INTERNATIONAL CONFERENCE RCIC'20
*Redefining Community in Intercultural Context*
Cluj-Napoca, 7-9 May 2020

# A REVIEW OF MACHINE LEARNING TECHNIQUES FOR THE CYBERSECURITY OF CRITICAL INFRASTRUCTURES

**Alexandru STANCIU*, Vladimir FLORIAN*, Ella-Magdalena CIUPERCA*, Carmen Elena CIRNU***

Critical Infrastructure Protection, National Institute for Research & Development in Informatics, Bucharest, Romania

***Abstract:*** *An essential component of the National security consists of the protection of its critical infrastructures (CIs), whether they are physical or virtual, as any disruption of their services could have a serious impact on economic well-being, public health or safety, or any combination of these. Any shutdown or delay may determine financial losses and major risks to people and the environment. All modern CIs are controlled by Industrial Control Systems (ICS) being dependent on their correct and continuous undisturbed functioning. Modern ICSs are inherently much less secure and exposed to the majority of cyber-attacks that are becoming more advanced and sophisticated. Consequently, efficient tools for the protection of hardware and software components of ICSs are required. One such class consists of intrusion prevention and detection systems (IPDS). Contemporary IPDSs use machine learning algorithms to detect threats manifested as anomalous behavior of a particular system. To provide robust detection systems with sufficient layers of protection, these must be combined with other methods and extensively tested with good datasets and using appropriate testbeds. Recent research suggests that conventional intrusion detection approaches are unable to cope with the complexity and ever-changing nature of industrial intrusion attacks. Moreover, deep learning methods are achieving state-of-the-art results across a range of difficult problem domains. The objective of our paper is to identify and discuss machine learning-based intrusion detection and protection methods and their implementation in industrial control intrusion detection systems, able to contribute to ensuring national security.*

***Keywords****: critical infrastructures; industrial control systems; cybersecurity; machine learning*

## 1. INTRODUCTION

All modern critical infrastructures (CIs) are controlled by Industrial Control Systems (ICS) being dependent on their correct and continuous undisturbed functioning. ICSs are inherently much less secure and exposed to the majority of cyber-attacks that are becoming more advanced and sophisticated. Consequently, efficient tools for protection of hardware and software components of ICSs are required. One such class are intrusion prevention and detection systems (IPDs).

Contemporary IPDSs use machine learning algorithms to detect threats manifested as anomalous behavior of a particular system. To provide robust detection systems with sufficient layers of protection, these must be combined with other methods and extensively tested with good datasets and using appropriate testbeds.

Recent research (Wilson *et al*., 2018; Yang *et al.*, 2019) suggests that conventional intrusion detection approaches are unable to cope with the complexity and ever-changing nature of industrial intrusion attacks. Moreover, deep learning methods are achieving state-of-the-art results across a range of difficult problem domains. The objective of our paper is to identify and discuss cybersecurity vulnerabilities for ICSs, as well as proposed solutions that mitigate the threats, their inherent limitations that affect implementation in order to support industrial control intrusion detection systems, able to contribute to ensuring the security of CIs. Section 2 highlights the threats to which control systems are exposed today. Considering this landscape, Section 3 addresses the search for defense techniques against APTs, especially intrusion detection systems. Finally, machine learning techniques for

intrusion detection systems, as well as the application of these mechanisms in practice, are presented in Sections 4 and 5, respectively.

## 2. SPECIFIC VULNERABILITIES OF INDUSTRIAL CONTROL SYSTEMS

A cyber-attack is an attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an information system, infrastructure, computer network, or other computing devices of a system that is executed by means of cyberspace (www.iso.org).

A cybersecurity threat is a potential successful cyber-attack that could lead to gaining unauthorized access, damage, disruption, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. It also refers to the malicious activity that seeks to damage data, steal data, or disrupt digital life in general (https://www.upguard.com/blog/cyber-threat). The first step to tackling the cybersecurity threats consists in understanding where attacks can come from, how the attacks are enabled, and what damages could produce.

