NETWORK INTRUSION DETECTION MODEL USING ENSEMBLE-BASED LEARNING

ONIETAN, IYANU-OLUWA CHRISTOPHER
(20PCG02292)
BSc. Computer Science, Samuel Adegboyega University, Ogwa

AUGUST, 2023

NETWORK INTRUSION DETECTION MODEL USING ENSEMBLE-BASED LEARNING

BY

ONIETAN, IYANU-OLUWA CHRISTOPHER
(20PCG02292)
BSc. Computer Science, Samuel Adegboyega University, Ogwa

A DISSERTATION PRESENTED TO THE SCHOOL OF POSTGRADUATE STUDIES AS A PARTIAL FULFILLMENT OF THE PREREQUISITES FOR OBTAINING A MASTER OF SCIENCE (M.SC) DEGREE IN THE DEPARTMENT OF COMPUTER SCIENCE WITHIN THE COLLEGE OF SCIENCE AND TECHNOLOGY AT COVENANT UNIVERSITY, OTA, OGUN STATE, NIGERIA

AUGUST, 2023.

ACCEPTANCE

This is to confirm that this dissertation is deemed worthy for the purpose of meeting partial requirements towards the attainment of the Master of Sciences in Computer Science degree from the Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Nigeria.

Miss Adefunke F. Oyinloye
(Secretary, School of Postgraduate Studies) **Signature and Date**

Prof. Akan B. Williams
(Dean, School of Postgraduate Studies) **Signature and Date**

DECLARATION

I, **ONIETAN IYANU-OLUWA CHRISTOPHER** (20PCG02292), assert that I conducted this project at Covenant University in Ota, Ogun State, Nigeria, under the guidance of Dr. Jonathan Oluranti from the Department of Computer and Information Sciences in the College of Science and Technology. I confirm that this research has not been previously submitted, either wholly or in part, for any other academic degree. This dissertation appropriately acknowledges all sources of data and scholarly information.

ONIETAN, IYANU-OLUWA CHRISTOPHER

Signature and Date

CERTIFICATION

We certify that this dissertation titled **"NETWORK INTRUSION DETECTION MODEL USING ENSEMBLE-BASED LEARNING "** is an original research carried out by **ONIETAN, IYANU-OLUWA CHRISTOPHER (20PCG02292)** in the Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria under the supervision of Dr. Oluranti Jonathan. We have examined and found this work acceptable as part of the requirements for the award of Master of Science (M.Sc.) in Computer Science.

Dr. Oluranti Jonathan
(Supervisor) **Signature and Date**

Prof. Olufunke O. Oladipupo
(Head of Department) **Signature and Date**

Prof. Adio T. Akinwale
(External Examiner) **Signature and Date**

Prof. Akan B. Williams
(Dean, School of Postgraduate Studies) **Signature and Date**

DEDICATION

With deep gratitude, I dedicate this project to You. Your guidance has been my constant light. May this work reflect my faith and gratitude. Thank you for your presence in my life. To my family, friends, mentors, and the countless individuals who have contributed to my journey, I dedicate this project. Your unwavering support and guidance have been invaluable, and this work is a reflection of our collective efforts. Thank you for being a constant source of inspiration and encouragement.

ACKNOWLEDGEMENTS

I want to express my gratitude to everyone who helped me out and gave me advice when I was working on this thesis. All the support, advice, and ideas they offered were priceless.

I would want to start by expressing my deepest gratitude to Dr. Oluranti Jonathan, my supervisor, for all of the help, advice, and encouragement they have given me. His perceptive criticism and guidance were crucial in determining the course of this study.

I appreciate my family's undying support and affection so much. Their tolerance, faith, and confidence in me encouraged me to push past obstacles and complete the task at hand.

I would like to thank everyone in my community who has helped me grow via shared experiences, conversations, and friendship. Their unique insights deepened my comprehension of the material and made the trip more fun.

I would like to express my gratitude to everyone who helps make the Computer and Information Sciences department such a great place to study and conduct research. All of the offered tools, space, and chances have been crucial to the accomplishment of this mission.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIDS	Anomaly-based IDS
ANFIS	Adaptive Network-based Fuzzy Inference System
AUC	Area Under the Curve
CIA	Confidentiality, Integrity, and Availability
CIC-IDS2017	Canadian Institute for Cybersecurity Intrusion Detection Systems 2017
CSV	Comma-Separated Value
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial-of-Service
DoS	Denial of Service
DT	Decision Tree
EDA	Exploratory Data Analysis
ET	Extra Tree
FP	False Positive
FN	False Negative
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection Systems
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID2T	Intrusion Detection Dataset Toolkit
IDS	Intrusion Detection Systems
IETF RFC	Internet Engineering Task Force Request for Comments
IMAP	Internet Message Access Protocol
IoT	Internet of Things

IPS	Intrusion Prevention System
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
JSON	JavaScript Object Notation
KDD	Knowledge Discovery in Databases
kNN	K-Nearest Neighbour
LSTM	Long Short-Term Memory
ML	Machine Learning
MANETs	Mobile Ad Hoc Networks
NGIPS	Next-Generation IPS
NMAP	Network Mapper
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NSL-KDD	Network Security Laboratory Knowledge Discovery in Databases
PCAP	Packet Capture
POD	Ping of Death
POP3	Post Office Protocol version 3
PPP	Point-to-Point Protocol
QoS	Quality of Service
TN	True Negative
ToS	Type of Service
TP	True Positive
TCP	Transmission Control Protocol
TTL	Time to Live
SMOTE	Synthetic Minority Oversampling Technique

SMUTE	Synthetic Majority Undersampling Technique
SNMP	Simple Network Management Protocol
SSH	Secure Shell
UDP	User Datagram Protocol
SVM	Support Vector Machine
WASC	Web Application Security Consortium
WSN	Wireless Service Networks

ABSTRACT

The interconnectedness of devices, technologies, networks and the services they provide has continued to increase. This has also resulted in increased cases of cyber threats and intrusions. detection has become a major concern for organizations. Intrusion detection system is one way to address the issue of intrusions and anomaly network traffic. Existing machine learning algorithms has performed well on intrusion detection however, the issues of high false positive rates as well as low accuracy still persists. This is largely due to fact that individual models are not able to efficiently detect previously unknown intrusions on their own. Other the hand, ensemble models have proven to be more efficient in identifying intrusions and anomalies in networks since they combine the predictive powers of several base models. However, the efficiency of ensemble models has not been sufficiently considered where imbalanced datasets are involved. This study therefore proposes and investigates the performance of various ensemble models when applied to conspicuously imbalanced datasets. Two largely imbalanced datasets were acquired namely IDT2 and CICIDS2017. Additional datasets were generated from each of the acquired datasets using SMOTE and SMUTE, oversampling and under-sampling techniques respectively. In order to investigate the performance of ensemble models, three ensemble models were constructed namely Bagging, Majority voting and Stacking. The performance of each model was effectively determined and compared.

Keywords: Network; Intrusion Detection Systems, Intrusion Prevention Systems, Machine Learning; Cybersecurity; Ensemble Models.