Available online at www.jpit.az

14 (2)
2023

Using machine learning methods for industrial control systems intrusion detection

Ramiz H. Shikhaliyev

Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

ramiz@science.az

0000-0002-8594-6721

ARTICLE INFO

http://doi.org/10.25045/jpit.v14.i2.05

Article history:

Received 11 January 2023

Received in revised form 14 April 2023

Accepted 26 May 2023

Keywords:

Industrial control systems

Intrusion detection

Anomaly detection

Machine learning

ABSTRACT

In recent decades, information technology has been integrated into industrial control systems (ICS). At the same time, there was a connection of the ICS to the Internet and a transition to cloud computing. Consequently, new vulnerabilities and threats to sophisticated cyberattacks have emerged that create significant risks for the cybersecurity of ICS, and the old security model based on the isolation of ICS is no longer able to ensure their cybersecurity. This situation makes it very important to intellectualize the cybersecurity of ICS, for which machine learning (ML) methods are used. The use of ML methods will make it possible to detect cybersecurity problems of ICS at an early stage, as well as eliminate their consequences without real damage. This paper discusses the issues of ICS intrusion detection based on ML methods. The work can help in the choice of ML methods for solving anomaly detection problems of ICS.

1. Introduction

Industrial control systems (ICS) are part of modern critical infrastructures. ICS are specialized information systems that significantly differ from traditional information systems available in the field of information technology (IT). There are such types of ICS as distributed control systems (DCS), supervisory control and data acquisition (SCADA), industrial automation system (IAS), industrial automation and control systems (IACS). ICS mainly used in industries such as electrical networks, water supply and wastewater treatment, oil and gas processing and transportation, nuclear and power plants, etc.

Most of the ICS in use today designed many years ago for functionality, not safety, and had different requirements and purposes. In most cases, ICS were physically isolated from external networks and based on special hardware, software, and communication protocols, such as Modbus RTU, Modbus TCP, or various wireless technologies such as Wi-Fi, Z-Wave, Zigbee, etc. These protocols had basic error detection and correction capabilities without regard to security. At the same time, the security of the ICS mainly consisted of physical protection of access to the network and consoles of the system managers. However, modern ICS must have such functional characteristics as the need for real-time response and extreme high availability, predictability, reliability, and distributed intelligence. For this, advanced computing, communication and Internet technologies have integrated into the ICS to meet more customer requirements, such as mobility, data analysis, expandability, etc.

Connecting the ICS to the Internet and moving to cloud computing have provided a number of benefits such as scalability, cost-effectiveness and flexibility. However, the connection to the Internet and the transition to cloud computing makes ICS open to the outside world. As a result, new vulnerabilities and threats for a number of cyber-

attacks appear in the ICS, which create significant risks, for example, for the health and life of people, the environment, production, the national economy, etc. Therefore, cyber security is becoming one of the most important problems of ICS due to the high cost of cyber-attacks.

The sophistication of attacks on ICS revealed their vulnerabilities and inherent security flaws (Van Der Zwan, 2010, Brenner, 2013). This has led to the fact that the old ICS security model based on network isolation is no longer able to ensure their security. However, despite the recent increase in the frequency and sophistication of cyberattacks against ICS, there have been a small number of openly documented cyberattacks. Consequently, the lack of enough attack patterns to determine the level of risk makes it difficult to understand the threat environment and prioritize security. This situation makes it very important to intellectualize the cybersecurity of ICS, for which machine learning (ML) methods are used. The use of ML methods will detect cybersecurity problems of ICS at an early stage, as well as eliminate their consequences without real damage. ML techniques can analyze large amounts of data efficiently, accurately, and quickly. Using the threat history, a ML-based security system can learn about past threats and use that knowledge to predict similar attacks in the future.

The purpose of this work is to analyze approaches to ensuring the cybersecurity of ICS based on the methods of ML. The work can help solve the problems of choosing methods of ML for ensuring cybersecurity ICS used in various industries.

2. Machine learning methods

ML provides an opportunity to discover and formalize the principles behind data, learn from data, and improve from experience. The main goals of ML are forecasting, clustering, extraction of association rules and decision support based on the information received.

ML methods can be classified as follows: supervised learning – classification; unsupervised learning – clustering; reinforcement learning (Helm et al., 2020).

The supervised learning algorithm uses a training dataset (examples) in which the data has known attributes and associated responses representing a class of data. Using the training set, the algorithm learns patterns in the data and generalizes them to correctly classify new inputs. Several methods of supervised learning are available, such as k-nearest neighbors, regression (linear, logistic, etc.), Bayesian (Naive Bayes, Bayesian networks), decision trees, artificial neural networks, rule induction, support vector machines (SVM), and discriminant analysis.

In an unsupervised learning algorithm, there are no responses associated with data attributes, and the algorithm identifies similarities between inputs and classifies them based on those similarities. The partially supervised learning algorithm is trained on a training dataset that contains both labeled (class-specific data) and unlabeled (non-class-specific data). This type of training is desirable when labels are missing or insufficient in the training data. Examples of unsupervised learning methods used to detect cyberattacks on ICS are isolation forest, single class SVM, and autoencoders such as sparse autoencoders, partial autoencoders, variational autoencoders, and fair clustering. These algorithms are trained only on normal data and any deviations or anomalies detected will be classified as "attacks".

In reinforcement learning, the algorithm receives feedback information about errors, but does not receive instructions to correct these errors, and therefore the algorithm is constantly learning using the trial and error method. Reinforcement learning involves training an agent to interact with an environment, which takes actions to maximize cumulative rewards over time. Reinforcement learning algorithms use exploration and exploitation strategies to find optimal policies. Notable examples include Q-learning, deep Q-networks, and policy gradient methods.

In many applications, the amount of data generated is extremely large, so deep learning (DL) techniques, also known as deep neural learning, are used. One of the advantages of DL over ML is its high performance. This is achieved by building larger neural networks and training them on large amounts of data. Like ML methods, DL methods support supervised learning, unsupervised learning, and reinforcement learning. DL methods that are commonly used in the field of cybersecurity are: feed-forward neural

networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), deep belief networks, multilevel autoencoders, generative adversarial networks, restricted Boltzmann machines, and ensemble of DL networks (Truong et al., 2020). DL models, such as convolutional neural networks and recurrent neural networks, are capable of automatically learning hierarchical representations from raw data. DL has proven to be effective in detecting malware and network intrusions.

ML techniques have broader applications in security, such as spam filtering, network anomaly analysis, botnet detection, and identification of user behavior anomalies.

ML algorithms and techniques can be applied to various aspects of ICS cybersecurity to enhance threat detection, anomaly detection, intrusion detection, etc.

IDSs can detect and identify potential intrusions in ICS networks. ML algorithms can analyze network traffic, system logs, and other data sources to identify patterns and anomalies associated with malicious activities. For example, SVM can be trained on labeled data consisting of normal and attack instances to classify incoming network traffic as either normal or malicious (Ghanem et al., 2017). This approach can help in detecting known attacks and even identifying unknown or zero-day attacks.

For anomaly detection, ICS environments can utilize ML techniques (Mubarak et al., 2021). By building models that learn the normal behavior of the system, any deviation from this behavior can be flagged as an anomaly. One approach is to use k-means algorithm to identify normal patterns or clusters in the data. This method can detect new or evolving threats that do not match known attack signatures.

ML algorithms can analyze the behavior of ICS components and users to detect suspicious activities or deviations from normal behavior (Koay et al., 2022)). For example, long short-term memory (LSTM) networks can be employed to model the sequential behavior of users or control system operations. These models can learn normal patterns of user behavior and identify any unusual or malicious actions in real-time.

ML algorithms can identify potential risks and vulnerabilities in ICS environments. They can analyzing data from public sources, security feeds, or internal incident reports. Natural Language Processing techniques can be applied to extract relevant information from textual sources, such as security advisories or vulnerability databases. By analyzing this information, ML algorithms can prioritize threats, assess their impact on ICS systems, and aid in proactive defense measures.

ML algorithms can assist in detecting and classifying malware targeting ICS environments. By analyzing malware samples, extracting features, and training models on known malware instances, machine learning can aid in the detection of new malware. CNNs or RNNs techniques can be employed to analyze the structure and behavior of malware, enabling automated classification and identification.

3. ICS cybersecurity threats analysis

Traditionally, ICS have designed with reliability and safety in mind (Russel, 2015). However, cybersecurity and mutual authentication of components were not taken into account in the design and operation of the ICS. Because, ICS were based on specialized equipment, codes and standard protocols and worked in a closed environment without interacting with other systems. Thus, safe and reliable ICS protocols were not created and cryptographic protections were not used. However, the transition of ICS to innovative information technologies and the use of networks have led to new realities in the field of cybersecurity. There are new threats and risks in the cybersecurity of ICS due to existing vulnerabilities. Therefore, the analysis of threats and vulnerabilities is a mandatory step that should precede decisions related to the cybersecurity of ICS. ICSs threat identification play an important role in determining the most appropriate countermeasures to mitigate their effects. Information technology and operational technology threats and vulnerabilities analysis is crucial to ensure a holistic approach to cybersecurity in ICS environments.

Threats to the security of ICS can come from several sources, such as hostile countries, terrorist groups, competitors, contractors, and disgruntled employees. In addition, the threats of human error malfunction and failure of equipment and

networks must considered. These threats and threat actors can classified as external and internal.

External threat actors include foreign intelligence services, hackers and hacktivists, industrial spies, cyberterrorists, and organized crime. These actors, for political, economic or reputational reasons, may carry out attacks to cyberespionage or disrupt technological processes.

Internal threats include network and operational problems, disgruntled employees and careless or poorly trained staff, etc. Internal threats are no less dangerous than external ones because some of these threats are beyond the organization's control, such as network and hardware misconfigurations. From a personnel perspective, insider threat actors, whether malicious or not, often has very deep knowledge and extensive access to an organization's infrastructure.

ICS security threats can be classified as follows (Van Der Zwan, 2010): organizational threats; architectural and technological threats; threats related to networks and the telecommunications system; human factor.

Organizational threats include threats to business objectives using the organizational aspects of the ICS and cover levels such as executive, information security administrator, cultural differences between IT and process control departments, IT security standards, etc.

At the executive level, risk management carried out for the organization's business goals. The executive level understands the organization's core business objectives, but the focus on business objectives causes a lack of interest in the core technological aspects of processes that lie outside of optimal performance and operational safety. The main business processes are controlled by ICS, which create a set of threats associated with new technologies, do not attract managers, since they concern the functional area, and not business and profit. Information security administrators often fail to identify SCADA threats and only focus on IT related issues as they can look like IT threats.

The cultures of the IT department and the process control department are often very different. ICS primarily focuses on the availability, visibility, operability of the processes controlled by the ICS, as well as the efficiency and safety of the processes. Cybersecurity, including aspects of integrity and confidentiality, is of less concern. Unlike the process control department, the IT department prioritizes confidentiality, followed by integrity and availability, which creates misunderstandings between departments.

Strict adherence to IT-based security standards in ICS can pose a threat to business objectives. The ISO27001 standard is a widely recognized information security management standard. This standard is accompanied by the ISO27002:2013 standard, which contains a set of information security controls divided into topics such as access control, communication security, physical security, human resource security, etc. These standards originally developed for offices, but the standard ISO/IEC 27001:2013 can applied to both IT and ICS. However, the organizational threat is that the IT department mandates strict application of the full set of IT controls to the ICS. While the ISO/IEC 27002:2013 security controls are generic and applicable to all types of information systems and applications, the implementation of certain security controls in an industrial ICS may not be effective.

Architectural and technological threats include threats related to aging technologies, new functionality of old systems, protocols, etc.

