CERTIFICATE

DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI – 110042

Date:_____

This is to certify that dissertation entitled "**A Remote Authentication Methodology for Secure Communication in Distributed Network**" has been completed by **Himanshu Mittal, University Roll No. 06/SWE/2010** in partial fulfillment of the requirement for the award of **Master of Technology** in **Software Engineering** at **Delhi Technological University, Delhi**.

This thesis is a record of his own work carried out by him under my supervision and support during the academic session 2011-2012. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

(Dr. DAYA GUPTA)
HOD & PROJECT GUIDE
DEPT. OF COMPUTER ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI – 110042

ACKNOWLEDGEMENT

It is a great pleasure to have the opportunity to extend my heartiest felt gratitude to everybody who helped me throughout the course of this project.

It is distinct pleasure to express my deep sense of gratitude and indebtedness to my project guide **Dr. Daya Gupta, Professor, Head of Department, Department of Computer Engineering, Delhi Technological University,** for her invaluable guidance, encouragement and patient reviews. With her continuous inspiration only, it becomes possible to complete the project.

I would also like to take the opportunity to present my sincere regards to **Mrs. KAKALI CHATTERJEE, Research Scholar, Department of Computer Engineering, Delhi Technological University,** for their technical support and encouragement throughout the program.

I would also like present my sincere regards to all the faculty members of the Department for their constant support and encouragement.

I am grateful to my parents for their moral support all the time. They have been always around to support me in all the way. I am also thankful to my classmates for their unconditional support and motivation during this work.

HIMANSHU MITTAL
M.Tech (Software Engineering)
Roll No. 06/S.W.E./2010
Department of Computer Engineering
Delhi Technical University, Delhi
(Formerly Delhi College of Engineering)

ABSTRACT

With the fast development of network technologies, increasing number of services are provided through internet instead of traditional ways. Owing to the openness of the internet, method of guarding valuable resources from unauthorized access is as essential the data/services itself.

To facilitate a legal user, to access a distant server in distributed environment for utilizing various information resources and services available on the multi-server network, we propose "A Remote Authentication Methodology for Secure Communication in Distributed Network".

This scheme is based on one-way hash function, XOR function and Diffie-Hellman. It provide more security, reduce the computational and communication cost and is less complex. It uses an authentication center, that consists of multiple servers registered on it and allow the remote users to securely and efficiently get authenticated and generate session key with the desired server. The User registers only once with the authentication center and can obtain the services from multiple servers without repeating registration process on every individual server.

The proposed scheme has many advantages such as no encryption, signature, verification tables, timestamps and public keys directory are needed to be maintained. Also the proposed scheme is invulnerable to the security attacks such as insider attack, man-in-the-middle attack, forward security, impersonation attack, replay attack and safe guard from many possible attacks effectively.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES