

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

Aytaç Özkan
<mailto:Aytac.Ozkan@inra.fr>

October 1, 2019

- 1 About me
- 2 Motivation
- 3 AI: The next Frontier in IT Security
- 4 The Contribution of Intelligent Systems to Cyber Security

About me

Universite // Paris Seine, École internationale des sciences du traitement de l'information, Cergy, France

M.S., Big Data, July, 2019

- Dissertation Topic: "Improving data quality for big data using advanced analytics"
- Advisor: Prof. Rachid Chelouah

Marmara University, Istanbul, Turquie

M.S., Information Systems and Engineering, May, 2017

Professional Experience

Institut national de la recherche agronomique, Avignon, France

Research Software Engineer

May, 2019 - present

Developing machine learning supported semantic search platform for bioinformatic data systems.

Ultra Marathon



Figure: Erciyes Ultra Sky Trail

Motivation

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.

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. This 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.

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 [KKMK16].

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. [KPS12] 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. [CZW⁺17] 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.

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” [RN95]. The importance of AI in cyber security is twofold and related to two opposing directions. The first direction focuses on AI-controlled systems as potential targets of cyber attacks, mainly due to their increasing role in controlling vital and complex systems. There are numerous examples of cyber risks related to AI-controlled systems, such as smart vehicles [BSEG13], smart grids and smart cities [AT17].

Knowledge-based systems and machine learning methods are two well-known classes of AI methods that contain valuable tools used in cyber security. In Knowledge-based systems, a huge amount of (experts') Knowledge is uploaded to the computer memory (thus, it is also called expert systems). [Fel77] The learning part in these systems is based on the reasoning related to this large body of knowledge, which is often obtained by programmed rules (such as "if-then" and "inference logic rules").

Antivirus and antispam software packages [BB08] represent straightforward implementations of expert systems in cyber security. In this case, expert knowledge (accumulated based on a large amount of transactions) regarding the procedures used—such as applied protocols, network traffic (e.g., HTTP, HTTPS, VoIP, or email), and I/O interactions with the operating system—is organized systematically to protect the users from cyber

breaches. There are several papers in this issue that serve as good examples of such expert systems [MGS17].

References I



Anwaar AlDairi and Lo'ai Tawalbeh, *Cyber security attacks on smart cities and associated mobile technologies*, Procedia Computer Science **109** (2017), 1086 – 1091, 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16-19 May 2017, Madeira, Portugal.



Enrico Blanzieri and Anton Bryl, *A survey of learning-based techniques of email spam filtering*, Artif. Intell. Rev. **29** (2008), no. 1, 63–92.

References II



Lars Torsten Berger, Andreas Schwager, and J. Joaquín Escudero-Garzás, *Power line communications for smart grid applications*, JECE **2013** (2013), 3:3–3:3.



Xiaodao Chen, Dongmei Zhang, Lizhe Wang, Ning Jia, Zhijiang Kang, Yun Zhang, and Shiyang Hu, *Design automation for interwell connectivity estimation in petroleum cyber-physical systems*, Trans. Comp.-Aided Des. Integ. Cir. Sys. **36** (2017), no. 2, 255–264.

References III






Edward A. Felgenbaum, *The art of artificial intelligence: Themes and case studies of knowledge engineering*, Proceedings of the 5th International Joint Conference on Artificial Intelligence - Volume 2 (San Francisco, CA, USA), IJCAI'77, Morgan Kaufmann Publishers Inc., 1977, pp. 1014–1029.



In-Young Ko, Han-Gyu Ko, Angel Jimenez Molina, and Jung-Hyun Kwon, *Soiot: Toward a user-centric iot-based service framework*, ACM Trans. Internet Technol. **16** (2016), no. 2, 8:1–8:21.

References IV

-  Nicos Komninos, Marc Pallot, and Hans Schaffers, *Special issue on smart cities and the future internet in europe*, Journal of the Knowledge Economy **4** (2012).
-  Alex Maltinsky, Ran Giladi, and Yuval Shavitt, *On network neutrality measurements*, ACM Trans. Intell. Syst. Technol. **8** (2017), no. 4, 56:1–56:22.
-  S. Russell and P. Norvig, *Artificial Intelligence - A modern Approach*, Prentice Hall International Editions, Upper Saddle River, NJ, 1995.