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
5. Literature review
6. How organizations are benefiting from AI In cybersecurity
7. Research Plan
8. Conclusions

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

INRA, Institut national de la recherche agronomique, Avignon, France *Research Software Engineer* May, 2019 - present

Ultra Marathon

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. 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.

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].

Literature review I

There have been several similar works done in IoT fields. Still, researchers are working in this area. Pahl et al. [PA18] have mainly developed a detector and firewall for an anomaly of IoT microservices in IoT site. Clustering methods like K-Means and BIRCH have been implemented [AYHW03] for different microservices in this work. In clustering, different clusters were grouped in the same if the center is in the three times of standard deviation distance. The clustering model has been updated using an online learning technique. With the algorithms implemented, the overall accuracy obtained by the system is 96.3%. A detailed description of a smart

Literature review II

home system where security breaches were detected by deep learning method Dense Random Neural Network (DRNN) [BYG18] have been introduced in [BYG18].

Liu et al. [LLLY18] proposed a detector for On and Off attack by a malicious network node in industrial IoT site. By On and Off attack they meant that IoT network could be attacked by a malicious node when it is in an active state or On state. Furthermore, the IoT network behaves normal when its malicious node is in the inactive or off state. The system was developed using a light probe routing mechanism with the calculation of trust estimation of each neighbour node for the detection of an anomaly.

Diro et al. [DC18] discussed the detection of attack using fog-to-things architecture. The authors of the paper gave a comparison study of a deep and a shallow neural network using open source dataset. This work's primary focus was to detect four classes of attack and anomaly. For four class the system got the accuracy of 98.27% for deep neural network model and accuracy of 96.75% for shallow neural network model.

How organizations are benefiting from AI In cybersecurity

AI lowers the cost to detect and respond to breaches: Using AI for cybersecurity enables organizations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify incidents, investigate them, and remediate threats. Close to two-thirds of executives (64%) say that AI lowers the cost to detect and respond to breaches. The reduction in cost for a majority of organizations ranges from 1% – 15% (with an average of 12%). However, a few organizations have managed to achieve even higher cost reductions (more than 15%) leading to higher benefits (see figure 2).

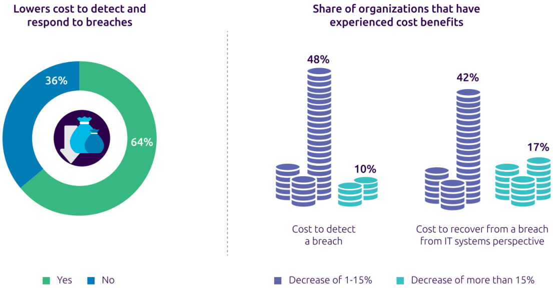


Figure: AI in cybersecurity lowers the cost to detect and respond to breaches [Ins19].

AI makes organizations faster at responding to breaches: Fast response is essential to securing an organization from cyber attacks. With AI, the overall time taken to detect threats and breaches is reduced by up to 12%. AI also reduces the time taken to remediate a breach or implement patches in response to an attack by 12%. A small subset of organizations even managed to reduce these time metrics by greater than 15% zPower, a leading rechargeable battery manufacturer, partnered with a startup to use AI to detect and autonomously respond to threats as they emerge. Just weeks after the solution was deployed, the security team was alerted to the fact that an employee had downloaded potentially malicious software. They were able to remove the threat and head off any attack in real time [Dar17]. (see figure 3 [1])

[1] Source: Capgemini Research Institute, AI in Cybersecurity executive survey, $N = 850$ executives

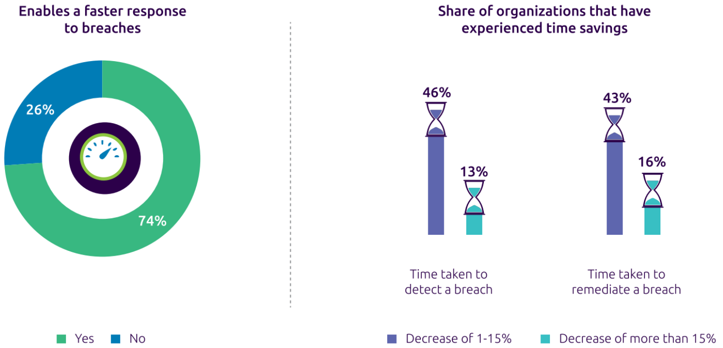


Figure: Nearly three in four executives say AI in cybersecurity enables a faster response to breaches Enables [Ins19].

AI results in higher efficiency for cyber analysts: Cyber analysts spend considerable time going through data logs and/or incident timesheets. With AI helping carry that workload, cyber analysts can spend more quality time analyzing the incidents identified by the AI cybersecurity algorithms.