In large ICS, due to the incompatibility of old technologies with new technologies, as well as unintentional misconfigurations of new functions, a number of threats can arise. However, some of these threats may occur in small ICS. However, mitigating most technology-related threats does not require technological changes, but organizational measures, as well as changes in the culture of manufacturers and system integrators.

Since, ICS components have a long lifespan, over time their processing capacity and memory capacity can be too limited to run new applications. Working with such components makes it difficult to implement and/or activate cryptographic protection modules that require processor and memory power. Moreover, many components of the ICS and application software developed at a time when only a limited circle of people could work in the ICS. The aging of ICS components entails another threat related to the fact that manufacturers may no longer exist or

may not be able to supply spare parts.

Another threat to SCADA is the factory default passwords built into the hardware and software. Security options disabled by default, meaning there is no way to change these passwords during the installation of SCADA components. Thus, the installation of components in the ICS is unsafe and security risks arise. For example, the Stuxnet worm abused such a strong password in the Siemens WinCC SCADA product that controlled the uranium enrichment centrifuges at Nathan, Iran (Nicolas, 2011). Another threat is that authentication information, including passwords, is often unencrypted and can discovered by cyber attackers in plain text in memory or intercepted in messages.

Threats associated with the new functionality of old systems arise because many ICS developed in the sixties and based on transistors (Russel, 2015). Replacement components for installations based on more technologies that are modern and have compatible interfaces. Manufacturers add new features to components, for example, PLCs can now contain a web server that offers easy access to PLC functions, a built-in email client, and an SNMP agent. However, replacing old components without proper configuration may result in unauthorized connection to the ICS.

In the specifications of the ICS protocols, security issues taken into account in the conditions of ambiguity and lack of knowledge about the technology and the closeness of the ICS. Therefore, many ICS protocols do not protect the contents of protocol messages from man-in-the-middle attacks and do not prescribe actions when errors detected. Various studies have analyzed the safety of SCADA protocols (Fovino, 2014). These studies have shown that SCADA protocols are not secure and resistant to cyberattacks. Insecure protocols create threats to ICS and can exploited by hackers and trojans. However, the implementations of the ICS protocols are not reliable.

Network and telecommunications threats include specific threats to ICS associated with the network technologies used, such as TCP/IP and WiFi, etc. Most of the threats to SCADA in this area are associated with weak protocols and protocol implementations, as well as the use of insecure functions that use wireless communication.

Currently, there is a business need to transfer operational data from ICS to business applications. In this case, the use of firewalls is required to control the flow of information from the ICS to business applications. At the same time, a threat appears, which lies in the fact that these connections can open the way for unauthorized access by intruders and malicious programs to the ICS. Because not all firewalls support specific SCADA protocols (Igure et al., 2006). However, the use of wireless communications in PCS will create new threats (Reaves and Morris, 2012). The main threat is that a wireless connection is established, for example, to connect devices, without any planning and guarantees for its maintenance in the future.

Usually, an operator, maintenance engineers, etc. remote access to the ICS is required to ensure the effectiveness of its management. To this end, various methods of access via the Internet are used. Most organizations use virtual private network technology to connect remotely to an organization's corporate network. Further, authorized users can connect to the ICS from the corporate network.

Some organizations allow a direct dial-up connection to their PCS and secure access to the internal network requires at least two-factor authentication and strong authorization controls. In this case, a combined organizational and technical threat may appear which may be because such accesses can not be controlled and unauthorized access to the ICS may by obtained.

One of the threats to the ICS is the human factor and can create very serious threats. Because operators, control, systems and maintenance engineers are very knowledgeable about the principles of operation of the components of the ICS and have authorized access to the ICS. At the same time, people themselves are subject to cyber-attacks, and there is the threat of disgruntled (former) employees. In addition, personal equipment connected to the SCADA component, such as USB drives may carry malware. For example, the Stuxnet virus penetrated highly secure connections between the IT domains and the ICS at the nuclear enrichment plant in Nathan, Iran, through malware on a USB drive. According to several analysis reports, a third party maintenance engineer delivered the USB stick (Langner, 2011).

