

PROJECT REPORT ON
SEQUORO: QR CODE BASED OPEN AUTHENTICATION

Submitted in partial fulfillment of the requirements for the award of the degree of
BACHELOR OF TECHNOLOGY

In
COMPUTER SCIENCE AND ENGINEERING
Of
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

By
ANJANA S
ASHLY CHACKO
JITHU R JACOB
RADHIKA P R



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
COLLEGE OF ENGINEERING POONJAR
POONJAR THEKKEKKARA
KOTTAYAM – 686582

MARCH 2015

cepoonjar@ihrd.ac.in

www.cep.ac.in

COLLEGE OF ENGINEERING POONJAR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CERTIFICATE



This is to certify that the project work entitled
“SEQUORO: QR CODE BASED OPEN AUTHENTICATION”

Submitted by
ANJANA S
ASHLY CHACKO
JITHU R JACOB
RADHIKA P R

*In partial fulfillment for the award of Bachelor of Technology in computer science and engineering from Cochin University of Science & Technology is a bona-fide record of the work done by them during the period of **DECEMBER 2014** to **MARCH 2015**.*

MANOJ S NAIR

Internal Project Guide

System Analyst

Dept. of Computer Science and Engg.

College of Engineering Poonjar

SREEKUMAR K

Project Coordinator

Assistant professor

Dept. of Computer Science and Engg.

College of Engineering Poonjar

ACKNOWLEDGEMENT

If the words are considered as symbols of Approval and Token of acknowledgment then let the words play the heralding of expressing my gratitude. First and Foremost, I praise the God Almighty for the grace he showered on us during our studies as well as our day to day life activities.

We would like to express our gratitude to our principal **Prof. SHINE P JAMES** for providing the facilities and constant encouragements in our achievement. We express our heartfelt thanks to **Mrs. SINDHU L** Head of the department of Computer Science and Engineering. We are also grateful to our tutor **Mr. RAJESH K R** and, project guide **Mr. MANOJ S NAIR**, project coordinator **Mr. SREEKUMAR K** who helped us to complete our project. We also sincerely thankful to the computer science faculty for providing us valuable help.

Heartfelt thanks to all members of the teaching faculty for their moral and academic support. Sincere thanks to all other staff of the Department of Computer Science for the priceless helps received and special thanks to Technical staff for assistance. Special thanks to all our teammates and pals for their support. Sincere thanks to all class mates. Above all, thanks to parents, without whose blessings, this would not have been accomplished.

ABSTRACT

The design of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. Therefore, relying on users to enhance security necessarily degrades the usability. On the other hand, relaxing assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm the users' trust. In this project, we demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. To that end, we propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol.

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Then, instead of the user directly invoking the regular authentication protocol, she invokes a more sophisticated but user-friendly protocol via the intermediate helping device. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing key-logging attacks.

TABLE OF CONTENTS

1. INTRODUCTION.....	01
2. PROBLEM DEFINITION/OBJECTIVES.....	03
3. SOFTWARE REQUIREMENT SPECIFICATION.....	04
3.1 INTRODUCTION.....	04
3.2 GENERAL DESCRIPTION.....	04
3.3 SPECIAL REQUIREMENTS.....	05
3.4 REQUIREMENTS.....	06
4. SYSTEM STUDY/LITERATURE.....	07
4.1 SURVEY OF LITERATURE/ EXISTING SYSTEM.....	07
4.2 PROPOSED SYSTEM.....	08
4.3 FEASIBILITY STUDY.....	09
5. SYSTEM DESIGN.....	10
5.1 MODULES.....	10
5.2 DATA FLOW DIAGRAMS.....	11
6. USE CASE DESIGN.....	16
7. DETAILED DESIGN.....	18
8. DATABASE DESIGN.....	22
9. SYSTEM IMPLEMENTATION.....	25
9.1 SYSTEM REQUIREMENTS.....	25
9.2 DEVELOPMENT ENVIRONMENT.....	25
9.3 FAMILIARISATION WITH TOOLS/TECHNIQUES/API'S	26
10 .SOURCE CODE.....	31
11. RESULTS AND FINDINGS.....	53
11.1 SCREEN SHOTS.....	53
12. CONCLUSION.....	60
13. REFERENCES.....	61

LIST OF FIGURES

1. DATA FLOW DIAGRAM LEVEL 0	11
2. DATA FLOW DIAGRAM LEVEL 1	11
3. DATA FLOW DIAGRAM LEVEL 2 FOR PROCESS 2.0.....	12
4. DATA FLOW DIAGRAM LEVEL 2 FOR PROCESS 3.0.....	12
5. DATA FLOW DIAGRAM LEVEL 2 FOR PROCESS 4.0.....	13
6. DATA FLOW DIAGRAM LEVEL 2 FOR PROCESS 5.0.....	13
7. DATA FLOW DIAGRAM LEVEL 3 FOR PROCESS 3.1.....	14
8. DATA FLOW DIAGRAM LEVEL 3 FOR PROCESS 3.2.....	14
9. DATA FLOW DIAGRAM LEVEL 3 FOR PROCESS 5.1.....	15
10. DATA FLOW DIAGRAM LEVEL 3 FOR PROCESS 5.2.....	15
11. USE CASE DIAGRAM.....	17
12. SEQUENCE DIAGRAM.....	21

LIST OF ABBREVIATIONS

QR code	: Quick Response Code
oAuth	: Open Authentication
TOTP	: Time Based One Time Password
API	: Application Program Interface
RSA	: Rivest Shamir Adleman
AES	: Advanced Encryption Standard
MAC	: Message Authentication Code
HMAC	: Hash based Message Authentication Code
SHA	: Secure Hash Algorithm
SMS	: Short Message Service
JSP	: Java Server Page
SQL	: Structured Query Language