CONSIDERATION OF ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY ASPECTS OF I&C SYSTEMS

I. BEN ZID
Framatome GmbH / Bielefeld University
Erlangen, Germany
Email: ines.ben.zid1@gmail.com

X. LOU
Framatome GmbH / Bielefeld University
Erlangen, Germany

Dr. K. WAEDT
Framatome GmbH
Erlangen, Germany

Abstract

After two extended up and down periods in the historical development of Artificial Intelligence (AI) during the last decades, since a few years, many AI solutions have become inherent components in several industrial business domains. The paper will briefly analyse how AI came to be, where it is now and what boundary conditions have to be met in order to be able to apply AI. The paper will look also at how AI is considered for security aspects in Industry 4.0 and how this can be applied for the nuclear domain, especially for Safety I&C, Operational I&C and Electrical Power Systems (EPS). According to the focus of the paper, types of Machine Learning (ML) that can be applied and what key security challenges have to be considered will be indicated. The key AI supported concepts that will be addressed include: identification and authentication with AI support, AI supported anomaly detection in data streams and AI based identification of potential malware. Finally, the paper will also address the integration of AI approaches with traditional approaches from implementing and validating security controls and for attack tree analysis. This is an ongoing development where decisions on the effort for supervised Machine Learning (identification of representative vectors, tagging of artefacts, tagging of relations) or unsupervised ML has to be balanced with the effort for validating the results obtained via involved AI algorithms. With a focus on security testing the validation of representativeness and coverage of the AI based results remains an important challenge for ongoing R&D. The strength of the AI supported protection may have an impact to nuclear safety (due to potentially remaining residual risks), a topic that will be outlined but not elaborated in detail in this paper.

1. INTRODUCTION

The term Artificial Intelligence (AI) 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 AI 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 and PROLOG and the concept of perceptron, which was seen as the core of the replication of biological brains, were created. It became clear in the early 1970s that AI's expectations of short-term achievable performance had been greatly overrated. Subsequently, enthusiasm over the subject and, with it, the bulk of national research funding abruptly collapsed. McCarthy wrote that it would not take 10 years for machines to acquire simple human skills, but up to 500 years, because of a technical breakthrough in terms of machine processing power.

Again, by the end of the 80s and the beginning of the 90s, AI experts failed to meet business expectations. However, this time different concepts outside the current focus started to appear and grow. In particular, a concept for multi-layered networks of perceptron was created. In 1986, Rumelhart, Hinton, and Williams used the method of "backpropagation" of parameter estimation on multi-layered neural networks, which was known from the 1960s, to establish methods of numerical mathematics and thus founded the concept of "deep learning" [1]. In 1989 LeCun had developed a new type of neural networks "Convolutional Neural Networks" (CNN) for area-oriented (image) data. This was used for the detection of hand-written postal codes

and thus automated the mail sorting of the USA [2]: A sensation. The basis for a next spring of the AI was prepared.

In the mid-nineties, the third phase of the AI, which is ongoing till this day, has begun which is "Machine Learning (ML)". ML, in simple terms, is one form of AI used to enable a system to learn from data rather than deploying 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.

With Industry 4.0, the potential for malicious attacks on industrial systems is increasing. As 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 such systems.

Dynamic and flexible I4.0 architectures cannot be statically described because their configuration has to be adaptable to changing 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 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 [3].

Some 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 [4] and the member survey from the VDMA at the end of 2017 [5]. According to the VDMA study, one third of cyberattacks 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 each and every 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 are managed and manipulated by human expertise, which 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 a tremendous amount of information that are not possible to analyse or assess with limited resources can be solved successfully with a noticeable reduced amount of resources. Many examples for pattern recognition in different fields such as medicine, quality assurance, system control are already a proof of impressive AI application, when dealing with with highly complex systems. 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 [3].

2. APPLICATIONS AND IMPLEMENTATION

2.1. The applications of AI for cybersecurity of I&C systems

For the domain of cyber security 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.

The essential prerequisite for a successful implementation of 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 be associated to secure identities [6].

For identification and authentication of people while accessing a 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 be extended 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 behavioural 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), accessed hard disk partitions, 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
  - Detecting email cybersecurity threats
  - Detecting malware threats
  - Detecting network anomalies
— Plan preventions
  - Securing user authentication and identification
— Take actions

In the following Figure1, we display the percentage of using AI in Cybersecurity within specific areas.

