Thesis Title

By

Your Name

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science
at the University of Windsor

Windsor, Ontario, Canada

2020

Thesis Title

by

Your Name

APPROVED BY:

____

Initial. last Name
Department of Electrical and Computer Engineering

____

Initial. Last Name
School of Computer Science

____

Initial. Last Name, Advisor
School of Computer Science

March 17, 2019

DECLARATION OF CO-AUTHORSHIP AND PREVIOUS PUBLICATION

I. Co-Authorship

I hereby declare that this thesis incorporates material that is the result of joint research, as follows:

I am aware of the University of Windsor Senate Policy on Authorship and I certify that I have properly acknowledged the contribution of other researchers to my thesis, and have obtained written permission from each of the co-author(s) to include the above material(s) in my thesis.

I certify that, with the above qualification, this thesis, and the research to which it refers, is the product of my own work.

II. Previous Publication

This thesis includes 3 original papers that have been previously published/submitted for publication in peer reviewed journals, as follows: TO EDIT PLEASE SEE **vlsithesis.cls**

Thesis Chapter	Publication title/full citation	Publication Status
Chapter 2		
Chapter 3		
Chapter 4		

I certify that I have obtained a written permission from the copyright owner(s) to include the above published material(s) in my thesis. I certify that the above material describes work completed during my registration as a graduate student at the University of Windsor

III. General

I declare that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Your Thesis Abstract

ACKNOWLEDGEMENTS

Here I would like to acknowledge the invaluable mentorship of my supervisor ...

TABLE OF CONTENTS

DECLARATION OF CO-AUTHORSHIP AND PREVIOUS PUBLICATION **iii**

ABSTRACT **v**

ACKNOWLEDGEMENTS **vi**

LIST OF TABLES **viii**

LIST OF FIGURES **ix**

1 Introduction **1**

1.1 Machine Learning Algorithms 1

References 1

2 The Curious Case of Machine Learning in Malware Detection **3**

2.1 Introduction 3

References 3

3 JSLess: A Tale of Fileless JavaScript Memory-Resident Malware **4**

References 4

4 Interpreting Machine Learning Malware Detectors Which Leverage N-gram Analysis **5**

References 5

5 Interpreting Machine Learning Malware Detectors Which Leverage Convolutional Neural **6**

References 6

6 Robustness Metric **7**

References 7

7 Conclusion **8**

VITA AUCTORIS **9**

LIST OF TABLES

LIST OF FIGURES

1.1.1 Neural Network with 6 nodes in the input layer, 6 in the hidden layer, and 3 in the output layer 2

CHAPTER 1

Introduction

Machine Learning has come a long way in recent years. There has been a vast amount of papers published in the last decade which offer a number of substantial improvements on machine learning algorithms both old and new. Along side this research there has also been many papers which study the various applications of machine learning algorithms. From perhaps the most well known, even among non-experts, such as machine vision and natural language processing, to the less well known but all the while pervasive and significant medical, commercial, and industrial applications.

1.1 Machine Learning Algorithms

Here is an example for citation that will show at the end of the chapter [1] and this is a second example [2]

Here is a figure example

References

[1] T. Hastie, R. Tibshirani, and J. Friedman. *The elements of statistical learning: data mining, inference and prediction.* 2nd ed. Springer, 2009. URL: `http://www-stat.stanford.edu/~tibs/ElemStatLearn/`.

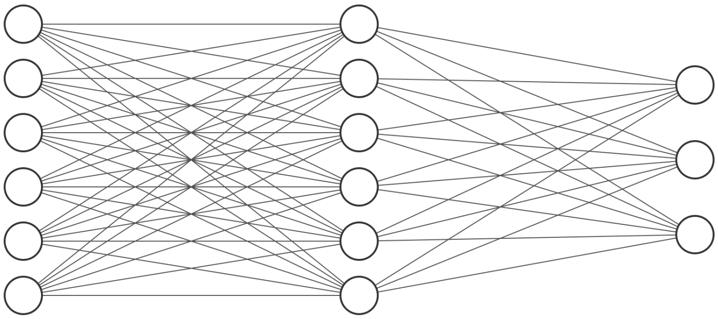

Fig. 1.1.1: Neural Network with 6 nodes in the input layer, 6 in the hidden layer, and 3 in the output layer

[2] S. Ruder. “An overview of gradient descent optimization algorithms”. In: *CoRR* abs/1609.04747 (2016). arXiv: 1609.04747. URL: http://arxiv.org/abs/1609.04747.

CHAPTER 2

The Curious Case of Machine Learning in Malware Detection

Paper 1st Author, 2nd Author, and 3rd Author

In Proceedings of the 5th International Conference on Information Systems Security and Privacy

2.1 Introduction

CHAPTER 3

JSLess: A Tale of Fileless JavaScript Memory-Resident Malware

Paper 1st Author, 2nd Author, and 3rd Author

In Proceedings of the 15th International Conference on Information Security Practice and Experience

CHAPTER 4

Interpreting Machine Learning Malware Detectors Which Leverage N-gram Analysis

Paper 1st Author, 2nd Author, and 3rd Author

In Proceedings of the 12th International Symposium on Foundations and Practice of Security

CHAPTER 5

Interpreting Machine Learning Malware Detectors Which Leverage Convolutional Neural

CHAPTER 6

Robustness Metric

CHAPTER 7

Conclusion

The work presented in this thesis provided a exploratory overview of machine learning interpretability in the malware detection domain.

VITA AUCTORIS

NAME:	Your Name
PLACE OF BIRTH:	Windsor, ON
YEAR OF BIRTH:	2000
EDUCATION:	
	University of Windsor, B.Sc in Computer Science, Windsor, Ontario, 2019
	University of Windsor, M.Sc in Computer Science, Windsor, Ontario, 2020