Advanced Persistent Threats are sophisticated, long-term attacks aimed at gaining unauthorized access to ICS networks. APTs involve multiple attack vectors and are typically conducted by well-resourced and motivated adversaries. Some examples of advanced persistent threats include: Sykipot APT malware family, GhostNet , Stuxnet worm, APT28, APT29, APT34, APT37, etc (Kanade, 2021).

Zero-day vulnerabilities are unknown software vulnerabilities that have not been patched by the vendor. Attackers who discover these vulnerabilities can exploit them to gain unauthorized access to ICS systems.

The proliferation of Internet of Things (IoT) devices in ICS environments has introduced new cybersecurity risks. Insecurely implemented or unpatched IoT devices can serve as access points for attackers to gain access to ICS networks (Dhirani et al., 2021).

Social engineering attacks exploit human psychology to deceive individuals and gain unauthorized access to ICS systems. Phishing, spear-phishing, and impersonation tactics are commonly used. In 2015, a spear-phishing attack targeted a Ukrainian power company, leading to a significant power outage affecting hundreds of thousands of people. (Case, 2016).

Human error and lack of cybersecurity awareness can introduce vulnerabilities into ICS environments. Employees may inadvertently click on malicious links, fall victim to phishing attacks, or mishandle sensitive information. Whether through intentional malicious actions or inadvertent mistakes, insiders with privileged access can cause disruptions or compromise system integrity.

The increasing use of wireless technologies in ICS introduces additional risks. Weakly secured or unencrypted wireless communications can be intercepted or manipulated, compromising the integrity and availability of ICS systems.

Insufficient network segmentation in ICS environments can allow attackers to move through systems once they gain initial access. This can lead to widespread compromise and control system disruptions.

The adoption of cloud-based services in ICS introduces new security challenges. Inadequate security configurations, shared infrastructure vulnerabilities, or compromised credentials can result in unauthorized access to ICS data and control systems.

The human-operator interface in ICS environments can be exploited to gain unauthorized access or manipulate control systems. Social engineering and phishing attacks targeting operators or system administrators have been successful in compromising ICS networks.

Many ICS systems operate on legacy software and lack regular patching or system updates. This leaves them vulnerable to known exploits.

To protect against these threats, organizations should implement a defense-in-depth approach, including network segmentation, strong access controls, regular patch management, intrusion detection systems, employee training, etc.

4. ICS cyber-attacks analysis

Today, ICS are the target of various cyberattacks that include network breaches, data theft, denial-of-service (DoS) attacks, privilege escalation, and so on. The presence of threats to the ICS makes specific cyber attacks possible. The nature and effectiveness of cyberattacks on ICS are largely determined by security flaws, as well as the architecture and technology of ICS. The main weakness in existing SCADA security solutions is the emphasis on process security while ignoring other critical issues such as people and processes, which is inconsistent with new security threats and attack trends. Typically, a one-sided security strategy focuses more on ICS , such as SCADA systems, that is, it contains industry solutions rather than general security solutions. However, due to the general lack of SCADA security, various critical infrastructure incidents can occur in controlled SCADA systems.

The consequences of successful attacks on networks and SCADA systems are potentially very serious and serious efforts are required to mitigate their consequences. Because, ICS are integral parts of the most important national infrastructures (energy, oil and gas industry, transport, aerospace industry, water system, communication system, production, etc.). Taking the example of manufacturing control systems, potential threats or attacks can take many forms. Attacks can include blocking or delaying the flow of service information through production control networks to disrupt critical production

operations, illegal changes to maintenance instructions, production commands, or alarm thresholds. As a result, they can disable or stop production lines or equipment, create harmful environmental impacts or endanger human life. Incorrect information can also be sent to system operators, either to mask unauthorized changes or to influence inappropriate operator responses to cause disruptive impacts. Modification of the ICS software or configuration settings, as well as malware infection, can be detrimental to product quality or production. Modern malware can determine the structure of physical devices and use this information to achieve the goal of attackers.

In (Zakarya et al., 2015), the authors divide SCADA attacks into three main categories such as accessibility attacks, confidentiality attacks, and integrity attacks.

