Securing Industrial Infrastructure against Cyber-Attacks Using Machine Learning and Artificial Intelligence at the Age of Industry 4.0

M. Aliyari[a]

[a] Faculty member of Ayatollah Boroujerdi University, Borujerd, Iran.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Fourth industrial revolution or industry 4.0, refers to advancements in manufacturing systems and services using "cyber physical systems" to increase manufacturing capabilities and flexibility to adapt production quickly and efficiently in response to changing conditions and demands. we first discuss a few applications of the industry 4.0 to get familiar with technologies used , we then identify the cyber security risks involved in different areas and phases of Industry 4.0 applications, finally, we will discuss possible solutions to mitigate the potential attacks and increase the system robustness using machine learning.

Keywords: industry 4.0, machine learning, artificial intelligence, internet of thing (IoT), SCADA system, support vector machine (SVM)

1. Introduction

With the advancements in data sharing and connectivity, manufacturing can benefit from concepts such as Internet of Things (IoT) and machine to machine (M2M) communications [1].

"Cyber-physical systems" (abbreviated CPS) is defined as "a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities" [7].

Figure 1 shows a model of such system and how the components such as sensors, actuators and communication networks connect and interact with other components [20].

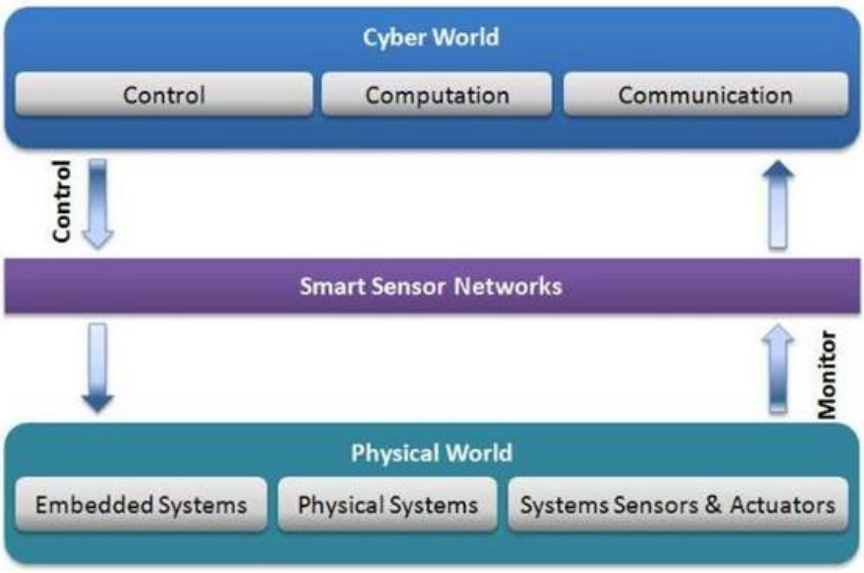

Figure 1: Model of a Cyber Physical System

IoT involves interconnecting various digital and electronic devices and platforms through communications networks, particularly through the Internet [2].

IoT device usage has gained popularity recently due to increased capability and increased internet speed. It is estimated that by 2025, 73.5 billion IoT devices will be in use as shown in Figure 2 [1].

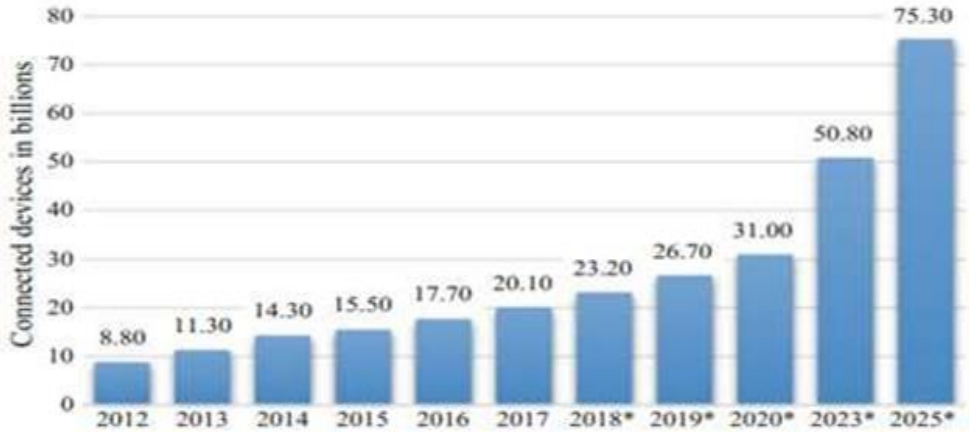

Figure 2: Number of IoT devices connected to Internet

According to Cotteleer and Sneiderman, Industry 4.0 can be explained as a three-stage process:

1- Collecting data from sensors installed on the equipment (sensor fusion) 2- Using data analytic techniques to process, optimize and visualize data. 3-Performing decision making activity and translating the results into meaningful commands so that the machines can perm required tasks [22].

Artificial intelligence has a strong presence in stage 2 of this process in the form of machine learning algorithms which enable the equipment to learn, diagnose and optimize the process autonomously. Although the machine learning solutions are helping industry solving problems in many areas, they are not immune to adversary attacks targeting the system.

This will be discussed in detail in section 2.

The solutions provided by enhanced connectivity using cloud, large volume of data collected from sensors as well as advanced data processing and visualization technologies is a breakthrough offering new and unique solutions in different areas.

The concept has affected the life cycle of new products from design stage to manufacturing and finally in the aftermarket phase in terms of asset integrity, increased reliability and energy efficiency.

In order to guarantee the automated function of the machines in Industry 4.0 Industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS) are used.

Collaborations between the end users, manufacturers, operators and service providers has also been affected in the form of using cloud platforms to share and store date. This, in turn, has created potential weak links in the manufacturing process as the systems will now be vulnerable to adverse effects of cyber-attack. Therefore, it is necessary to identify and acknowledge the system security weaknesses and address these using cyber security processes and techniques.

In order to be able to fully embrace the concept of Industry 4.0 and IoT, it is critical to make sure these technologies can provide sufficient data privacy and security as failure to achieve this on a practical level can have severe consequences, damaging several sectors of the industry.

2. Industry 4.0 applications

Industry four is now a widely used term in various applications such as supply chain management, Automation, additive manufacturing and 3D printing, smart factories, health care, smart equipment, robotics, digital design, condition monitoring, preventative maintenance and reliability.

2.1. Supply chain management

Supply chain management is a critical component in manufacturing. Strategies implemented in supply chain management govern how and when raw material will enter the plant , the quantity of raw , unfinished and finished material that need to be stored in the plant to meet the consumer demand while optimizing the cost and investment , as well as the vendors and distribution channels to be used in order to have a reliable , cost effective flow of product from factory to the end users [4].

Industry 4.0 has affected many scenarios when it comes to supply chain management. By using digitally interconnected platforms and receiving real time feedback from users as well as production and distribution lines, it is now much easier to predict the demand and balance the demand, production, raw material and resources more efficiently. At the same time, vendor and distribution network management has become much easier with the use of live and historical data stored in cloud platform provided from various locations [4].

2.2. Smart Equipment

Smart equipment is defined by three major characteristics: Networkability, transparency and functions and services [3].

Networkability allows provision of historic and real time process data via platforms such as cloud.

Transparency refers to availability and ease of access to equipment specific information such as specification, datasheets and manuals. This can be achieved via various apps and methods such as QR code.

A unique digital twin is created for each equipment in order to create an information source related to the specific equipment, specification, operation data (spare parts list, installation and operating manual) maintenance and service history.

According to AMFG Blog, the digital twin also represents the physical machine and allows for efficient simulation and optimization of the process based on the feedback received from sensors attached to the machine [19].

Smart equipment has unique functions as it can analyse data and make decisions and create control commands based on the live sensor information autonomously. This in turn, will decentralize the system intelligence [3].

2.3. Additive manufacturing and 3D printing

Additive manufacturing and 3D printing offer a valuable solution in areas such as reverse Engineering, medical devices and aviation components [19].

Computer Aided Design (CAD) files communicate detail design features with different machines such CNC machines and 3D printers which in turn makes it much easier to have local manufacturing plants with access to quick and cost-effective production methods in several locations[19].

3. Potential cyber security risks, attack methods and consequences

Cyber security plays an important role in mitigating the risks involved in the smart manufacturing and services in industry four era.

3.1. Cyber security Risk analysis in Industry 4.0 setting

Risk analysis requires deep understanding of two main sides of the emerging industry four trend: Operational Technology and Information Technology. It is necessary for the industry to review the requirements and risks in both aspects in order to identify and mitigate the risks involved.

Cybersecurity can be further classified into the following detailed categories [11].

- Network security: The aim in this category of the cyber security is to keep the network and communication safe with intrusion detection and neutralization methods
- Application security: Organizations need to ensure that the applications and software are safe from any malicious activity that can cause loss of data.

- End-user security: The key to end user security is raising awareness among end users regarding potential system weaknesses and data security best practices.
- Operational security: In order to keep the day to day function of an operation in Industry

4.0 era, it is critical to make sure that the data can securely flow in high volumes between different parts of the business structures.

Informational security: With the large volumes of data being stored and archived, it is now critical to make sure the databases are safe and will not be accessed by unauthorized parties.

- Cyber-attack recovery: After a system experiences a cyber-attack, it is critical to make sure that the operation is resilient enough to be able to recover the data and restore the operation functionality in a timely manner. Industrial shut downs can prove quite costly, therefore it is important that the a business has strategies to keep the down time due to a potential cyber attack at minimum [11].

As data sharing is the backbone of the new supply chain management system in the age of Industry 4.0, it is critical to make sure the data access is controlled efficiently with strategies in place to monitor and alarm unauthorized data access in all access points defined in the system [5].

In order to successfully carry out a comprehensive risk analysis activity in an Industy 4.0 settings, traditional risk analysis methods such as Failure Mode and Effects Analysis (FMEA) and the application of risk priority numbers (RPN) to digital assets can be used [10].

Industry 4.0 relies heavily on the concept of IoT, usage of smart gadgets and sensors on a large scale. Many of these devices are similar in structure and features. The similarity can be a major venerability when a weak feature is discovered and targeted by attackers. Such an attack will have a much larger impact on the industry. At the same time multiple data collection and data access points create an inherent venerability for such systems[5].

Another potential threat to the privacy and security of systems in the Era of Industry 4.0 is the everchanging nature of new technologies. As new technologies such as 5G emerge, affecting IoT and Industry 4.0, it is necessary to review and implement necessary data privacy and security strategies[5].

Attackers can also target the intellectual property of different businesses by getting unauthorized access to CAD (computer Aided Design) files via several communication nodes in the system and gain valuable information in terms of detail design features of a certain product in order to get leverage in the market.

System integrity attacks can also aim at gaining access to customer, finance or supplier information[10].

Loss of system functionality and manufacturing and delivery delays can also accrue if the availability of devices and services are threatened by denial of service attacks. This, in turn, can lead to incurring commercial penalties due to breach in delivery time stated in the sales contract as well as loss of sales [6].

3.2. Attack types

3.2.1. IoT device attacks

IoT devices are one of the weak links in terms of cyber security in Industry 4.0 setting. These devices are normally connected to the internet and other devices permanently creating a good opportunity for attackers to access the system through the IoT device.

