** USER-AIDED ENCRYPTION**

**USING VIRTUAL PASSWORD**

**MECHANISM**

**A PROJECT REPORT**

***Submitted by***

**SUDHASREE.V (090606112055)**

**VAISHNAVI.G (090606112059)**

***in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION TECHNOLOGY**

**MAHARAJA ENGINEERING COLLEGE, AVINASHI**

**ANNA UNIVERSITY::CHENNAI 600 025**

**APRIL 2013**

**ANNA UNIVERSITY::CHENNAI 600 025**

**BONAFIDE CERTIFICATE**

Certified that this project report “**USER- AIDED ENCRYPTION USING VIRTUAL PASSWORD MECHANISM”** is the bonafide work of “**SUDHASREE.V, VAISHNAVI.G”** who carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Ms.S.UMA RANI M.E.,(Ph.D)., Ms.N.GEETHA B.Tech.,(M.E).,**

**HEAD OF THE DEPARTMENT SUPERVISOR LECTURER** Dept. of Information Technology, Dept. of InformationTechnology, Maharaja Engineering College, Maharaja Engineering College, Avinashi-641 654.Avinashi-641 654.

Submitted for the university VIVA-VOCE held on ­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**INTERNAL EXAMINER External Examiner**

**ACKNOWLEDGEMENT**

Our heartfelt thanks to **Thiru K.PARAMASIVAM B.Sc.,** Chairman, Maharaja Engineering College, Avinashi for having provided us with all necessary infrastructures and other facilities and our Correspondent **Thiru P.SATHIYAMOORTHY B.E., MBA., M.S.,** for his extensive support to successfully carry out this project.

We extend our sincere gratitude to honorable Principal, **Dr.N.KUPPUSWAMY M.E.,Ph.D.,F.I.E.,** Maharaja Engineering College, Avinashi for his high degree of encouragement and moral Support during the course of this project.

We are extremely happy for expressing our heartfelt gratitude to **Ms.S.UMA RANI M.E.,(Ph.D).,** Head of the Department of Information Technology, who has been the source of inspiration.

We also express our heart full thanks to our project guide **Ms.N.GEETHA B.Tech.,(M.E).,** for their valuable guidance and suggestions throughout the work.

**ABSTRACT**

People enjoy the convenience of on-line services but online environments may bring many risks. Let us discuss how to prevent users’ passwords from being stolen by the adversaries. We propose a virtual password concept involving a small amount of human computing to secure users’ passwords in on-line environment. We adopt user-determined randomized linear generation functions to secure users’ password based on the fact that a server has more information than any adversary does. We analyze how the proposed scheme defends against phishing, key logger and shoulder-surfing attacks. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks together.

**TABLE OF CONTENTS**

**CHAPTER TITLE PAGE**

**NO. NO.**

**LIST OF TABLES viii**

**LIST OF FIGURES ix**

**LIST OF ABBREVIATIONS x**

**1 INTRODUCTION 1**

1.1 OVERVIEW 1

1.2 OBJECTIVE 2

1. **LITERATURE REVIEW** **3**

2.1 GENERATING UNIQUE PASSWORD 3

2.2 SOURCE AUTHENTICATION SCHEME 4

2.3 SECURED BROWSING 4

2.4 LOGIN FROM INTERNET CAFÉ 5

2.5 SELF ENCRYPTION AUTHENTICATION 5

2.6 VIRTUAL PASSWORD FOR ATM 6

2.7 PIN-ENTRY METHOD 6

2.8 MULTICAST AUTHENTICATION 7

2.9 SHOULDER-SURFING RESISTANT 7

2.10 SECRET LITTLE FUNCTIONS 8

**3 SYSTEM ANALYSIS 9**

3.1 EXISTING SYSTEM 9

3.2 PROPOSED SYSTEM 10

**4 SYSTEM SPECIFICATION 12**  4.1 HARDWARE REQUIREMENTS 12

4.2 SOFTWARE REQUIREMENTS 12

**5 SOFTWARE DESCRIPTION 13**

5.1 PHP 13

5.2 HTML 14

5.3 DATABASE 14

5.4 MYSQL 15

**6 PROJECT DESCRIPTION 16**

6.1 OVERVIEW OF THE PROJECT 16

6.2 ENTITY RELATIONSHIP DIAGRAM 17

6.3 MODULE DESCRIPTION 18

6.3.1 User Registration 18

6.3.2 Login 19

6.3.3 Passport Application 19

6.3.4 Admin Login 20

6.3.5 View Registered User 20

6.3.6 Update Passport Status 21

6.3.7 View Passport Status 21

6.4 SYSTEM DESIGN 22

6.4.1Design Process 23

6.4.1.1 Input Design 23

6.4.1.2 Output Design 24

6.4.1.3 Code Design 25

6.4.1.4 Database Design 25

6.4.2 DFD 28

6.4.3 Codebook 28

6.4.4 Security Analysis for Secret Little Functions 29

6.4.5 Security Analysis for Codebook 30

6.4.6 Quantitative Analysis for Attacks 30

**7 SOFTWARE TESTING 32**

7.1 SYSTEM TESTING 32

7.2 TESTING & METHODOLOGIES 32

7.3 SECURITY TECHNOILOGIES & POLICIES 35

**8 SYSTEM IMPLEMENTATION 36**

8.1 IMPLEMENTATION36

8.2 IMPLEMENTATION PROCEDURE 36

8.3 OPERATIONAL DOCUMENTATION 36

8.4 MAINTENANCE 37

**CONCLUSION & FUTURE ENHANCEMENT 38**

**APPENDICES 39**

**REFERENCES 53**

**LIST OF TABLES**

**TABLE NO . TITLE PAGE NO.**

3.1 Difference between existing and proposed 11

6.1 Breaking Password by Phishing Attack 23

6.2 Attribute of the table “passport” 26

6.3 Attribute of the table “register” 27

**LIST OF FIGURES**

**FIGURE NO. TITLE PAGE NO.**

6.1 E-R Diagram for applying passport 17

6.2 DFD for user login 19

6.3 DFD for admin login 20

6.4 DFD for passport approval 21

6.5 Password Authentication 22

**LIST OF ABBREVIATIONS**

**ID** Identification

**HTTP** Hyper Text Transfer Protocol

**CHC** Convex Hull Click

**SSL** Secured Socket Layer

**TLS** Transport Layer Security

**PHP** Hypertext Preprocessor

**IIS** Internet Information System

**HTML** Hyper Text Markup Language

**SGML** Standard Generalized Markup Language

**WWW** World Wide Web

**TBL** Triple Bottom Line

**W3C** World Wide Web Consortium

**MIT** Massacheusetts Institute of Technology

**SQL** Structured Query Language

**VBA** Visual Basic for Applications

**DFD** Data Flow Diagram

**GUI** Graphical User Interface

**URL** Uniform Resource Locator

**PDA** Personal Digital Assistance