The Application of Artificial Intelligence for Cybersecurity in Industry 4.0

Ines BenZid[1], Mithil Parekh[2], Karl Waedt[3], Xinxin Lou[4]

Abstract: The use of Artificial Intelligence (AI) in different domains is continuously growing. In particular for cybersecurity, we can see the implementations of AI solutions, e.g. machine learning, in a wide range of applications from various domains. While some consider this step as risk for cybersecurity, others agree that it is in fact a solution to many issues as well. This leads to a higher necessity of having a right understanding as well as handling of cybersecurity controls that enforce meeting domain, project and application specific security targets. This implies that more efforts and resources have to be focused and invested towards cybersecurity. One reason for this is that attackers (threat agents) may integrate AI based algorithms and AI based evaluation of data, which forces the security staff to respond at a similar level. Thus, we are considering AI as a potential solution for satisfying a set of rising needs and objectives. In this paper, we present the concept for merging and integration of these three major domains and applications. Also, we detail the relevant motivations, requirements and challenges to be considered when coming to such combination.

Keywords: Industry 4.0, Cybersecurity, Artificial Intelligence

1 Introduction

The term "Artificial Intelligence" was coined by McCarthy, one of the participants in the legendary AI conference at Dartmouth College (New Hampshire, USA, 1956), which today is considered the beginning of the KI (Künstliche Intelligenz in German) era. At that time, AI was understood as a machine reasoning ability. In the beginning of the high phase of research activity, the languages LISP, PROLOG and the concept of perceptron, which were seen as the core of the replication of biological brains, were created. When it became clear in the early 1970s that AI's expectations of AI's short-term achievable performance had been greatly overrated, enthusiasm over the subject and with it the bulk of national research funding abruptly drained.

While by the end of the 80s and beginning of the 90s AI experts failed to meet business expectations, subsequently different concepts outside the current focus of the started to appeared and grew. In particular, a concept for multi-layered networks of perceptron was created. In 1986, Rumelhart, Hinton, and Williams used the method of

[1] Bielefeld University, Faculty of Technology, ibenzid@techfak.uni-bielefeld.de
[2] Otto-von-Guericke-University Magdeburg, mithil.parekh@ovgu.de
[3] Framatome GmbH, karl.waedt@framamtome.com
[4] Bielefeld University, Faculty of Technology, xlou@techfak.uni-bielefeld.de

doi:10.18420/inf2019_ws29

"backpropagation" of parameter estimation on multi-layered neural networks, which was known from the 1960s, to establish proven methods of numerical mathematics and thus founded the concept of "deep learning" [RHW86]. In 1989 LeCun, deployed the largely developed by him new type of neural networks "Convolutional Neural Networks" (CNN) for area-oriented (image) data. He applied this for the detection of hand-written postal codes and thus automated the mail sorting of the USA [Ly89], which was a sensation. So, the basis for a next spring of the AI was prepared.

In the mid-nineties, the third phase of the AI, has begun which is "Machine Learning (ML)". ML in simple term is one form of AI used to enable a system to learn from data rather than explicit programming. However, the process isn't really that simple. It uses a variety of algorithms that iteratively learn from input data in order to predict outcomes. Depending on the chosen learning method, supervised, unsupervised or semi supervised learning, etc., the machine is trained with a specific set of data that allows it to predict future outcomes.

In the I4.0 age, more digital systems are utilized in the industrial domain. AI is considered to apply on cybersecurity issues, as the potential for malicious attacks on industrial systems is increasing. The Previously isolated systems are now being more interconnected through communication networks crossing national borders, as well as more automated processes that are integrated within the industry such as collaboration with third parties in the supply chain. This eventually results in a growing attack surface causing the system to get more vulnerable against cyber-attacks and breaches. This grows along the significant technological advances and capabilities certain parties are gaining, with their different intentions, trying to take advantage out of such weaknesses within critical target systems.

Dynamic and flexible I4.0 architectures cannot be fully described because their configuration can adapt to requirements. This can be a use case for AI. Examples of this are AI-supported, self-organizing inventory management, or a dynamic change in the production process chain according to machine utilization or production costs. Therefore, they require agile and adaptive security solutions. A static anomaly detection, that e.g. works on the basis of learned production processes, would give the above mentioned examples very often false reports, since the processes can change fundamentally in a short time. In these cases, additional metadata must be included in the learning process. Also, the underlying learning processes themselves must be protected against manipulation. In the above examples, attackers who manipulate the learning process would be able to manipulate the dynamic production process chain so that no product would be created [Mh18].

2 Combining AI technique for cybersecurity

2.1 Motivations

All known threats from the Industry 3.x world are also relevant in Industry 4.0. There are regularly massive cyber-attacks with the objectives of industrial espionage and sabotage and data theft identified, such as the BSI management report for 2018 and the member survey from the VDMA at the end of 2017 [V19]. According to the VDMA study, one third of cyber-attacks in 2017 resulted in production or operational failures.

In Industry 4.0 we are starting to deal with systems that are highly complex, technologically advanced and widely interconnected. Keeping track of every and each data stream flowing into this network and trying to guarantee a secure and trustworthy environment is a key task. This growing amount of data and its complexity managed and manipulated by human expertise requires a big amount of effort and time.

This is where AI can be considered. Through the deployment of an appropriate AI algorithm, problems related to tremendous amount of information that are not possible to analyse or assess with limited resources can be solved successfully with a noticeable less amount of resources. Many examples for pattern recognition in different fields such as medicine, quality assurance and system control are a proof of how impressive AI application when dealing with systems with high complexity. In the security area, assistance systems can support specialized personnel, take over a number of tasks completely, increase the efficiency of processes and, with machine learning, open up task areas that were previously inaccessible to programmed algorithms. Thus, AI provides new perspectives for overcoming skill shortages and improving protection [Mh18].