The IoT devices normally communicate via HTTP requests. These requests contain a header section which has a URL address and a body consisting of the information to be sent to the server.

Attacks which work based on manipulating the URL section can be detected at the IoT device level , however, attacks which are carried out by changing the HTTP body , need to be analysed deeper and several comparisons needs to be made in order to correctly identify the attack , therefore , it is normally not possible to detect these type of attacks at the IoT device level [18].

Based on the discussion above, a distributed cyber security method addressing attacks on IoT level as well as

network and server level is best suited to address the attacks specific to IoT devices [18].

Figure 3 ([18], figure 1) shows the weak points in an IoT infrastructures where attackers might be able to get unauthorized access to the system.

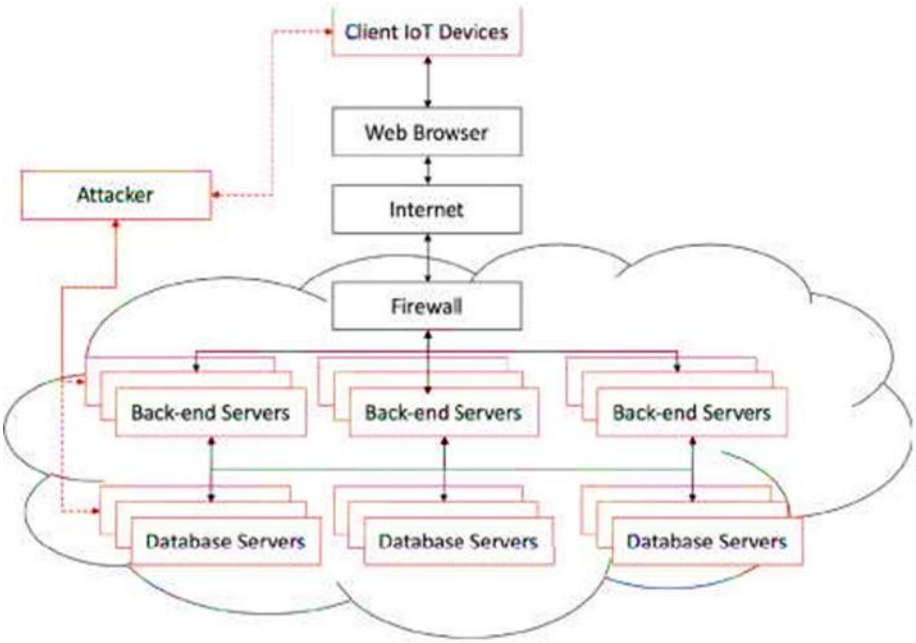

Figure 3. Vulnerabilities in different layers of a typical IoT infrastructure

Another type of attack targeting IoT devices are phishing attacks which aim to get access to personal, organizational or financial data by convincing the end user to reveal the username and password on a fake website or by downloading a malicious code [18].

As Industry 4.0 is relying more and more on smart PCS using Artificial Intelligence to carry out the tasks , the intelligence (which is created in training and testing phases) has become a main target for hackers via data poisoning attacks to adversely affect the decision making function of the PCS [8].

The fact that data is being collected in real time manner from various sources such as sensors, makes it more challenging for the PCS's internal security to assess the authenticity of the data and leave the PCS vulnerable to data injection attacks [8].

3.2.2. Vulnerabilities in SCADA systems

SCADA systems are used extensively in various industrial settings to collect data, control and monitor system status, facilitate communication between different sensors and automation components and create necessary alarm and error messages for the operators. The SCADA system normally includes a Human Machine Interface (HMI) , the intranet system which can be used for data collection and data analysis , the Master Terminal Unit (MTU) which is connected to remote terminal units (RTU) and collects and transmits data to and from equipment , sensors , actuators , motors and local controllers such as VSDs(variable speed drives). The field devices are installed in various (and sometimes remote) locations and usually consist of a local control device.

Figure 4 shows the different components of a typical SCADA system and the interactions between the different modules [8].

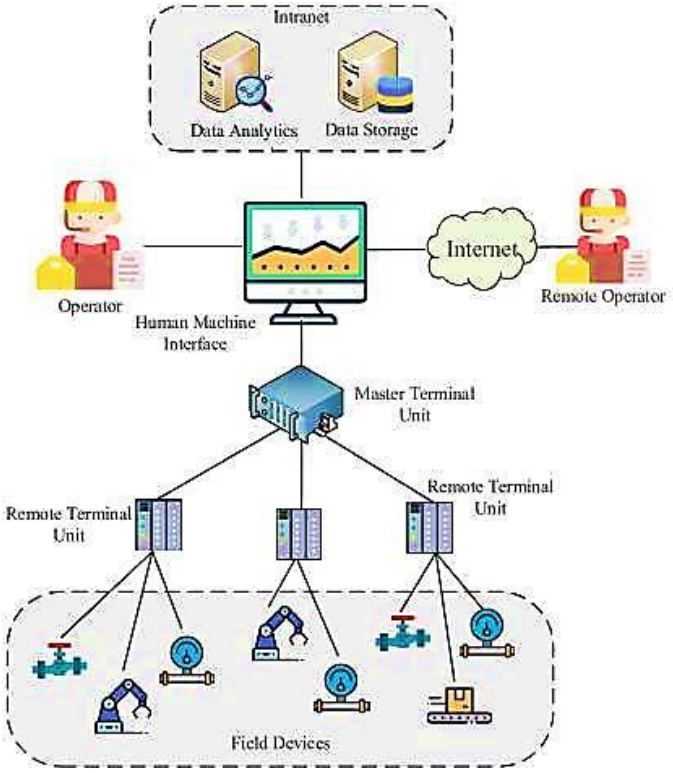

Figure 4: Typical SCADA system components [8].