Cybersecurity vulnerabilities have several different, but similar definitions in the literature. For example, Internet Engineering Task Force (IETF) defines vulnerabilities as "flaws or weaknesses in a system design, implementation, or operation and management that could be exploited in order to violate the system's security policy" (RFC 4949). Analogously, the National Institute of Standards and Technology (NIST) promotes the following definition: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (NIST, 2020). Consequently, a vulnerability can be seen as a specific instance of a weakness and can be found in either software, hardware, a network or inside an organization.

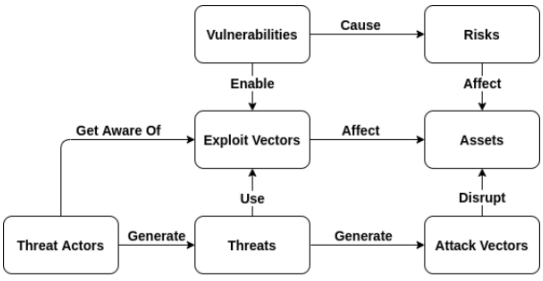


Figure 1. Cybersecurity Concepts Taxonomy (*apud* Atif *et. al*, 2018)

When talking about malicious code such as viruses or worms, a vector represents the pathway used by that code to propagate itself or infect a computer. In the cybersecurity domain, an attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network.

The threat, risk, asset, and vulnerability are the main concepts of a cybersecurity taxonomy developed by Atif *et. al* (2018).

According to this taxonomy (fig. 1), vulnerabilities cause the appearance of exploit vectors. Threat actors get a certain level of awareness about those exploit vectors and use them to generate threats.

Threats generate attack vectors that could disrupt the infrastructure assets. Vulnerabilities induce risks to the assets by allowing temporary or permanent functioning disruptions.

Macaulay (2016) distinguishes vulnerabilities and threats based on whether an action has been taken. A threat appears when a person, group or thing is acting, whereas a vulnerability exists as a flaw in a system. While the attack vectors are known, vulnerabilities are dynamic and cyber assets must continuously be monitored and assessed. In order to develop appropriate mitigation actions, it is necessary to understand how the Operational Technologies (OT) environment can be accessed and what impacts can be achieved.

The main challenge present in the modern Industrial Control Systems (ICS) is due to the dual nature of their composing technologies (Amoroso & Ginter, 2018). On one side, Operational Technologies (OT), consisting of hardware and software that detects or causes changes in physical processes through direct monitoring and/or control of industrial equipment. On the other side, conventional ICT components connected with the corporate business information systems and the internet. The two different interface types can be related to different forms of vulnerability: degradation of communications or degradation of I/O control.

In order to ensure the exchange of information with both IT and OT systems, Industrial Control System (ICS) component devices must provide both types of access points and connection capabilities across the ICS network or system interfaces. This is the main pathway of malicious actions on ICS. Firstly, besides classical security threats, conventional IT hacking tools and techniques become able to reach proximity to OT devices. Then, because the OT devices are not protected, an attack on OT control or the device directly could be executed (Amoroso & Ginter, 2018).

Macaulay & Singer (2011) when dealing with ICS vulnerabilities, have classified them from the perspective of security controls. They identified the following categories of security vulnerabilities: management (business), operational, and technical types. Management vulnerabilities are due to human flawed decisions and are basically deficiencies in enterprise risk management in ICS. They include: the lack of ICS security policies, management-level accountabilities and guidance and also bad security investment budgeting.

ICS operational vulnerabilities consist in weaknesses the procedures and policies, like improper separation of duties for administrative accounts and roles, insecure Internet communication channels and wireless system deployments. There are also: improper incident detection, response, and reporting, poor change management, and poor vulnerability and acceptance testing procedures.

Technical vulnerabilities are due to security weaknesses in hardware, software, and networks (Macaulay & Singer, 2011, Calvo et al., 2016) detailed a comprehensive synthesis of these. Accordingly, the following categories can be identified: (1) Platform and applications vulnerabilities, (2) Network vulnerabilities, (3) Vulnerabilities related to Communication Protocols.

Platform and application vulnerabilities are deficiencies and flaws found in hardware, software and malware protection software of the system. They include: usage of outdated equipment and software; usage of default settings in applications; absence of backups of the critical configurations; inappropriate security configuration for remote access; inadequate authentication control at equipment and software level; software components containing errors that produce buffer overflow situations or resource unavailability due to traffic flooding (Denial-of-Service); missing or inadequate malware protection measures; improper configuration of the operating system; flawed designed applications.