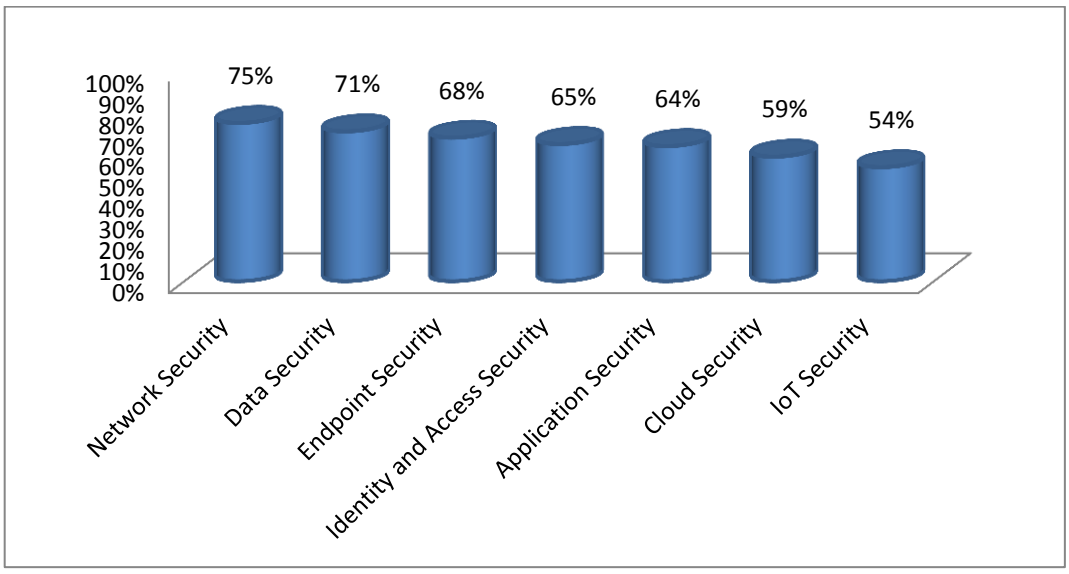

FIG. 1. Deployment of AI in Cybersecurity for different areas [7].

We can notice that the top areas of security where AI is deployed are the major areas considered in the nuclear domain as well. The areas: Network security, Data security, endpoint security and identity and access security, represent the attack vectors which most recent or even the majority of cybersecurity breaches in nuclear power have been recorded.

2.2. The implementation of AI techniques for cybersecurity of I&C systems

Artificial intelligence (AI) applied to cybersecurity provides security professionals with an augmented ability to protect endpoints, data, and networks. By using sophisticated abilities to predict problems based on prior solutions and an ability to use natural language processing (NLP) to analyze unstructured data, unique solutions and detailed insight are provided to the Security Operations Center (SOC) to quickly and cost-effectively stop intrusions or even prevent them before they happen. It's also the only way to protect a network against malicious attackers also using AI [8].

Most areas of application of AI use two 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), accessed hard disk partitions, 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.

Beside the knowledge concerning the AI techniques, specific awareness within the organization have to be recognized. This awareness concerns mainly software requirements and their configuration. For instance, Python is highlighted in particular for its continuous growing and appreciation among most programmers. It also has been known as the language of choice for Machine Learning (ML) and Deep Learning (DL). Some of the different characteristics of this language, that boosted its success when used with AI, are the fact that it is an easy to learn, interpreted and object-oriented language along with the availability of open source libraries. Some of these libraries are Cybersecurity-specific [9].

Especially when dealing with critical system where security incidents have a high cost on different levels, it is important to have the required confidence and about the effectiveness and reliability of the solutions. In this case, the continuous monitoring and the scalability of the AI-based solutions has to be planned, in order to guarantee the expected outcomes. This is possible to realise, also based on AI-Solutions, by following specific procedures. Among these we can mention the evaluation of algorithms, where the application of best practices in terms of dealing with raw data, secure development environment and secure testing are checked. Another recommended behaviour is exploring the methods hackers might use to evade the implemented AI-based solutions.

