**3D-PASSWORD**

**Technical Seminar Report**

A Dissertation submitted in partial fulfillment of the requirement for the award of the Degree of

Bachelor of Technology

in

**Electronics and Communication Engineering**

By

K.RAJI KRISHNAN 07621A0418

Under the guidance of

Mr. SRIKANTH PRASAD



## Department of Electronics and Communication Engineering

## Aurora's Engineering College

**Bhuvanagiri, Nalgonda District – 508 116**

**(Affiliated to JNTUH and Accredited by NBA, New Delhi)**

**(April, 2011)**

## Aurora's Engineering College

**Bhuvanagiri, Nalgonda District – 508 116**

**(Affiliated to JNTUH and Accredited by NBA, New Delhi)**

**(April, 2011)**

****

**CERTIFICATE**

This is to certify that the Seminar report entitled 3D PASSWORD has been submitted by Ms.K.RAJI KRISHNAN bearing roll No 07621A0418 under my guidance in partial fulfillment of the degree of Bachelor of Technology in Electronics and Communication Engineering to the Jawaharlal Nehru Technological University Hyderabad during the academic year 2010-11.

Date:

**(Internal guide)**

**Mr. Srikanth Prasad**

**T. Sireesha Dr. U.M. Choudhari**

### Head of Department Principal

**ACKNOWLEDGEMENT**

Behind every achievement there lies an unfathomable sea of gratitude to those who activated it, without whom it would never ever come into existence. To them, lay the words of gratitude imprinted within.

I am firstly thankful to our Head of the Department **T.Sireesha**, for her indispansable suggestions and kind help throughout the project.

My deepest and sincere thanks go to my internal guide **Mr. Srikanth Prasad**, for his extensive guidance, encouragement, immense help and cooperation throughout.

We would like to express our sincere gratitude to our principal **Dr. Uday Chaudhari** for providing the opportunity to carry out the technical seminar.

K. RAJI KRISHNAN (07621A0418)

**ABSTRACT**

Usually the authentication scheme the user undergoes is particularly very lenient or very strict. With all the means of technology developing, it has become very easy for others to fabricate or to steal identity or to hack someone’s password. Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc .Mostly textual passwords follow an encryption algorithm. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas(Biometric scanning).Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names etc. Year’s back the tests were performed and people could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a child's play.

Therefore the idea of 3D passwords, are more customizable and very interesting way of authentication. Now the passwords are based on the fact of human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen for e.g. a garage. Now in a day to day garage one will find all sorts of tools, equipments, etc. each of them having unique properties. The user will then interact with these properties accordingly. Each object in the 3D space, can be moved around in an (x,y,z) plane. That’s the moving attribute of each object. This property is common to all the objects in the space. That can be identified as an authentication. Only the true user understands and recognizes the object which he has to choose among many. This is the Recall and Recognition part of human memory coming into play. There can be levels of authentication a user can undergo which can be implemented so as to enhance security.

**CONTENTS PAGE NO**

1. **INTRODUCTION**  1

1.1 Draw backs for preexisting password mechanisms

1.2 3D Password scheme

1.3 Password

1.4 Easy to remember, hard to guess 2

1.5 Factors in the security of a password system 3

1.6 Procedures for changing password 5

1.7 Password longevity 6

1.8 Number of users per password

1. **PRESENT TECHNOLOGY** 7
   1. Design of the protected software
   2. Password cracking 8
   3. Alternatives to passwords for authentication
   4. Graphical passwords 9
   5. Web site password systems
2. **3D PASSWORD TECHNOLOGY** 11
   1. Proposed system
   2. Expected functionalities
   3. Brief Description of system
   4. System implementation
   5. 3D password selections and inputs
   6. Virtual environment design guidelines
   7. State diagram of 3D password application
3. **SECURITY ANALYSIS**  19
4. **APPLICATIONS**  22
5. **CONCLUSION**  24
6. **REFERENCES**  25