The main network vulnerabilities (Calvo et al., 2016) are: ill-designed network architecture without adequate security measures; lack of backup or/and storing network settings; absence or poor authentication mechanisms at the protocol levels; bad management of network passwords; lack of network traffic monitoring; use of nonencrypted protocols (e. g. Telnet, FTP or wireless connections); lack of integrity checking at the hardware device level.

Another major vulnerability in an OT/IT infrastructure is enabled by allowing critical and non-critical components to communicate across shared mechanisms such as a fieldbus. So, vulnerability paths to remote control are opened and hacks can occur even in the presence of proper network security controls.

## 3. SPECIFIC THREATS AND CYBERSECURITY TOOLS

As opposed to cyber-attacks against IT systems, usually oriented on data theft or financial loss, cyber-attacks against OT systems additionally focus on the disruption of cyber assets. They focus on operational impact trying to achieve loss, denial, or manipulation of view, control, safety, or sensors and instruments. According to (Ani, He & Tiwari, 2017) threats fall into one of six categories: (1) Denial of view (DoV), (2) Loss of view (LoV), (3) Manipulation of view (MoV), (4) Denial of control (DoC), (5) Loss of control (LoC), and (6) Manipulation of control (MoC).

A DoV is caused by a temporary communication failure between a device and its control source, resolved when the interface recovers and becomes available. The reception of status and reporting messages is temporarily blocked. Thus, operator visibility is denied preventing him from noticing a change in state or anomalous behavior. It increases the risks of incorrect or damaging behaviors.

A LoV results from a sustained or permanent interface communication failure and requires local hands-on user intervention. The impact of this threat is similar to DoV, but more severe because of the effort required to bring the system back to the expected functioning state.

MoV is an attempt to manipulate the information reported back to the operator or to controllers. Harmful actions are enabled via information distortion (falsified ICS data) transmitted to the operator or controller. This manipulation may be short term or sustained.

DoC is a threat to temporarily prevent the operator from controlling the processes and (or) devices. The affected process may still be operating during the period of control loss, but not necessarily in a desired state. The threat targets control devices, I/O control interface functions and only gets recovered as soon as it is removed.

A LoC condition appears when the operator could be prevented from issuing any commands even if the malicious interference has vanished. The impact of LoC is similar to the impact of the LoV, but recovery can only be achieved via the operator’s interventions, such as system rebooting.

MoC, the most critical threat, appears when control system devices are controlled and altered by malicious actors. Manipulation of physical process control within the industrial environment becomes possible, legitimate process instructions, and operator commands can be overridden. The duration of manipulation may be temporary or longer sustained, depending on operator detection. Methods of Manipulation of Control include: Man-in-the-middle, spoof command message, changing setpoints.

Starting from mid 2000s, a new type of cyberattack, the advanced persistent threat (APT) has posed an unprecedentedly dangerous threat to CIs. APTs are a category of cyber threats that are malicious, organized, highly sophisticated in their use of tactics, techniques and procedures (TTPs) and target IT networks for long-term access, in order to obtain information or sabotage one organization operations. As stated by NIST (Chen et al., 2014), their source is "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)".

Apart from traditional threats, the distinguishing characteristics of an APT are: it pursues its objectives repeatedly and for a long time, it adapts to defending actions by using stealthy and evasive attack techniques and "it maintains the level of interaction needed to execute its objectives".

APTs consist of a complex of actions, their life cycle including preparatory, acting and persisting stages. In Chen *et a*l. (2014), one of the most detailed description, an APT contains six stages: (1) reconnaissance and weaponization; (2) delivery; (3) initial intrusion; (4) command and control; (5) lateral movement; (6) data exfiltration. First stage is intelligence gathering, mainly relying on the internet, active scan, and social engineering methods. Second and third stages cover the access and invasion into the target network through phishing emails, SQL injection, mobile storage devices and any other methods. In the fourth stage, remote control, by installing back door programs or Trojan programs, attackers control the user infrastructure and keep communication with the control servers via the network communication protocols. Next stage is lateral movement, attackers use vulnerability scanning, listen to network traffic for password, embedded remote control tool (RAT) and other methods, continue to search for important computers which store sensitive information. The final stage is data theft or system damaging by sending back sensitive data to servers or controlling devices.

