HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

GRADUATION THESIS

Malware Detection System Using Machine Learning

Tran Ngoc Dung
dung.tn194742@sis.hust.edu.vn

Major: Global ICT
Specialization: Information Technology

Supervisor: Associate Professor Nguyen Linh Giang _____

Signature

Department: Computer Engineering

School: Information and Communications Technology

HANOI, 06/2024

ACKNOWLEDGMENTS

This Graduation Thesis would not be completed without the enthusiastic advice and support from my supervisor - Associate Professor Nguyen Linh Giang. I would like to express my gratitude to him and wish him gain more success in researching and supporting students, as well as success in life.

During 5 years of studying at Hanoi University of Science and Technology, I would like to sincerely thank the professors with knowledge and enthusiasm who have been teaching and helping to shape my knowledge.

Finally, I would also dedicate all my sincerity to thank my grandparents, my parents, my big family and all of my friends for supporting me on this way.

ABSTRACT

Recently, network security is becoming more integrated, so detecting and addressing network attacks become a huge issue. One of the hot topics in cyber security now is Malicious software or Malware which is any program or file that's intentionally harmful to a computer, network or server.
Early detecting malware attacks help network administrator to find appropriate solution to tackle problem, and minimize the impact of the attacks.
The development of Machine learning these days help computers to do the complicated work as detection or classification problems.
In this thesis, I consider the problem of malware detection and classification based on image analysis. I will convert executable files into images and apply image recognition using Machine learning and deep learning model.

Tran Ngoc Dung

(Signature and full name)

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION 1

1.1 Motivation 1

1.2 Objectives and scope of the graduation thesis 1

1.3 Tentative solution 1

1.4 Thesis organization 2

CHAPTER 2. SURVEY AND ANALYSIS 3

2.1 Status survey 3

2.2 Malware attack 3

2.2.1 Definition of Malware 3

2.2.2 Types of Malware 3

2.3 Learning Techniques 5

2.3.1 Multiplayer Perceptron 5

2.3.2 Convolutional Neural Network 6

2.3.3 Recurrent Neural Network 6

2.3.4 Long Short-term Memory 7

2.3.5 Gated Recurrent Unit 7

2.4 Transfer learning 7

2.4.1 ResNet152 7

2.4.2 VGG-19 8

CHAPTER 3. EXPERIMENTS 9

3.1 Dataset 9

3.2 Software 10

3.3 Data Preprocessing 11

3.4 Deep Learning Experiments 13
3.4.1 Multilayer Perceptron Experiments 13
3.4.2 Convolutional Neural Network Experiments 14
3.4.3 Recurrent Neural Networks Experiments 16
3.4.4 Transfer Learning 17
CHAPTER 4. RESULTS AND DISCUSSION 19
4.1 Results and discussion 19
4.1.1 KNN experiments 19
4.1.2 Random Forest experiments 21
4.1.3 XGB experiments 22
4.1.4 RNN experiments 24
4.2 Discussion 26
CHAPTER 5. CONCLUSION AND FUTURE WORK 29
5.1 Conclusion 29
5.1.1 Knowledge gained during working process 29
5.2 Future work 29

LIST OF FIGURES

Figure 3.1 Converting binaries to images 12
Figure 3.2 Unrelated binaries as images 12
Figure 3.3 Malware family images 13
Figure 3.4 Summary hyperparameters of CNNs experiments 14
Figure 3.5 Summary hyperparameters of RNNs experiments 16

Figure 4.1 Confusion matrix of KNN experiment 20
Figure 4.2 Normalized Confusion matrix of KNN experiment 21
Figure 4.3 Confusion matrix of Random Forest experiment 22
Figure 4.4 Normalized Confusion matrix of Random Forest experiment 23
Figure 4.5 Confusion matrix of XGB experiment 24
Figure 4.6 Normalized Confusion matrix of XGB experiment 25
Figure 4.7 Confusion matrix of RNN experiment 26
Figure 4.8 Normalized Confusion matrix of RNN experiment 27
Figure 4.9 Model loss of RNN 27
Figure 4.10 Model loss of RNN 28

LIST OF TABLES

Bảng 3.1 Type of each malware family. 9
Bảng 3.2 Samples per malware family. 11

LIST OF ABBREVIATIONS

Abriviation	Full Expression
CNN	Convolutional Neural Networks
DL	Deep Learning
GRU	Gated Recurrent Units
LSTM	Long Short-term Memory
Malware	Malicious Software
ML	Machine Learning
MLP	Multilayer Perceptrons

CHAPTER 1. INTRODUCTION

1.1 Motivation

These days, the infinity development of Internet makes not only the vast of positive effects but also brings a large number of problems. The big problem of using network now is cyber attacks including DoS and DDoS attacks, Malware, Phishing attacks, Man-in-the-Middle attacks, Password attacks, etc.

Malware (or Malicious Software) is any programs or files that intentionally harmful to a computer, network or server. Malware can infect networks and devices and is designed to harm those devices, networks and their users in some way depending on type of malware and its goal.

There have been many detect system for others attacks but not much for malware. As there are more types of malware appears, I personally think that it is necessary to improve the existing model to detect as many types of malware as possible. That the reason why I do this thesis.

1.2 Objectives and scope of the graduation thesis

Traditionally, malware detection and classification has relied on pattern matching against signatures extracted from specific malware samples. While simple and efficient, signature scanning is easily defeated by a number of well-known evasive strategies. This fact has given rise to statistical and machine learning based techniques, which are more robust to code modification.

Malware is not very a complicated attacks but it leads to a vast of risky problems. Detecting malware soon in the cybersecurity is crucial and help decrease the negative impact.

I would like to train a model using Machine Learning and Deep Learning techniques to detect and classsify malware attacks with a dataset cover as many types of malware as possible.

1.3 Tentative solution

In this thesis, my goal is to compare Deep Learning for malware detection and classification. I will apply DL models using image-based features, and also opcode features. The DL models consider include a wide variety of neural networking techniques, including multilayer perceptrons (MLP), several variants of convolutional neural networks (CNN), and vanilla recurrent neural networks (RNN), as well as the advanced RNN architectures known as long short-term memory (LSTM) and gated recurrent units (GRU).

I would like to use Python with skicit-learn and torch library for some reasons below:

- Scikit-learn provides a user-friendly interface with a consistent API, making it accessible for beginners and easy to implement various machine learning
- Scikit-learn is highly compatible with other Python libraries like NumPy and Pandas, facilitating seamless data manipulation and analysis
- PyTorch excels in building and training deep learning models, such as convolutional neural networks (CNNs), which are highly effective for image-based tasks
- PyTorch uses dynamic computation graphs, allowing for more flexibility and ease in building complex models and custom architectures
- Pytorch is suited for deep learning tasks, providing flexibility, powerful deep learning capabilities, and efficient training with GPU support

In this work, I have built some modules including:

- Module to convert binary file to image
- Module to extract features
- Module to extract opcode from image
- Module use ML and DL algorithms
- Module log to log write and save history

1.4 Thesis organization

The remaining of Thesis report will be organized as below.

Section 2: I would like to represent about Theoretical basis about classification techniques such as the definition of cyber attacks especially malware, definition of techniques used in this thesis, and information about library used.

Section 3 is about how I build Model to detect and classify malware using above techniques and dataset. Furthermore, I would like to show some codes and explain them

In Section 4, Result of model trained will be showed and evaluated by some criterions. I will also want to show my future work with this system to improve and widen it.