Technische Universität München

PhD Thesis Proposal

Artificial Intelligence in Cyber Security of Cloud Based Systems: Detection, Repair and Defense

by

Aytac Ozkan

Supervisor:
Co-Supervisor:

August, 2019

Abstract

The speed of process and the amount of data to be used in defending the cyber space cannot be handled by humans without considerable automation at the cloud base systems. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending against the dynamically evolving attacks in networks. This situation can be handled by applying methods of artificial intelligence that provide flexibility and learning capability to software.

Computer Security system providers are unable to provide timely security update. Most security systems are not designed to be adaptive to the increasing number of new threats. Companies lose considerable amount of time and resources when security attacks manifest themselves.

As a answer to these problems this research is aimed at developing security systems capable of learning and updating themselves.

The goal is to create security systems that will autonomously mature with expose to threats over time. To achieve this goal this research is proposing artificial intelligence based security systems with learning capability to perform intrusion, detection, repair and agnostics and defending network.

Contents

Chapter 1

Introduction

1.1 AI: The next Frontier in IT Security

AI in cybersecurity is a set of capabilities that allows organizations to detect, predict and respond to cyber threats in real-time using machine and deep learning.

AI-enabled cybersecurity is increasingly necessary, organizations face an urgent need to continually ramp up and improve their cybersecurity.

This is because the number of end user devices, networks and user interfaces continues to grow as a result of advances in cloud, the IoT,5G and conversational interfaces.

The increases the difficulty involved with administering a computer network. Having artificially intelligent network infrastructure that can learn to detect, report and repair network security problems is an advantage to network administrators.

Adaptability is another key reason that brought AI and computer security close to each other. The malicious entities that generate computer security attacks have gained intelligence. The type of attacks evolved from a simple password guessing to a staged and distributed network attack that can be equipped with a stealth mode and attack that mutation. The compute security field has to adopt to rapid change and the evolution of security attacks. AI us well situated to answer this situation. AI is concerned with creating systems that evolve and react depending on the changes in the surrounding environment.

Fighting the Unknown. For many years, the efforts of the IT security industry were based on the assumptions that attacks were conducted on a large scale and major threats spread before arriving at a specific network or computer. Solutions were created on the basis of these assumptions and addressed as fellows. A typical threat was identified as a virus, which was investigated by IT security company labs that identified the virus signature and sent this information to endpoints installed with leading antivirus software.

Internet of Things In the past, most Internet interactions were interactions between humans that communicated via different platforms over the global network. Communications between humans, as the primary users of online communications will change dramatically with the evolution of the IoT realm [1].

Most of the entities that will communicate on the Web in the future will be machines, and they will be used to initiate reports, make contact, or respond to requests. [2] The means to facilitate this is characterized by easy access to the Web and the abil-

ity for mass distribution. For example, there is a possibility to turn households into smart homes with intercommunicative technology instead of investing in designing a supporting infrastructure. Even scattering sensors along oil fields is the result of technological developments that led to a decrease in the price of materials, easy logistical operation, and resistant products that meet industrial standards. [3]

The cyber world has barely begun to focus on new types of dangers such as the autonomous world, since this process has just started. However, the severity level of the threat is clear. In coming years, the cyber defense community will be called upon to develop new and effective technologies to meet the challenges posed by our changing and increasingly autonomous world.

1.2 Research Plan

This should begin with the specific aims of the research and provide a concrete plan for completion of the research including the design and methods. This section should include an explanation of how the methods will address the aims and the significance of the results for the field.

1.3 Progress Report

This should be a report on the research achievements of the student in the laboratory of the proposed supervisor during Preliminary Thesis Research. The report should not duplicate material previously submitted for evaluation as part of a previous degree, but may include work completed during rotations at OIST. The report may include examples of results obtained with the methods proposed. It is understood that results may not be available in projects requiring, for example, development of methods, sample preparation, or recruitment of participants, in which case other evidence of progress should be reported.

Chapter 2

How to use the template

This is a practical guide into how to use this template, by explaining the role of the different folders and files.

If some practices seem like overkill for a 20 page proposal (splitting the content across different files), that is because it probably is, but we built it this way because the PhD thesis template is structured identically. That means that you will be able to incorporate this document into your thesis seamlessly.

2.1 Folders

The main folder contains three folders detailed here:

- **Images.** This folder should contain all the images that you will use in your thesis. It can contain subfolders, for example one for each chapter. To include an image from the main text, use something like `\includegraphics{subfolder/image.jpg}` without worrying about the path to the `Images` folder.

- **MainText.** This folder contains a series of LaTeX files that form the main text: chapters and appendices. The PhD thesis template also has Introduction and Conclusion, here you can include them in the chapters.

- **Preamble.** This folder contains a series of LaTeX files with the pages that will appear before the main text. Please write (or copy and paste) your own text in those files and delete the dummy text when appropriate. The files are:

  - `abstract.tex` — Abstract. Follow directions in the file.
  - `mydefinitions.tex` — **Important** — This file should contain all the values relevant for the title page (name, thesis title, etc, which will be used automatically in the title and various preamble files), your bibliography style, all packages you need for your thesis and your custom definition and commands. Be careful of not importing a package that has already been imported in `xxx_Thesis.tex`, and be aware that some packages might interfere with each other.