Besides raising risk awareness to these new categories of threats, an additional effort is needed to mitigate the risks posed by these threats in the ICS domain. This implies using a complex of measures and tools for the effective detection of APTs and other sophisticated threats. These should include combining traditional countermeasures (e.g., intrusion detection systems, firewalls, antivirus) with novel security techniques.

When focusing on the OT domain of the ICS architecture, several specific security tools can be identified. From the perspective of their main functionality, these can be included in one of the following categories (Hurd & McCarty, 2017).

*Detection of the Indicator of Compromise (IOC).* IOC is a forensic artifact, observable on the network or host, that indicates a computer intrusion with high confidence. IOC examples include: signatures of known malware, traces of malicious network traffic and URLs or domains that are known malware sources. IOCs are directly linked to measurable events. A tool in this category is able to detect all malicious data generated by such events.

*Network Traffic Anomaly Detection*. Network traffic anomaly detection tools are based on the statistical properties of the network where they are used. These properties refer to IP addresses, ports, frequencies of communication, packet content, etc. Anomaly detection does not necessarily require updates when new threats are detected. An anomaly detected on the network is, by definition, a new threat or a false positive. An anomaly detection tool should be able to be trained on a network for normal traffic, and then to use that model to determine anomalous traffic.

*Outlier Analysis*. Tools in this category have the ability to analyze anomalous data for future threat intelligence. This data is usually identified by searching for meaningful differences across large datasets spanning many hosts that share common configurations.

*Log Review*. Log review is the process of analyzing computer generated records of internal events, including a temporal reference. A log review tool does anomaly analysis within the logs in order to identify areas of interest in a log file or correlates different logs into a timeline of event activity. Other functionalities can include the removal of uninteresting data while maintaining the integrity of the log file.

*System Artifact Review*. A system artifact review tool analyzes system artifacts that are created as a byproduct of execution. These could include registry files, data files, memory resident information, environment variables, or similar.

This tool should be capable of extracting all possibly useful information from the analysis and storing it for future execution.

*Reverse Engineering (RE) Analysis*. A RE analysis tool extracts information from a given set of data. The data sources include files and/or firmware of a device and also network traffic. The tool is able to decompose software and firmware architectures and to display the information in an easy understandable structure that facilitates the RE process.

The objective of an Intrusion Detection System (IDS) is to correctly detect attacks against networks with the lowest possible number of false positives. Recently, new anomaly-based detection techniques using machine earning have been used. Even in the research phase, many of them could provide satisfactory results, as regular ICS traffic is related to a limited number of requests and responses, making it clearly different from malicious traffic.

## 4. MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION SYSTEMS

Machine learning techniques are suitable to be applied in various domains where is a need for adaptation to different types of data, as they provide an efficient way to learn a nonlinear system without the need to use a physical model.

Specifically, for ICSs, in order to mitigate the security aspects related to the operation of the CIs, intrusion detection mechanisms need to be employed to protect against malicious attacks. Among the most acute security problems that affect the ICS, one of the most prominent is related to the legacy communication protocols that were not designed with security as a priority, but rather to optimize the performance and provide functionalities. Moreover, insecure deployments are caused by a lack of specific network segregation and access control mechanisms.

In general, an IDS could be conceived as anomaly or signature based. The former is implemented using algorithms that calculate deviations from the normal behavior of the system, while the latter makes use of signature databases or known patterns in order to identify an intrusion.

Another detection approach uses model-based techniques that characterize the acceptable behavior of the system and detect attacks that cause unacceptable behavior. These types of methods are applicable for detecting an intrusion based on the analysis of the network protocol (e.g. Modbus) or the network infrastructure, however they are of limited use because in practice it is difficult to construct such models. Moreover, as these models are not very accurate (as it is very difficult to capture all possible operating scenarios), this approach could cause many false alarms.