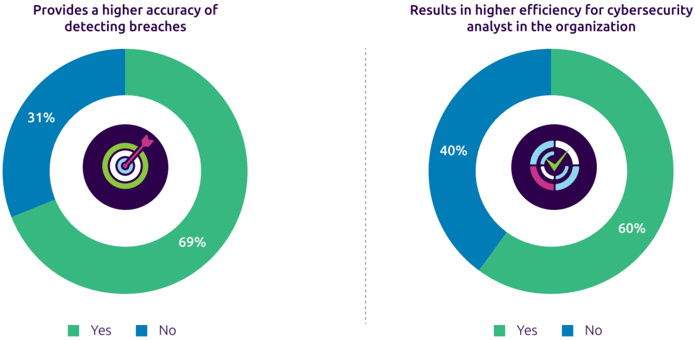
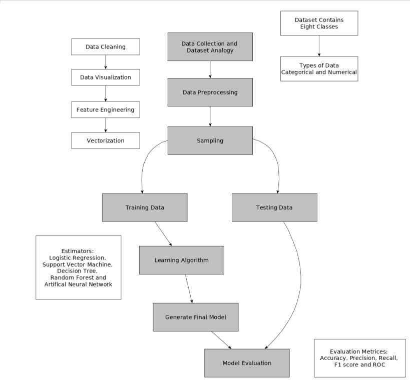


Figure: AI can help organizations provide a higher accuracy of detecting breaches Provides [Ins19].

- **AI results in new revenue streams through cybersecurity offerings:** With the proliferation of smart products – electronic devices generally connected wirelessly to other devices or networks – the attack surface for hackers increases. This creates an opportunity – offering cybersecurity services to manufacturers that sell smart products. A number of organizations are already targeting this opportunity:
  - **GE's** Digital Ghost technology offers an AI-enabled protective layer for industrial control systems. Digital Ghost leverages the digital twins (which are often referred to as the brains of the associated control systems) to gain knowledge of the machine's working pattern. Digital Ghost detects if the machine, while appearing to operate normally, is actually being influenced by cyber attacks [Res19].

- Similarly, **Siemens'** 'Industry Anomaly Detection' solution uses AI to detect anomalies, either via intrusion or data theft by hackers. The solution analyzes data traffic in the network in a learning phase to establish transparency of every device connected to the network. It can then identify any vulnerabilities while providing continuous monitoring to detect anomalies. [Sie18]

Research Plan



Data Cleaning
Data Visualization
Feature Engineering
Vectorization

Data Collection and Dataset Analogy
Data Preprocessing
Sampling

Dataset Contains Eight Classes
Types of Data Categorical and Numerical

Training Data
Testing Data

Estimators: Logistic Regression, Support Vector Machine, Decision Tree, Random Forest and Artifical Neural Network

Learning Algorithm
Generate Final Model
Model Evaluation

Evaluation Metrices: Accuracy, Precision, Recall, F1 score and ROC

Figure: Overall framework for attack and anomaly detection in IoT and Cloud Base Services.

Research Plan

- 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.

Research Plan

- 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.

Research Plan

- 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.

Conclusions

Thank You!

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.

References II

Charu C. Aggarwal, Philip S. Yu, Jiawei Han, and Jianyong Wang, - *a framework for clustering evolving data streams*, Proceedings 2003 VLDB Conference (Johann-Christoph Freytag, Peter Lockemann, Serge Abiteboul, Michael Carey, Patricia Selinger, and Andreas Heuer, eds.), Morgan Kaufmann, San Francisco, 2003, pp. 81 – 92.

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 III

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

- Olivier Brun, Yonghua Yin, and Erol Gelenbe, *Deep learning with dense random neural network for detecting attacks against iot-connected home environments*, Procedia Computer Science **134** (2018), 458 – 463, The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops.

References IV

Xiaodao Chen, Dongmei Zhang, Lizhe Wang, Ning Jia, Zhijiang Kang, Yun Zhang, and Shiyan 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.

Darktrace, *Darktrace stops emerging insider threat at battery plant*, `https://www.darktrace.com/en/press/2017/199/`, 2017, Accessed: 2019-08-31.

References V

Abebe Abeshu Diro and Naveen Chilamkurti, *Distributed attack detection scheme using deep learning approach for internet of things*, Future Generation Computer Systems **82** (2018), 761 – 768.

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.

References VI

Capgemini Research Institute, *Reinventing cybersecurity with artificial intelligence the new frontier in digital security*, `https://www.mendeley.com/catalogue/reinventing-cybersecurity-artificial-intelligence/`, 2019, Accessed: 2019-08-31.

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 VII

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).

Xiao Liu, Yuxin Liu, Anfeng Liu, and Laurence T. Yang, *Defending on-off attacks using light probing messages in smart sensors for industrial communication systems.*, IEEE Trans. Industrial Informatics **14** (2018), no. 9, 3801–3811.

Alex Maltinsky, Ran Giladi, and Yuval Shavitt, *On network neutrality measurements*, ACM Trans. Intell. Syst. Technol. **8** (2017), no. 4, 56:1–56:22.

References VIII

Marc-Oliver Pahl and Francois-Xavier Aubet, *All eyes on you: Distributed multi-dimensional iot microservice anomaly detection.*, CNSM (Stefano Salsano, Roberto Riggio, Toufik Ahmed, Taghrid Samak, and Carlos Raniery Paula dos Santos, eds.), IEEE Computer Society, 2018, pp. 72–80.

GE Research, *Digital ghost: Real-time, active cyber defense*, `https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense`, 2019, Accessed: 2019-08-31.

References IX

- S. Russell and P. Norvig, *Artificial Intelligence - A modern Approach*, Prentice Hall International Editions, Upper Saddle River, NJ, 1995.
- Siemens, *Siemens heightens industrial cyber security by detecting anomalies*, https://assets.new.siemens.com/siemens/assets/api/uuid:3f3c5e90-56c9-4a45-ac7f-b8d253a2de88/PR2018040235DFEN.pdf, 2018, Accessed: 2019-08-31.