Industrial control systems have been identified as the most critical components in terms of cyber security by (ENISA) (European Union Agency for Networked and Information Security (ENISA), 2018) .The private industrial networks interconnecting these devices and telecommunication protocols used in the process have major inefficiencies in terms of cyber security [7].

SCADA systems can be the target of several types of cyber-attacks. Some of the attack types are common between SCADA system and any other Network system, however, since SCADA systems are usually controlling critical industrial assets of many forms and importance level, the consequence of such attacks can be very serious and expensive. It is therefore important for the field device and local control manufacturers to be aware of the system vulnerabilities when such devices are used in the Industry 4.0 context. As an example, if a mining site loses the operation of one of its slurry pumping system for 24 hours, the financial damage can be as large as hundreds of thousands of dollars. If the attack is carried out in a manner that can cause physical damage to the asset, the financial damage can be multiplied as it can take several weeks to repair or replace a critical asset in an industrial plant.

In 2000, a disgruntled ex-employee of one of the Maroochy Shire council contractors in Queensland Australia successfully carried out an attack on a SCADA system controlling more than 140 sewage pumps. This has allegedly caused a large-scale spillage (close to 1 Mega Litter) of untreated sewage into the nearby river causing multiple environmental issues. The malicious control massages have been introduced to the pump station control system via wireless interface connected to the SCADA system. The attacker took advantage of the prior knowledge regarding the system telecommunication architecture as well as the system cyber- security and access control deficiencies [2].

Table 1 shows different types of attacks experienced by SCADA systems [2].

Table 1. Types of potential attacks in SCADA system

Attack	Targeted/Untargeted	Violated Objectives
Denial of Service	Targeted	Availability
Eavesdropping	Targeted	Confidentiality, Authorization
Man-In-The-Middle	Targeted	Authentication, Confidentiality, Integrity
System break-in	Targeted	Authentication, Authorization
Virus	Untargeted	Availability, Integrity, Confidentiality, Authentication
Trojan	Untargeted	Confidentiality, Authentication
Worm	Untargeted	Confidentiality, Integrity, Authorization

When Denial of Service (Dos) attacks are successfully carried over, the system will no longer be available, and the operation of the system will be negatively affected. Hackers can achieve this by using all available resources so that new requests could no longer be processed and responded by the system [8].

Eavesdropping normally happens in wireless communications where the attackers get access to confidential information by capturing the communication.

In order to target a system using the Man In the Middle method, the attacker will disguise as a legitimate user at a location between the communication nodes. The consequence of such an attack could be that the confidentiality of the information will be compromised as well as potential for system messages to be altered so that incorrect info to be injected into the system. This type of attack can be potentially harmful in Address Resolution Protocol where the system doesn't use any authentication routine, therefore, it is easy for any device connected to the network to disguise as a legitimate user [8].

In Section 3, we will investigate possible solutions to address the cyber security concerns in Industry 4.0 era with extra focus on the use of several machine learning algorithms, their advantages as well as the weaknesses and areas of concern.

4. Cyber security solutions for Industry 4.0 including machine learning solutions

Machine learning is a valuable tool that can offer a robust solution to data security threats in digital supply chain management by creating self-aware machines which can perform system health monitoring and prognosis independently [5].

In order to address the cyber security issues related to the cognitive nature of PCS such as data poisoning attacks which target the ML component of PCS, it is possible to use the common defence mechanisms used in adversary attack defence for any other machine learning process. These methods are aiming to increase the system resilience and robustness such as data sanitization and adversarial learning.

Also, in the initial stages of developing IoT applications, it might be quite expensive to come up with a strong cyber security solution. Therefore, new IoT applications are launched as pilot programs with open, but strictly monitored network connections. Once the system weaknesses are reviewed, addressed and removed, the application will be fully released [10].

One of the solutions suggested to address the cyber security concern by Dimitrov 2018 is designing Cyber Physical platforms which are able to identify the cyber attack and prevent them before the actual attack happens. In order to achieve this, the CPP needs to have an embedded fault diagnosis algorithm which works based on processing the fault symptoms.

The system will have a similar approach when it comes to dealing with faults and cyber- attacks, therefore, similar strategies used for fault diagnosis could be used for cyber threat detection.

The definition of the fault in any system is normally defined by measuring several system characteristics and comparing the measurements with the acceptable tolerance limits. Cyber- attacks create abnormality in some characteristic in the systems and therefore the same approach can be used to detect them.

The system will constantly monitor and analyse live data using this algorithm and will be able to detect and remove any cyber-attacks or potential cyber threats [7].

Fig.5 shows a diagram of different steps and strategies involved in such a platform. ([7], figure 3)

