A

Dissertation

On

Geometric Based Remote Login Password Authentication Using Smart Card

Submitted in Partial Fulfillment of Requirement

For the Award of the Degree of

Master of Technology

in

Computer Science and Engineering

by

Pooja Mithoo

University Roll No. 2K13/CSE/15

Under Esteemed Guidance of

Vinod Kumar

Associate Professor, Computer Engineering Department, DTU

2013-2015

Delhi Technological University

Delhi-110042, India

ABSTRACT

Authentication of remote user and server is a great research challenge in today's advanced wire and wireless communication. Engineers have proposed many password authentication schemes for remote login systems in past decades. In recent years, the biometrics technology has become a new issue in computer science. This new technology has allowed us to develop a novel method of user authentication using a smart card.

In 2005, Ku et al. proposed an improved version of Password authentication scheme without using password table based on Geometric property of Euclidean plane, Which stands on better resistance to the offline password guessing attack and easily reparable. But unfortunately, their scheme is more difficult by user point of view and vulnerable by an wangle the legal user smart card and known password and PIN. Again In 2010 Li and Hwang proposed a remote user authentication scheme based on biometric verification but above scheme does not provide proper authentication and cannot resist man-in-the middle attack, In this paper we integrated passwords (what the user know), smart card (what the user has) and biometric(what the user are), and then construct a secure three factor authentication scheme that can be solved the above problems. Here we present a geometric based authentication scheme using smart card with having finger print, in this scheme the user needs to be enter only password and impression of finger print which provides better resistance in all aspect easily reparable and it can resist man-in the middle attack. .

In this project, we proposed a Biometrical Geometric Based password authentication scheme using smart card. Which is better resistance in all aspect and easily reparable too.

Keywords- Cryptocraphy, Attacks, Biometrical, Password authentication, Smart card.

ACKNOWLEDGMENT

I would like to express my deep sense of respect and gratitude to my project supervisor Mr. Vinod Kumar for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

I am grateful to Prof. O.P.Verma, HOD, Computer Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Pooja Mithoo
Roll No. 2K13/CSE/15
M.Tech (Computer Science & Engineering)
Department of Computer Engineering
Delhi Technological University
Delhi-110042

CERTIFICATE

This is to certify that the project report entitled **"Geometric Based Remote Login Password Authentication Using Smart Card"** is a bonafide record of work carried out by **Pooja Mithoo (2K13/CSE/15)** under my guidance and supervision, during the academic session 2013-2015 in partial fulfillment of the requirement for the degree of Master of Technology in Computer Science & Engineering from Delhi Technological University, Delhi.

Vinod Kumar
Associate professor
(Project Guide)
Department of Computer Engineering
Delhi Technological University
Delhi-110042

Table of Contents

List of Figures

List of Abbreviations

U_i :	The user.
Id_i :	The identity of user.
Pw_i :	Password of the user.
B_i :	Extracted template of biometric.
RS:	Remote server.
CA:	Central Authority.
V_i:	Verification Identity.
E_i:	Secret Number for Authentication.
ru:	One time usable random value chosen by Ui.
rs:	One time useable random value chosen by RS.
f:	One way hash function.
P:	A large prime number.
‖:	Bitwise OR symbol.
$\oplus$:	xor operation.