The main task of anomaly detection systems is thus to monitor the network traffic or the parameters of the production installations in order to detect suspicious activity and to alert on possible attacks. The signature-based intrusion detection systems work well to recognize patterns that were already provided to them, however they are not so efficient for novel attacks or patterns that were not seen previously. Instead, an anomaly-based IDS is capable of learning new standard profiles and then to update its model such that new behavior can be learned and classified.

The information about the network traffic and installation operation statistics is provided by management tools that monitor the system hardware and the communication links, such that the traffic can be characterized as normal or anomalous based on specific detection methods like pattern matching which detects anomalies by analyzing deviations from normal behaviors. In this case, the normal traffic of the system is used to build a model for normal behavior. In addition, usage profiles are created for different scenarios, using system parameters such as CPU utilization, network bandwidth, or processes in memory. These profiles are then used to evaluate if a particular data traffic pattern fits a predefined type, which could indicate an anomaly or a possible intrusion.

However, anomaly detection in ICS is a challenging problem and it cannot solely depend on network protocol information. Additional information related to physical processes needs to be examined. This significantly increases the dimensionality and complexity of data samples. In addition, physical process control variables may exhibit noisy behaviors by nature, which is likely to result in high false-positive rates for anomaly detectors and low detection rates of attacks. There are several limitations with most existing solutions, as presented by (Feng et. al., 2017): the majority of the methods rely on predefined models and signatures to detect anomalous behaviors, and this approach requires human effort, which is inconsistent and error prone. These models are not capable of detecting unknown attacks because they use only known signatures, and they are specifically designed for specific use-cases, and lack the flexibility to adapt to new systems.

Nonetheless, machine learning is an essential component of the cybersecurity domain, as it is used in malware detection, events classification, and alerting. It is critical for the identification of infrastructure vulnerabilities and exploits (Fraley & Cannady, 2017).

## 5. APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY

Anomaly based intrusion detection techniques are capable of identifying unknown attacks as they follow the normal behavior of the system and observe any deviation from that baseline, and can be customized to different systems and network types (Xin *et al.*, 2018).

Advanced machine learning techniques such as Deep Learning have been widely applied to various application domains such as image processing, natural language processing or speech recognition. In the area of cybersecurity, numerous approaches have been proposed to tackle intrusion and malware detection, as well as phishing or spam detection (Mahdavifar & Ghorbani, 2019).

For example, Bakalos et al. (2019) proposed an attack detection framework for critical water infrastructure protection based on multimodal data fusion and adaptive deep learning. Their solution is based on tapped delay line convolutional neural network (TDL–CNN), which contains a deep CNN with autoregressive moving-average attributes, that allows the model to better adapt to dynamic attack characteristics.

A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system networks using Deep Belief Network (DBN) was proposed by (Huda et al., 2018). This system is based on two different types of deep learning based detection models - a disjoint training and testing data for a DBN and corresponding artificial neural network (ANN), and a DBN which is trained using new unlabeled data that can provide additional knowledge about the changes in the malicious attack patterns.

While many existing solutions rely on human-defined features to develop machine learning based attack detectors against prominent exploits, such features are becoming more expensive and less effective. To supplement more high-quality features for machine learning based threat monitoring, Wilson, Tang, Yan & Lu (2018) proposed a stacked autoencoder (SAE) based deep learning framework to develop machine-learned features against transmission SCADA attacks. Compared with the state-of-the-art machine learning detectors, the proposed framework leverages the automaticity of unsupervised feature learning to reduce the reliance on system models and human expertise in complex security scenarios.

In He, Mendis & Wei (2017), a real-time detection mechanism based on deep learning techniques was introduced. This system is capable of recognizing the behavior patterns of False Data Injection (FDI) attacks using the historical measurement data. Deep learning techniques are used to capture the higher-order statistical structure of the complex data by arranging the feature detectors in layers. A Deep Belief Network is constructed with a stack of Restricted Boltzmann Machines (RBMs) in order to extract high-dimensional temporal features. This DBN architecture is designed to analyze the temporal attack patterns that are presented by the real-time measurement data from the geographically distributed sensors/meters.