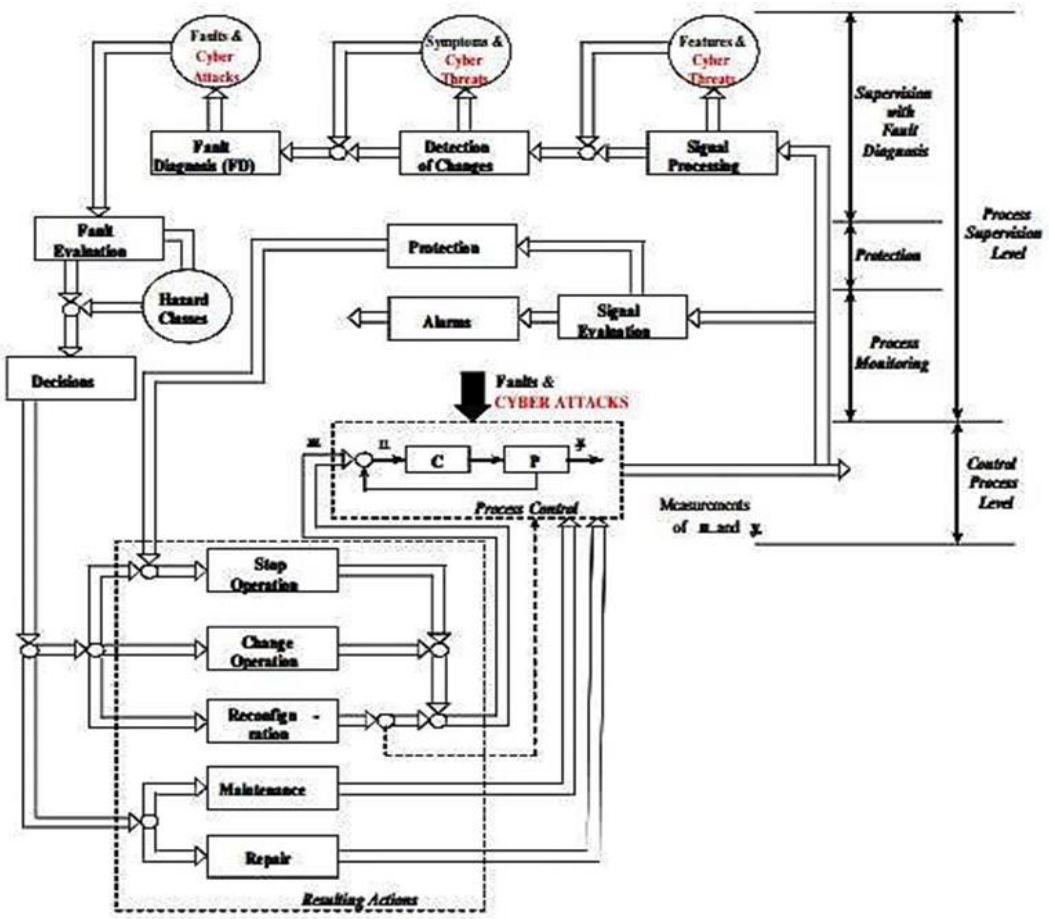

Figure 5. Generalized Algorithm for using fault diagnosis approach for identifying and removal of Cyber Threats and Cyber Attacks

4.1. Artificial Neural Networks (ANN)

One of the machine learning algorithms suggested by Dimitrov, 2018 to carry out the supervision and removal

of faults and cyber attacks is Artificial Neural Networks (ANN).

Artificial Neural Network is a collection of nodes / connection points that are heavily interconnected. The idea is loosely based on biological neurons or human brain. The collection of neurons normally consists of several layers where the information will flow in a single direction. A single node at any location is normally connected to several other nodes where it receives data from the nodes on layers before and then sends the data to the nodes located on the layers forward. Each of the connections entering a node will be assigned a "weight". Once the data is received it will be multiplied by the weight of the connection that the data is received from and then passed to the next layer.

At the beginning of any training phase, random weights will be assigned to each connection, as the model gets trained the weights will be adjusted to improve the performance of the algorithm and get similar predictions to the labels presented [12].

Some of the main characteristics which makes ANN a good candidate for cyber security tasks is the combination of ability to get trained on real time data as well as ability to process and match large amount of data simultaneously and produce data using pattern recognition feature. This is an important aspect of using ANN for Industry 4.0 applications as we are aiming to process variety of data from different sensors at the same time [7].

4.2. Fuzzy neural networks (FNN)

Fuzzy neural networks (FNN) can also be used alongside ANN to create a resilient cyber-attack defence system in Industry 4.0 [7].

Souza et al, 2020 define fuzzy neural networks as "hybrid structures that can act in several contexts of the pattern classification, including the detection of failures and anomalous behaviours."

The advantage of using a fuzzy neural network model is that we can represent quantitive labels such as small, medium, warm and cold using fuzzy elements. This is especially important when binary model cannot successfully simulate the problem. Using fuzzy features enables us to represent data with linguistic labels.

Souza et al, 2020 represented the anomaly detections results using a fuzzy neural network and compared the performance of the proposed algorithm with other conventional AI algorithms such as MLP, Random Tree and SVM . FNN has the best performance among all other algorithms even though the training dataset was quite imbalanced [13].

Figure 6 shows an example of fuzzy rules used to construct the model, the quantitive and linguistic nature of the rules is the main difference between FNN and other AI algorithms used in the Souza et al , 2020 research for comparison [13].

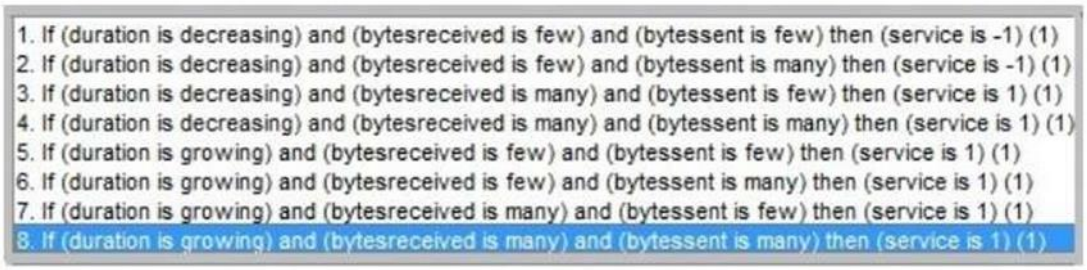

Figure 6. Fuzzy rules to construct a model for anomaly detection in cyber security application

4.3. Decision Tree

Decision tree algorithms have been successfully used for several cases in attack classification as well as intrusion detection activities. In order to train this algorithm , it is necessary to have a large labelled dataset to get the model familiar with the structure and features of different types of attacks, however, using this method system will be vulnerable to new types of attacks where no or limited training data is available. This issue can be partly overcome by constantly updating the model training to keep it up to date and ready to detect new types of attacks [11].

