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

In recent years, a large amount of research addressing the contribution of intelligent systems to cyber security has been conducted. One can hear more and more about artificial intelligence (AI), machine learning, and deep learning systems in cyber security. As often happens with buzz words, nonexperts tend to use them casually and loosely. Despite the fact that the borderlines between such terms are not always clear and these borderlines become even fuzzier with new practical and theoretical developments, it is important to try to characterize the focus of these systems in the field.

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 identi-

fied 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 ability 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 The Contribution of Intelligent Systems to Cyber Security

Artificial intelligence (AI), which was officially established in the late 1950s by scholars such as Marvin Minsky, is used as a generic name representing a wide variety of methods, tools, and techniques that mimic "cognitive" functions or tasks that people associate with the human mind, such as "learning," "planning," "reasoning," or "problem solving" [4].

1.3 Research Plan

As an aims of the research and We provided a concrete plan for completion of the research including the design and methods.

- Analyzing previous AI solutions which is developed for cybersecurity and figure out the deficiencies of the application.
- Investigating "exploit databases" and collecting data related the kind of the threats.
- Analyzing Cloud Based Systems' network infrastructures for collecting data.
- Researching common and recent threats for the computer networks.
- Investigating the literature of the machine learning algorithms.

- Analyzing the vulnerabilities of the cloud systems.
- Defining the constraints of the problem.
- Modeling the problem.
- Creating the fittest machine learning models for AI application
- Developing the AI application that can detect, repair and defense the cloud based systems to against the cyber threats and attacks.
- Creating real-world test environment and creating real-time cyber-attacks scenarios for test the developed AI supported security applications.
- Regarding the test results of the application, optimize the AI algorithms with heuristic and metaheuristic approaches.

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).

[4] S. Russell and P. Norvig, *Artificial Intelligence - A modern Approach*, Prentice Hall International Editions, Upper Saddle River, NJ (1995).