3. CHALLENGES AND BOUNDARIES

3.3. The challenges met when applying AI for cybersecurity of I&C systems

As any new and growing domain, many challenges can be faced when integrating AI for cyber security within the 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. This aspect usually rises the complexity of the anomaly detection tool which is an inevitable challenge.

Also, along the use of AI techniques to improve security postures for new systems used in Industry 4.0, we should examine the potential implications related either to 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.

Additionally, as explained in the previous section, acquiring the right and especially most up to date input data for the learning algorithm can present some difficulties which will have an influence on the performance of the method.

Finally, and along the previous technical challenges we might face using AI-based solutions with Cybersecurity, aspects of data and model quality has to be tested and proven to be maintained.

3.4. The boundaries set for integrating AI with cybersecurity of I&C systems

In order to get the most of AI with security in the new cyber industry, it is important to meet certain requirements. The two most important requirements we can state here are: the choice of the AI technique and the 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 irrelevant and with no useful result if not applied in the right place.

A number of criteria to keep in mind making this choice are explained in the following Figure 2.

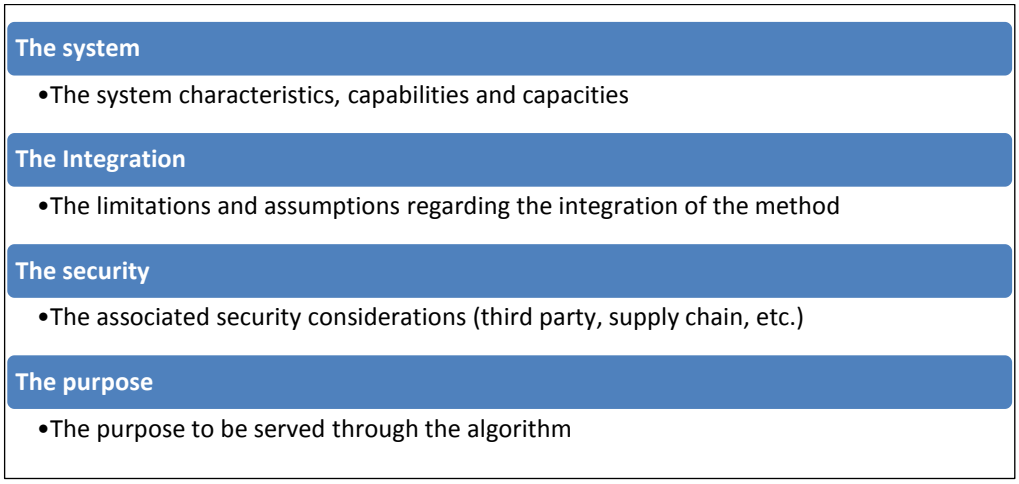

FIG. 2. Main Criteria for applying AI with Cybersecurity.

Once we have 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 the performance of the algorithm. Also, it is important to keep in mind that we are dealing with the topic of security with systems where technology is growing in a remarkable way and where sensitive and critical information can be concerned. Thus providing the learning algorithm with the most updated inputs is quite important.

4. CONCLUSION

As explained in the paper, using AI applications for security in Industry 4.0 can be beneficial on different levels but can also come up with new obstacles. This has to be considered already now, as typically industry proven solutions will later on also be deployed in the nuclear domain.

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 preconditions for using AI algorithms in order to acquire an significant success rates.

REFERENCES

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

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

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

[4] www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html, accessed on 30/04/2019.

[5] 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.

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

[7] Capgemini Research Institute, Reinventing Cybersecurity with Artificial Intelligence: The new frontier in Digital Security, 2019

[8] Ted Coombs, Artificial Intelligence & Cybersecurity, 2018

[9] Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity, 2019

BIBLIOGRAPHY

ISO/IEC 27002, Information Technology—Security techniques—Code of Practice for Information Security Controls, 2013.

IEC 62645, NPPs—I&C Systems—Requirements for Security Programmes for Computer-Based Systems, 2014.

I. Ben Zid, A. Tellabi, K. Waedt. End-user interface security in nuclear power plants. SNE: 43rd Annual Meeting Spanish Nuclear Society, 2017.

I. Ben Zid, D. Gupta, X. Lou, K. Waedt: A Functional Specification-Based Approach For Analyzing The Cyber Security Of End-User Interfaces Within NPPs