MAJOR PROJECT

on

An Efficient Intrusion Detection System

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE AWARD OF DEGREE

Of

MASTER OF ENGINEERING

(Computer Technology and Applications)

Delhi University, Delhi

Submitted by:

VIJAY KUMAR

University Roll No 8556

17/ME/CTA/2K9

Under the Guidance of:

Mr. Manoj Kumar

Asstt. Professor

Department of Computer Engineering

Delhi College of Engineering, Delhi

DEPARTMENT OF COMPUTER ENGINEERING

DELHI COLLEGE OF ENGINEERING

BAWANA ROAD, DELHI-110042

DELHI UNIVERSITY

2011

CERTIFICATE

This is to certify that **Mr. Vijay Kumar (17/ME/CTA/2K9, 8556)** has carried out the major project titled "**An Efficient Intrusion Detection Approach**" as a partial requirement for the award of Master of Engineering degree in Computer Technology and Application by Delhi University.

The major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session **2009-2011**.

The matter contained in this report has not been submitted elsewhere for the award of any other degree.

(Project Supervisor)
Mr.Manoj Kumar
Asstt. Professor
Department of Computer Engineering
Delhi College of Engineering
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I express my gratitude to my major project guide Mr. Manoj Kumar, Asstt. Professor, Computer Science and Engineering, Delhi College of Engineering, for the valuable support and guidance he provided in making this project. It is my pleasure to record my sincere thanks to my respected guide for his constructive criticism and insight without which the project would not have shaped as it has.

I humbly extend my words of gratitude to other faculty members of this department for providing their valuable help and time whenever it was required.

Last but not the least; I thank my family members who have motivated me to complete the work.

VIJAY KUMAR
17/ME/CTA/2K9
M.E.(CTA)
Department of Computer Engineering
E-mail: vijaykumar_nrw@hotmail.com

ABSTRACT

Network security has become a critical issue due to increase of traffic on the internet. Traffic on the internet has also increased the attack types. Intrusion detection has become one of the major tasks. It faces a number of challenges; an intrusion detection system must reliably detect malicious activities in a network and must perform efficiently to cope with the large amount of network traffic. In this thesis we are trying to analyze various techniques for intrusion detection on the bases of efficiency, accuracy and robustness.

It has been seen that various anomaly based approaches face the problem of a large number of false alarms which may cause the network administrator to ignore them completely. We have implemented two of the latest hybrid approaches Layered approach using conditional random fields and Fuzzy clustering with artificial neural networks (FCANN). We observed that FCANN provide better results.

LIST OF FIGURES

LIST OF TABLES