4.4. Support Vector Machine (SVM)

SVM algorithms can also be used as an efficient tool to perform cyber security tasks. SVM works based on constructing boundaries to classify the data. These models are usually used in intrusion detection applications. Similar to decision tree algorithm, this algorithm relies heavily on the data provided during the training stage to predict if an activity can be classified as "benign" or "threat". Therefore, the main disadvantage of using this model is that it is not autonomous and relies on human review and repeated training at certain time intervals in order to be efficient in detecting new types of attack.

4.5. K Nearest Neighbour

Another AI algorithm normally used for anomaly detection in cyber security is the K Nearest Neighbour which works based on measuring the distance between two data points. As anomalies normally have characteristics outside the acceptable limits and tolerances, KNN is an efficient model to detect them.

Bhuvaneswari in [15], also introduces several deep learning algorithms to be used in improving cyber security models. The advantage of using deep learning method compared to more conventional shallow learning methods is that the machine will only learn the highly relevant data and need less maintenance and human input once successfully commissioned. At the same time, deep learning methods are more time consuming and complicated and require more skills for developers in order to successfully design an efficient framework [11].

4.6. Using vector convolutional deep learning in IoT fog environment

Diro & Chilamkurti , 2018 proposed a distributed deep learning based IoT/Fog network attack detection system. The suggested artificial intelligence algorithm was successfully used for attack detection in an Industry 4.0 setting (in this case a smart city).

In a white paper published by Cisco in [16] , it is discussed that edge computing or fog computing is introduced in order to create an opportunity to analyse the time sensitive data in applications where analysing data in cloud is not efficient enough. The advantages of using fog environment for data analysis are:

1) Data can be analysed faster and closer to the were data is generated
2) System can respond to the collected data faster depending on the control philosophy 3- Ability to send selected amount of data to cloud for further analysis and archive instead of bulk data transfer

The method suggested by Diro & Chilamkurti in [21] is using a distributed model which divides the training and calculation load between the fog nodes and therefore it is possible for the system to classify the network traffic at fog layer and then send the attack incident to cloud for neutralization / removal of the attack.

The suggested method relies on an interconnected network of "master nodes" and "worker nodes" in order to create a distributed anomaly detection model and decrease the response time [7].

The master nodes in the fog system will collaborate and share the parameters and update and optimize them during the training process. The updated and optimized parameters then will be distributed among the worker nodes. The distributed nature of the proposed method makes it more efficient. The suggested algorithm's performance was compared to some of the conventional attack detection methods (centralized and distributed) such as SVM , Naïve Bayesian and RNN. The result showed that the suggested approach has similar or in cases better performance compared to some of the state-of-the-art methods in network traffic anomaly detection [7].

4.7. Deep Belief Networks (DBN)

Deep Belief Networks (DBN) is one of the deep learning algorithms which can be used in cyber security. DBN is an unsupervised machine learning model consisting of several layers with hidden units which are interconnected to each other.

As DBN is capable of training one layer at a time, the computational load on the system remains minimal during the training stage. DBN is capable of autonomously enhancing and optimizing itself, therefore it has a

main advantage when compared to supervised shallow learning models. At the same time, the autonomous unsupervised training of the model can diminish the algorithm's performance as bias may be developed over time. In order to address this issue, it is possible to use increased layers which prevent development of bias.

DBN models have been successfully used on NSL-KDD datasets achieving high detection rate as well as excellent accuracy in detection data injection incidents [11].

4.8. Recurrent neural network (RNN)

Thanki et al 2019 define RNN or feedback neural network as a type of ANN model, in which the outputs from neurons are used as feedback to the neurons of the previous layer. In other words, the current output is considered as an input for the next output. The concept is illustrated in figure 7 [17].

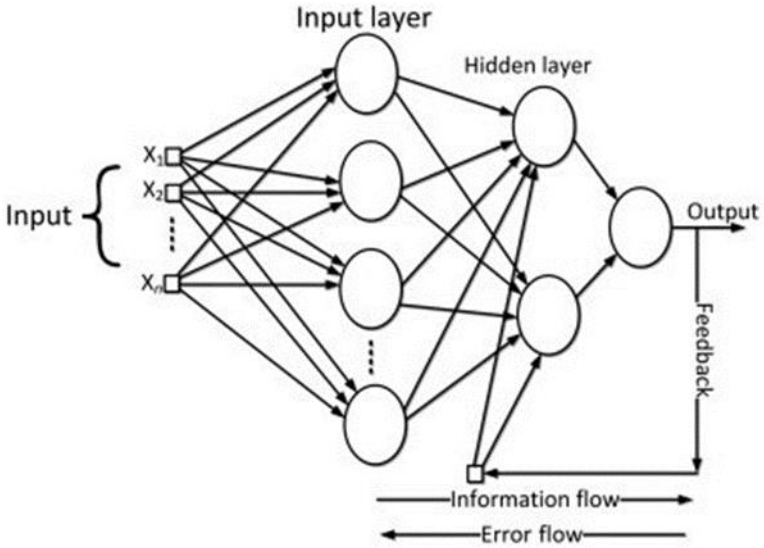

Figure 7. Flow of information and feedback in RNN

Recurrent neural network has some enhanced abilities in terms of analysing data with variable lengths compared to other traditional neural network. At the same time, the training process of this algorithm is complex due to the complex architecture and layer arrangement of RNN algorithm [11].

Recently researches have focused more on using the RNN algorithm in cyber security applications.

