NAIF ARAB UNIVERSITY FOR SECURITY SCIENCE
COLLEGE OF COMPUTER INFORMATION SECURITY
DEPARTMENT

USING ENSEMBLE MACHINE LEARNING FOR INTRUSION DETECTION USING MULTIPLE MODELS WITH SAME ADAPTIVE AI CLASSIFICATION ALGORITHMS ON WEKA

BY:

MUTEB AL-YOUSEF

A THESIS

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF:

MASTER OF SCIENCE IN INFORMATION SECURITY

TO:

INFORMATION SECURITY DEPARTMENT

THE COLLEGE OF COMPUTER AND INFORMATION SECURITY

NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES

MAR 2018

SUPERVISED BY:

DR. NABIH T.ARAR

NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES

Table of Contents

List of Figures

List of Tables

List of Acronyms

Abbreviations	Explanations
BIDS	Behavior-Based Intrusion Detection System.
CDB	Complementary Database.
DDOS	Distributed Denial of Service.
DOS	Denial of Service.
FP	False Positive.
FSDB	Frequent Signatures Database.
HIDS	Host-Based Intrusion Detection System.
ICMP	Internet Control Message Protocol.
IDS	Intrusion Detection System.
IPS	Intrusion Prevention System.
NIDS	Network-Based Intrusion Detection System.
SIDS	Signature-Based Intrusion Detection System.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.