Availability attacks aim to deny access to system assets as well as operations. In ICS, this refers to denying access to all system components, such as ICS assets; operator workstations, engineering stations, communication system, as well as control devices.

Integrity attacks aimed at illegally changing the content of a message or the content of system resources. In ICS, this means changing received messages or control commands passing through three system levels, as well as changing the contents of databases or control programs in the PLC (Programmable Logic Controller).

Privacy attacks aimed at obtaining unauthorized data or resources on the SCADA network, such as passwords, PLC configurations, etc. The obtained data can be used to reproduce some of the ICS operations.

Cyber-attacks on ICS carried out in various forms and modes. The authors in (Pasqualetti et al., 2015) identified four broad classifications of attacks aimed at ICS. These include deception attacks, denial-of-service attacks (DoS attacks), replay attacks, and covert attacks:

– Deception attacks aimed at violating the integrity of control packets or data and are usually performed by changing the behavior of nodes, equipment, sensors and actuators. An unconventional type of deception attack that can cause significant damage to an ICS called a decoy attack (Liu et al., 2011).

– Denial-of-service attacks aimed at compromising the availability of resources, for example, by blocking the communication channel, connecting device and SCADA nodes. The same approach called in (Ashok et al, 2014) a “timing attack”, which works by saturating the communication network with data packets, which causes a decrease in network speed and a possible complete shutdown.

– Replay attacks performed by recording sensor readings over a period and repeating such recorded readings to the system. Research has shown that such a deliberate anomaly can be corrected by inserting random signals unknown to attackers into the system (Ashok et al., 2014), (Pasqualetti et al, 2013).

– In covert attacks, covert agents can change the behavior of a physical object, while remaining unnoticed by the controller (Smith, 2011).

The following are the most sophisticated attacks on ICS identified by researchers and security experts:

– Stuxnet is a Microsoft Windows computer worm discovered in July 2010 and designed specifically for industrial software and equipment of the nuclear enrichment plant in Nathan (Iran) (Nicolas et al., 2013). The worm initially spreads indiscriminately, but includes a highly specialized malware payload designed to attack only certain SCADA systems configured to control and monitor a manufacturing process. Stuxnet exploited several vulnerabilities in the runtime environment as well as in the implementation of the SCADA protocol (Bonnie and Sastry, 2010).

– Slammer is a Microsoft SQL Server worm that was discovered in 2010. The Nuclear Regulatory Commission has confirmed that the Slammer worm infected a private computer network at a nuclear power plant in Ohio, shutting down the safety monitoring system for nearly five hours. In addition, the plant's process computer failed and it took about six hours for it to become available again. Slammer has also reportedly affected communications in the control networks of at least five other utilities by spreading so quickly.

– Havex malware is malicious software that was discovered in 2013. It was designed to monitor systems that control industrial equipment and was a remote access trojan that allowed hackers to control computers remotely. Havex has targeted thousands of European, and Canadian companies, especially in the energy and petrochemical industries and the US.

– Shamoon is malware. This malware was targeted at Saudi Aramco refineries, which is the 8th largest oil refinery in the world. The malware targeted the system's Master Boot Records (MBR), partition tables, and other arbitrary data files. This resulted in systems becoming unusable (Keith et al., 2014).

– Triton malware was first discovered in 2017 and targeted oil company Petro Rabigh from Saudi Arabia. It could cause massive damage, including marine pollution, a surge in gasoline prices, and even death from the explosion. This program reprograms the controllers of the Triconex automated security system.

5. ICS intrusion detection based on ML methods

Over the past decades, the number of cyber attacks on ICS has increased and become more sophisticated. Under these conditions, the traditional methods of ensuring the security of ICS are insufficient and, as a rule, allow detecting certain types of threats and attacks. However, the nature of existing threats and attacks have changed, making them unpredictable. Attackers are using new methods and tools to attack and compromise systems and steal data. In addition, in large and complex systems, new vulnerabilities appear that are difficult to detect. At the same time, conventional methods for detecting vulnerabilities react to events only after the vulnerability has been exploited.