- `physics_bibstyle.bst` — Bibliography style file modified by Jeremie Gillet in 2011 to suit his thesis. Might be suitable for physics. If you want to use another custom bibliography style, include the file in this folder.
- `Thesis_bibliography.bib` — BibTeX file containing your bibliography.

The PhD thesis template includes several other files, such as Acknowledgments or Glossary.

2.2 `Thesis_proposal.tex`

This is the main files, the only one that need to be compiled to build the document. Compile once with LaTeX, once with BibTeX and finally twice with LaTeX to get all the references right.

Let's go through each section and comment them briefly. The last section will emphasize the differences between the two files.

2.2.1 PACKAGES AND OTHER DOCUMENT CONFIGURATIONS

This section contains the minimum number of packages and definitions to compile the thesis. No line should be removed or modified.

2.2.2 ADD YOUR CUSTOM VALUES, COMMANDS AND PACKAGES

This section should not be modified directly. Instead, your packages and definitions should be included in `Preamble/mydefinitions.tex`.

2.2.3 TITLE PAGE

Creates the title page. Do not modify.

2.2.4 PREAMBLE PAGES

Structures the style (header) for the preamble pages and builds them. Do not modify.

2.2.5 LIST OF CONTENTS/FIGURES/TABLES

Creates the list of contents. Do not modify.

2.2.6 THESIS MAIN TEXT

Structures the style for the main text chapters and builds them.

2.2.7 APPENDICES

Structures the style for the appendices and builds them. The appendices are numbered with letters but are structured like regular chapters.

2.2.8 BIBLIOGRAPHY

Builds the bibliography. The style of the bibliography can be defined in `Preamble/mydefinitions.te`

Chapter 3

Figures, tables and images

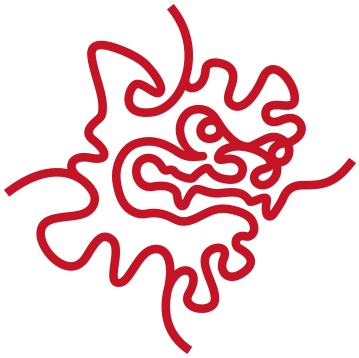
3.1 Figures

Figures should appear as close as possible to the first mention of them in the text. All figures must be referred to in the text by either a parenthetical mark-up (Figure 3.1) or a phrasing such as "Sequencing data, shown in Figure 3.1, shows that...". A parenthetical mention, but not an in-text mention, may be abbreviated as (Fig. 3.1). The number of the chapter should be part of the Figure number.

Figures must be accompanied by a caption that describes the material clearly and succinctly. Figure captions may start with a brief title in bold, which can then be referenced in the list of figures.

Figures should not have captions that run across pages, as a general rule. If a figure and its caption will be larger than a page, consider rewriting the caption, or reorganizing the figure. If this cannot be avoided, the figure caption should continue on the immediate next page, with a reference comment at the start of the text to the fact that it is a continuation of the caption from the previous page. No other main body text should then appear on that page.

Figure 3.1: Short caption (if wanted). Full caption with all the details here.



This secret image won't be numbered and won't appear in the List of Figures because of the *

Table 3.1: Short heading for the List of Tables.

Parameter	Value
Δ	0, 150
α	85
ϵ	6
κ	6.8
γ	0.2

Full caption with all the details here.

Parameter	Value
Δ	0, 1500
α	850
ϵ	60
κ	68
γ	2

This secret table won't be numbered and won't appear in the List of Figures because of the *

3.2 Tables

All tables should be referred to in the text by number (for example) "Table 3.1 describes all particles found in...". Tables may be printed in landscape mode rather than portrait mode, but must then be printed on a separate page (with continuing and sequential pagination). Tables may extend for more than one page, but should then have the table header row repeated on each page. Do not use font sizes smaller than 9 point. Tables should have a heading and may have a caption. The number of the chapter should be part of the Table number.

3.3 Images

Images are vital to the presentation of scientific data. Ensure that all textual annotations are correctly labeled, and that legends (if provided) are clear and legible. Use small symbols on charts for data points. Ensure that axis marks and axis labels are large enough to read clearly. Use all the white space where possible. Provide meaningful headings for charts, as well as a caption explaining the data. Be aware of the expected standards covering image manipulation and the standard practice for image presentation in your field, and adhere to them. In particular, avoid excessive density, contrast, and hue manipulation of photographic images. Where extensive manipulation of images is required for data extraction or analysis, this must be clearly explained as part of your methods, and explicitly in the caption for each figure.

Appendix A

About Appendices

Appendices are optional and should only be used if necessary.

Bibliography

[1] I.-Y. Ko, H.-G. Ko, A. J. Molina, and J.-H. Kwon, *SoIoT: Toward A User-Centric IoT-Based Service Framework*, ACM Trans. Internet Technol. **16**, 8:1–8:21 (2016).

[2] N. Komninos, M. Pallot, and H. Schaffers, *Special Issue on Smart Cities and the Future Internet in Europe*, Journal of the Knowledge Economy **4** (2012).

[3] X. Chen, D. Zhang, L. Wang, N. Jia, Z. Kang, Y. Zhang, and S. Hu, *Design Automation for Interwell Connectivity Estimation in Petroleum Cyber-Physical Systems*, Trans. Comp.-Aided Des. Integ. Cir. Sys. **36**, 255–264 (2017).