Instead of relying on hand-crafted features for individual network packets or flows, Yang, Cheng, & Chuah (2019) employ a convolutional neural network (CNN) to characterize salient temporal patterns of SCADA traffic and identify time windows where network attacks are present. The model uses realistic SCADA traffic data sets and shows that the proposed deep-learning-based approach is well-suited for network intrusion detection in SCADA systems by achieving high detection accuracy and providing the capability to handle newly emerged threats.

## 5. CONCLUSIONS

The goal of this paper was to provide a better understanding of cybersecurity aspects that are relevant to the Industrial Control Systems on which CIs are dependent. The need to protect against malicious attacks is a paramount concern, as unknown vulnerabilities can be exploited with extremely damaging effects. To mitigate this risk, various intrusion detection techniques are used, and in particular, anomaly-based detection solutions are implemented using machine learning methods. We have presented a suite of examples related to deep learning architectures that are used in the cybersecurity domain, and which are relevant for the protection of Critical Infrastructures.

## BIBLIOGRAPHY

1. Amoroso, E. & Ginter, A. (2018). *An Introduction to SCADA Security Handbook*. Rosh Ha'ayin:Waterfall Security Solutions

2. Ani, U. P. D., He, H. & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*. 1(1). 32-74.
3. Atif, Y., Jiang, Y., Jeusfeld, M. A., Ding, J., Lindström, B., Andler, S. F., Brax, C., Haglund, D. & Lindström, B. (2018). *Cyber-threat analysis for Cyber-Physical Systems: Technical report for Package 4.* Activity 3 of ELVIRA project.
4. Bakalos, N., Voulodimos, A., Doulamis, N., Doulamis, A., Ostfeld, A., Salomons, E., Li, P. (2019). Protecting water infrastructure from cyber and physical threats: using multimodal data fusion and adaptive deep learning to monitor critical systems. *IEEE Signal Processing Magazine*, 36(2). 36–48.
5. Calvo, I., Etxeberria-Agiriano, I., Iñigo, M. A., & González-Nalda, P. (2016). Key vulnerabilities of industrial automation and control systems and actions to prevent cyber-attacks. *International Journal of Online and Biomedical Engineering* (iJOE).12(01). 9-16.
6. Chen, P., Desmet, L., & Huygens, C. (2014, September). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* Berlin, Heidelberg: Springer. 63-72.
7. Feng, C., Li, T. & Chana, D. (2017, June). Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 261-272.
8. Fraley, J. B. & Cannady, J. (2017). The promise of machine learning in cybersecurity. *SoutheastCon 2017*. 1–6.
9. He, Y., Mendis, G. J. & Wei, J. (2017). Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Transactions on Smart Grid*. 8(5). 2505–2516.
10. Huda, S., Miah, S., Yearwood, J., Alyahya, S., Al-Dossari, H. & Doss, R. (2018*).* A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. *Journal of Parallel and Distributed Computing*. 120. 23–31.
11. Hurd, C.M. & McCarty, M.V. (2017). *A survey of security tools for the industrial control system environment* (No. INL/EXT-17-42229). Idaho Falls, ID: Idaho National Lab.(INL).
12. Macaulay, T. & Singer, B.L. (2011). *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press. Boca Raton, FL: Taylor & Francis Group. 33487-2742.
13. Macaulay, T. (2016). *RIoT Control Understanding and Managing Risks and the Internet of Things*. Bulington, MA: Morgan Kaufmann,
14. Mahdavifar, S. & Ghorbani, A.A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*. 347, 149–176.
16. Wilson, D., Tang, Y., Yan, J. & Lu, Z. (2018). Deep Learning-Aided Cyber-Attack Detection in Power Transmission Systems. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*. 1–5.
17. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H. & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access: Practical Innovations, Open Solutions*. 6. 35365–35381.
18. Yang, H., Cheng, L. & Chuah, M. C. (2019). Deep-Learning-Based Network Intrusion Detection for SCADA Systems. In *2019 IEEE Conference on Communications and Network Security (CNS)*. 1–7.
15. ***. (2020). Computer Security Resource Center Glossary. *NIST* [online]. URL: https://csrc.nist.gov/glossary/term/NIST [Accessed on March, 2020].