashree.T]

Signature of HOD
[Dr. M. Ravishankar]

Signature of Principal
[Dr. A. N. N Murthy]

Name of the Examiners

Signature with Date

1. _____

2. _____

ACKNOWLEDGEMENT

A successful project is a fruitful culmination of efforts by many people, some directly involved and some others who have quietly encouraged and extended support from the background.

We take this opportunity to express our sincere gratitude to **Dayananda Sagar College of Engineering** for having provided us with a great opportunity to pursue our Bachelor Degree in this institution.

In particular we would like to thank **Dr. A. N. N Murthy**, Principal, Dayananda Sagar College of Engineering for his constant encouragement and advice.

Special thanks to **Dr. M. Ravishankar**, HOD, Department of Information Science & Engineering, Dayananda Sagar College of Engineering for his motivation and invaluable support well through the development of this project.

We are highly indebted to our internal guide **Mrs. Padmashree T.**, Asst. Professor, Department of Information Science & Engineering, Dayananda Sagar College of Engineering for his constant support and guidance. He has been a great source of inspiration throughout the course of this project.

Finally, we gratefully acknowledge the support of our families during the completion of the project.

Prachi Lakhotia (1DS10IS071)

Saurav Mawandia (1DS10IS080)

Sankalp Kak (1DS10IS081)

Tanvee Singh (1DS10IS107)

ABSTRACT

Personal Health Records (PHRs) should remain the lifelong property of patients, who should be able to show them conveniently and securely to selected caregivers and institutions. We present a cloud-based PHR system taking a radically new architectural solution to health record portability. However, there have been wide privacy concerns as personal 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. Here, we use 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, we leverage the outsourcing decryption technique and a newly proposed key private proxy re-encryption to encrypt each patient's PHR file. This shifts the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design. We will also deploy portable sensors in wireless body sensor networks to collect various physiological data, such as body temperature, heart beat rate. Such physiological data could then be sent to a central server using an online portal, which could then run various web medical applications on these data to return timely advice to the client.

CONTENTS

• Chapter 1: Introduction.....	01
1.1 Motivation	
1.2 Objective of the work	
1.3 Problem Statement	
• Chapter 2: Literature Survey	05
• Chapter 3: System Analysis.	09
3.1 Existing System	
3.2 Proposed System	
3.3 Dynamic Programming for point Correspondence	
• Chapter 4: Requirement Specification.....	15
4.1 Hardware Requirements	
4.2 Software Requirements	
• Chapter 5: Implementation	18
5.1 Algorithms	
5.2 System Design	
• Chapter 6: Verification and Validation.....	28
6.1 Testing	
• Chapter 7: Snapshots.....	31
• Chapter 7: Conclusion and Future Enhancements.....	40
• References.	42

LIST OF FIGURES

• Figure :4.2.a Pictorial Representation of Proposed system.....	12
• Figure: 4.2.b Pictorial Representation of Hardware system.....	13
• Figure: 5.1.1.a Pictorial Representation of AES Algorithm.....	20
• Figure 7.a. Screenshot of the home page.....	32
• Figure 7.b. Screenshot of the PHR home page.....	32
• Figure 7.c. Screenshot of the Provider login.....	33
• Figure 7.d. Screenshot of the STA login.....	33
• Figure 7.e. Screenshot of the User login.....	34
• Figure 7.f. Screenshot of uploading the document.....	34
• Figure 7.g. Screenshot of user details.....	35
• Figure 7.h. Screenshot of User management.....	35
• Figure 7.i. Screenshot of STA generating the tokens.....	36
• Figure 7.j. Screenshot of list of token generated	36
• Figure 7.k. Screenshot of user home page	37
• Figure 7.l. Screenshot of Personal health record of a user.....	37
• Figure 7.m. Screenshot of token generated for different users.....	38
• Figure 7.n. Screenshot of different queries requested by a user.....	38