According to Alghamdi, 2020 RNN model can offer different solutions in various cyber security areas such as traffic analysis, malware, and intrusion detection. This method of deep learning uses the technique of random temporal projection to extract full information from the data and use it to secure the systems against malware and intrusion]. RNNs also analyses the patterns of the data by communicating between multiple layers and elements at a time to reach an accurate result. Thus, by carrying out an extensive analysis and learning of data, RNNs gain the ability to fight against various cyber threat. Also, they have a feature of predicting the patterns for the future, which also makes them effective against unknown ways of intrusion.

4.9. Convolutional neural networks (CNNs)

Alghamdi, 2020 presented a cyber security model built based on Convolutional neural networks (CNNs).

CNN is a neural network, based on deep learning method. This method structures the data in the form of arrays. These arrays enable the classification of the data systematically separating the classes according to their properties.

CNNs are highly effective in structuring the data based on their spatial and temporal properties. Thus, making the process of learning easier.

The learning model in CNN can be divided into three section [11]:

1) Convolution layer which is effectively the core layer of this model. This layer is defined the weights of the original input of the data. The results of the convolution layer are passed through a feature map to develop physical or temporal relationships within the data.
2) Pooling layer which is capable of reducing the size of the feature maps by using a nonlinear down sampling method. This ability allows storing a large memory in a small space and improves the training process.
3) Classification layer

CNNs are using "dropout" technique for training. This technique enables the model to perform iterations, which removes the irrelevant information from the layers, making the model highly effective for the cybersecurity applications. Dropout also enhances the accuracy and generalizability of models, making them highly efficient at identifying unusual behaviour]. Also, these models are self-learning models that learn from the experiences and patterns available in the data, which makes them highly effective against malware and intrusion. However, this method of deep learning is complex and time-consuming, which limits its use in some of the cybersecurity systems [11].

4.10. Multi Layer Perceptron (MLP)

Susilo and Sari in [14], define a Multilayer perceptron as a feed forward neural network that has a number of neurons or nerves that are connected with other neurons with connecting weight neurons, where every neuron that exists is a unit that has the task of processing and calculating the activation value, which symbolizes the set of predecessors of each unit from input to output or from one unit to another unit .

Using MLP algorithm, Susilo and Sari, 2020 has been able to construct a model to successfully identify attacks with high performance.

4.11. Random Forest (RF)

Random forest has been traditionally used in different classification applications.

Susilo and Sari, 2020 conducted an experiment using RF, CNN, and MLP algorithms on as a dataset called the BoT-IoT. The dataset was created by constructing a surrounding system at the Cyber Range Laboratory in the UNSW Canberra Cyber centre. The environment was made by combining normal traffic and botnets. Random forests and the CNN provided the best result in terms of accuracy and the AUC for multiclass classification.

4.12. Cyber-attack defence specialized for SCADA systems

SCADA attack detection solutions can be divided into three categories as per Pliatsios and Lagkas , 2020.

4.12.1. Traffic classification

In this method different machine learning algorithms can be used to monitor the network traffic, detect anomalies and raise alarms for attacks to be removed. The first step or training requires a large labelled dataset of network activities clearly labelled "normal" or "attack" . Once the training phase is successfully completed, another set of data with known labels will be fed to the algorithm. This time, the labels will not be presented to the algorithm but rather algorithm "predicts" the labels based on the observation and learning activity don on the previous stage. This phase is called the testing phase. Once the predicted labels are produced by the algorithm, they will be compared with the known labels in order to get some measurements on the algorithm's performance [15].

Neural network and k-nearest neighbour are a few examples which have been successfully implemented along with other methods to address the cyber security issue in SCADA system by developing efficient autonomous network monitoring systems. These systems need to be constantly reviewed and updated to increase their adaptability [9].

4.12.2. System variable inspection

Carcano et al, 2011 introduced a new formalized language called Industrial State Modelling language (ISML). The main objectives of introducing ISML was a) to provide a detailed description of the system to monitor, which

will be used to generate the virtual system used by the Intrusion Detection System and b) to describe a particular class of system states called Critical States that is a hazardous or undesirable situations in the system. For each Critical State, a risk level will be identified. The risk level 1 is related to a low risk critical state). The value 5 corresponds to a critical state dangerous for the system. Depending on the system characteristics and application, each system condition will be defined in the system as well as constraints and formulas for evaluation if a condition should be considered as "critical state condition" [9].

Carcano et al, 2011 suggested creating a virtual image of the monitored system using ISML and a State Evolution Monitoring (SEM) software which screens the system states. The virtual image will be periodically updated to make sure the virtual image is as close to the physical system as possible. If the system status in the SEM matches the critical system status, an alarm will be raised [9].

In order to make sure risk of Eavesdropping attacks are removed from SCADA systems, it is possible to use encrypting algorithms to encrypt the messages.Man in the Middle attacks can be neutralized and removed by providing authentication for messages as well as establishing certificates in the connection points [7].

4.12.3. Attack detection

Pliatsios and Lagkas, 2020, Introduce a multi-layer cyber security framework for SCADA cyber security. The main benefit of using such a system is that it can detect attacks performed from inside the SCADA network as well as attacks carried out by hackers from outside the network. The proposed system works based on three of three characteristics: 1) access-control whitelists; 2) protocol-based whitelists; and 3) behaviour-based rules.

The access-control whitelist includes detectors in the layers 2-4 of TCP/IP model, namely Data link, Network / Ethernet and Transport. If an address or port is detected which is not included in the whitelist, an alarm will be raised in the IDS.

Protocol based whitelist approach, monitors layers 4-7 of the TCP/ IP and is related to specific telecommunication protocol used. If any communication between the components is not complying to the telecommunication protocol used in the system, it will create an alert message [8].

