ANOMALY DETECTION IN WINDOWS OPERATING SYSTEM THROUGH MACHINE LEARNING

B.A.T.L Wijayawickrema

(209396P)

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2023

ANOMALY DETECTION IN WINDOWS OPERATING SYSTEM THROUGH MACHINE LEARNING

B.A.T.L Wijayawickrema

(209396P)

Thesis submitted in partial fulfilment of the requirements for the degree Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

April 2023

DECLARATION

I declare that this is my own work, and this report does not incorporate without acknowledgement any material previously submitted for the degree or diploma in any other university or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles of books).

Signature: Date: 21-April-2023

Name of the Student: B.A.T.L Wijayawickrema

I certify that the above candidate has carried out research for the Master's thesis under my supervision.

Signature: Date: 21-April-2023

Name of the Supervisor: Dr. Kutila Gunasekara

ABSTRACT

One of the main challenges of the new computer world is dealing with anomalies. This nature came to the computer without knowing it. Log files are crucial for detecting and mitigating anomalies in computer systems. Traditional human inspection approaches and rule-based systems become inadequate for log-based anomaly identification as the number and complexity of logs created by contemporary software systems rise. Machine learning approaches have emerged as interesting options for detecting anomalies in log files to overcome this obstacle. This study focuses on the creation of an anomaly detection mechanism for Windows operating system using machine learning. Our methodology offers significant advantages over existing rule-based methods for Windows operating system log analysis by integrating machine learning techniques. It provides a proactive defence against cyber-attacks and enables early identification and reaction to security risks. In addition, our methodology permits the discovery of previously unknown or undetected dangers, so enhancing the overall security posture of computer systems. Our effort contributes to the field of anomaly identification in Windows operating system and emphasizes the significance of log analysis for detecting and mitigating security threats.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ML	Machine Learning
NLP	Natural Language Processing
ANN	Artificial Neural Network
CNN	Convolutional Neural Network
RAD	Registry Anomaly Detection
PAD	Probabilistic Anomaly Detection
OCSVM	One Class Support Vector Machine
SOC	Security Operations Centre
PCA	Principal Component Analysis
GPU	Graphics Processing Unit
SRE	Site Reliability Engineer