2.2 Advantages of combining AI techniques for cybersecurity

For the domain of cybersecurity in Industry 4.0, AI can be applied in different ways. The main applications of AI with cybersecurity are identification and authentication, anomalies detection like software, malware, data streams anomalies, etc., and vulnerability assessment.

An essential prerequisite for implementation of AI in Industry 4.0 is a secure and trustworthy treatment of data and a reliable protection of inter-company communication from external attacks. Inter-company value creation networks can only be established and profitably used if the data streams are unambiguous and able to allocate to secure identities [Lj16].

For identification and authentication of people while accessing certain system, AI is used to check the integrity of the acquired information by comparing the input data against stored information. Also, AI can be used when checking typing patterns on the keyboard

or computerised hand writing, in order to have a unique identification of the user. For pattern recognition through image or video identification, specific trained AI algorithms can provide high success rates. This kind of algorithms is also beneficial when dealing with quality assurance of products where similar principles are used to compare new products against those with the required set of qualifications.

The detection of anomalies whether related to software, malware or within large streams of data is the field which is most known for AI applications. In a sort of Intrusion Detection and Prevention System (IDPS), AI algorithms are used with attack patterns. In this case, the algorithms are trained with normal states of the system. The uses of AI in this context can extend to include classification of attacks and alarms in order to avoid false positive alarms caused by unusual behaviour of the security personnel. Market forecasts suggest that by 2020, new technologies and methods such as analytics, machine learning, and behavioral detection will be integrated into most IDPS tools and offered on the market.

Another area of application of AI is the detection of malicious software using 2 different techniques: machine learning and classification techniques. The machine learning technique requires monitoring of either the system or the network activity in order to detect any anomalies as early as possible. The monitoring is realized through the analysis of different system features such as accessed Application Programming Interfaces (APIs), fields of disk, consumed power, etc. The second technique which uses classification algorithms helps with the classification of malware, since the difference of malware signatures can be very minor and especially hard to detect.

Other applications of AI techniques related to maintenance can also be conducted. In this context, specific algorithms are trained to inform relevant parties of future maintenance or products replacement appointments which improves the reliability and timeliness of updates.

Overall AI algorithms can be applied for three main goals:

- Create predictions
- Plan preventions
- Take actions

3 Requirements for utilizing AI as part of cybersecurity controls

In order to get the most of AI for the implementation of advanced security controls it is important to meet certain requirements. We think that the two most important requirements are: the choice of the AI technique and the choice of comprehensive representative input data.

With the different techniques of AI available and their different applications, the choice of the right method is important to guarantee the expected outcome. While some algorithms can demonstrate high efficiency for a specific use case others can be useless and with no significant result when not used in the right place. A number of selection criteria are:

- the system characteristics, capabilities and capacities,
- the limitations regarding the integration of the method,
- the associate security considerations (third party, supply chain, etc.),
- the purpose to be served through the algorithm.

Once we chose the right algorithm to use, it is also important to have the most up to date input data provided to the learning system. This is crucial for getting high performance of the algorithms.

4 Challenges of deploying AI for security controls

As for any new growing domain, many challenges can be faced. This also applies when trying to integrate AI for the implementation of security controls within Industry 4.0. Similarly to any other traditional anomaly detection tool, when using AI algorithms we are actually trying to detect something which is not clearly known or defined which can present a challenge.

Also, as explained in the previous section, acquiring the correct and especially latest input data for the learning algorithm can present some difficulties which affect the performance of the method.

Last but not least, along the use of AI techniques to improve security postures for new systems used in the Industry 4.0, we should examine the potential implications related either the used method itself or the consequences of its deployment on the security posture of certain systems. These implications can be a form of new vulnerabilities as well as new attack vectors created within either the office IT systems, the production OT systems or the used AI system itself.

Conclusion

As justified and outlined in the paper, using AI techniques for the implementation of advanced security controls in Industry 4.0 can be beneficial on various levels, but can also cause new obstacles. On one hand, while common attack techniques severely limit the effectiveness of classic implemented security tools e.g. IDS/IPS, “black box” solutions such as AI algorithms can help to solve this issue. Also, the upgrading during

the transformation phase of Industry 3.x into I4.0 environments requires better defence strategies against this type of maximum invasive attacks. On the other hand, it is important to meet the specific set of requirements using AI algorithms in such industry in order to help with acquiring an acceptable success rate using the method.

Bibliography

[ARH86] Rumelhart, D.E., Hinton, G.E., and Williams, R.J.(1986b). Learning representations by backpropagating errors. Nature, 323, 533–536.

[Ly89] LeCun, Y., Jackel, L., Boser, B., and Denker, J.(1989). Handwritten digit recognition: Applications of neural network chips and automatic learning. IEEE Communications Magazine, 27(11), 41–46.

[Lj16] Dr Lutz Jänicke, et al, IT Security in Industry 4.0, 2016.

[Mh18] Markus H., et al, Künstliche Intelligenz (KI) in Sicherheitsaspekten der Industrie 4.0, 2018.

[V19] VDMA, www.vdma.org/documents/15012668/22538766/Grafik_PI_Industrial_Security_2017-11-29_1512390672976.pdf/b94c55dc-5b8f-44f1-ad03-1b7628499e21, Accessed on 29/04/2019.