5. Conclusion

Industry 4.0 represents new and unique solutions in different industry sections and applications, with the large scale adoption of Industry 4.0 concepts , it is now critical to make sure cyber security systems are up to date and robust enough to keep up with the industry trend and advancements in device connectivity.

Cyber security plays an important role in mitigating the risks involved in the smart manufacturing and services in industry 4.0.

SCADA system is another critical component currently used in many Industry 4.0 settings. The risks involved in SCADA system cyber security can be critical. The potential consequences of a cyber attack accessing the SCADA system can be of a large scale, affecting and disturbing sensitive, critical infrastructure.

Machine learning is a valuable tool in ensuring cyber security in Industry 4.0 components. Supervised machine learning algorithms such as decision tree , KNN and SVM have been successfully used for cyber security tasks such as anomaly detection in network traffic , however, these algorithms need to be constantly reviewed and re-trained in order to remain efficient when dealing with new types of attacks.

Using deep learning algorithms such as ANN , FNN , RNN and CNN for cyber security purpose is gaining popularity due to the fact that they enable autonomous system updates and their ability to analyse different types and lengths of data .However, according to Alghamdi, 2020, these algorithms normally have a complex architecture which makes the training process difficult , therefore more research needs to be done in this area in order to take advantage of the unique potential deep learning algorithms can offer to cyber security solutions.With the concept of Industry 4.0 closely related and relying on IoT , we witness using smart devices in various settings at large scale , therefore , it is also important to consider the distributed attack detection approach at different layers in order to share the computational load and increase the cyber security system efficiency.

Depending on the application, after careful consideration and thorough risk analysis practice, it might be necessary to use a combination of several types of artificial intelligence algorithms to address the security concerns inherent to each environment.

References

1. Ervural , B.C., Ervura,B 2018 'Industry 4.0: Managing The Digital Transformation', Chapter 16, retrieved 12 September 2020. <https://www.researchgate.net/publication/319861803_Overview_of_Cyber_Security_in_the_Industry_40_Era >.
2. Prinsloo, J, Sinha ,S and von Solms B 2019 ' A Review of Industry 4.0 Manufacturing Process Security Risks'.
3. KSB SE & Co. KGaA , 2018 ,' Industry 4.0: We have experience with the future' , retrieved 14 September 2020.
4. Waslo , R, Lewis T, Hajj, R, Carton R , 2017, ' Industry 4.0 and cybersecurity Managing risk in an age of connected production' , retrieved 19 September 2020.
5. Tawalbeh, L, Muheidat , F, Tawalbeh , M and Quwaider , M , 2020 ' IoT Privacy and Security: Challenges and Solutions'.
6. Corallo, A, Lazoi, M, Lezzi, M, 2020 'Cybersecurity in the context of industry 4.0_ A structured classification of critical assets and business impacts', Elsevier , Computers in Industry 114 (2020) 103165.
7. Dimitrov ,K 2018 'Cyber Defence in Industry 4.0 Systems and Related Logistics and IT Infrastructures', NATO Science for Peace and Security Series D: Information and Communication Security - Vol. 51 , IOS Press , Amsterdam, Netherland.
8. Pliatsios , D, Lagkas ,T 2020,'A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics', IEEE Communications Survey & Tutorials , VOL. 22, NO. 3, Third Quarter 2020.
9. Carcano, A, Coletta, A, Guglielmi, M, Masera, M, Nai Fovino, I , and Trombetta , A, 2011, 'A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems', IEEE Transactions on Indstrial Informatics, VOL. 7, NO. 2, May 2011
10. Culot, G, Fattori , F, Podrecca , M, and Sartor, M , 2019 , 'Addressing Industry 4.0 Cybersecurity Challenges', IEEE Engineering Management Review , VOL. 47, NO. 3, Third Quarter, September 2019.
11. Alghamdi, M , 2020 , 'Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security '.
12. Hardesty, L , 2017 ,' Explained: Neural networks. Ballyhooed artificial-intelligence technique known as "deep learning" revives 70-year-old idea' , MIT News office , retrieved 25 September 2020 .
13. Souza , P , Guimarães , A, Rezende , T , Arauju, V, 2020, ' Detection of Anomalies in Large- Scale Cyberattacks Using Fuzzy Neural Networks' , AI. 1. 92-116. 10.3390/ai1010005.
14. Susilo, B, and Sari , R , 2020'Intrusion Detection in IoT Networks Using Deep Learning Algorithm'.
15. Bhuvaneswari Amma , N.G. and Selvakumar , S. , 2020 , ' Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment' , Elsevier , Future Generation Computer Systems 113 (2020) 255–265.
16. Cisco White paper , ' Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are' , Retrieved , 01 October 2020. ,<https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf> 17- Thanki R and Borra, S , 2019 , ' Machine Learning in Bio-Signal Analysis and Diagnostic Imaging' , Academic Press.
17. De La Torre Parra,G, Rad, P, Choo, K, Beebe, N , 2020, 'Detecting Internet of Things attacks using distributed deep learning', Elsevier, Journal of Network and Computer Applications 163 (2020) 102662.
18. AMFG Blog, 2019,'Industry 4.0: 7 Real-World Examples of Digital Manufacturing in Action' , retrieved 14 September 2020.
19. Boulilia , N 2018, 'Guidelines for Modeling Cyber-PhysicalSystems – A Three-Layered Architecture forCyber Physical Systems' , Technical Report , Siemens Corporate Technology , retrieved 12 September 2020.
20. Diro , A, and Chilamkurti , N, 2018, ''Distributed attack detection scheme using deep learning approach for Internet of Things' , Elsevier , Future Generation Computer Systems 82 (2018) 761–768.
21. Cotteleer , M , Sneiderman, B 2020, 'Forces of change: Industry 4.0', retrieved 12 September 2020.