Recently, ML methods have been developing rapidly and widely used to ensure the cybersecurity of ICS. There are many works in the literature devoted to the use of ML methods to ensure the cybersecurity of ICS (Jiang and Zhao, 2019, Hemavati Er. and Aparna R, 2019). ML methods can provide effective tools for detecting vulnerabilities, malware, network intrusions, phishing and spam, attack detection as well as data leakage, detection and accurate prediction of security incidents, etc. In addition, ML methods are able to predict problems through predictive analysis based on previous decisions. ML methods are also capable of analyzing large volumes of data quickly, efficiently, and accurately. Therefore, the use of ML methods quickly and accurately identifies cyber threats to ICS , which will greatly increase the effectiveness of responding to threats. In addition, the use of ML methods makes it possible to predict possible cyber risks and identify potentially dangerous actions. By analyzing all kinds of previous attacks, machines can predict previously unknown attacks. Consequently, it will improve the efficiency of prioritization for ensuring cybersecurity, as well as the improvement of policies and procedures aimed at improving the overall cyber resilience of ICS.

Anomaly detection creates models for normal behavior and any behavior that deviates from the model can be detected and treated as an intrusion.

Traditionally, intrusion detection has mainly used predefined models and trained to detect specific cyber-attacks. However, this intrusion detection models do not take into account the imbalance of datasets, which leads to low accuracy in detecting cyber-attacks and a high level of false positives.

There are three types of intrusion detection model: signature-based, specification-based, and behavior-based. When using the signature-based model, predefined attack pattern dictionaries are required. It detects an intrusion if any detected pattern matches one or more predefined attack patterns (Gao and Morris, 2014). While this approach maintains a low false positive rate, it cannot detect zero-day attacks. However, it is often difficult to compile a comprehensive dictionary of attack signatures in complex physical processes.

Specification-based intrusion detection models use a mathematical model to determine the normal functioning of the physical process in question. An anomaly exists when a process deviates from the prediction of a predetermined model (Mitchell and Chen, 2015). Such models developed with the help of specialists and designers of the enterprise. Although experts may have knowledge of the physical processes, there are problems associated with the aging of the physical system, the inaccuracies that may exist in

operating manuals, and the interpretation of process behavior.

Behavior-based intrusion detection models are based on physical system behavior data. Based on the collected data, the models trained on the normal and abnormal behavior of the process. This approach is preferable to incorrect supplier specifications because the model trained on empirical data (Junejo. 2020) and thus helps to detect incorrect supplier specifications.

There are some problems when using intrusion detection models in the ICS, which are associated with the lack of attack patterns on the ICS, the heterogeneity of the physical processes of the ICS, etc. Because there are no templates for attacks on the ICS due to the difficulty of compiling exhaustive dictionaries of attack signatures in the complex physical processes of the ICS. Therefore, it becomes difficult to detect some attacks, such as zero-day attacks. However, the physical processes of ICS are heterogeneous because the components, size and functionality of each process differ from each other. Therefore, the detection of attacks in heterogeneous physical processes controlled by ICS is a difficult task (Hu et al., 2018).

Modern intrusion detection models use ML techniques for pattern recognition to detect dangerous activities that are anomalous for a particular system (Pinto et al., 2023). For example, ML methods are widely implemented to detect and prevent anomalies in SCADA systems. Because, SCADA systems have regular communication patterns, that can be analyzed by ML methods. In (Yasakethu and Jiang, 2013) for the protection of SCADA, an intrusion detection system (IDS) based on ML methods were proposed. The authors compare rule-based methods, artificial neural networks, hidden Markov models and support vector machines. In (Maglaras and Jiang, 2014), the authors propose an OCSVM (One-Class Support Vector Machine) intrusion detection model based on unsupervised learning methods that does not use any information about the anomaly for learning. The authors in (Zhang et al, 2013) propose a SCADA intrusion detection model based on a self-learning semi-supervised OCSVM (S2 OCSVM) and demonstrate that S2 OCSVM can improve detection accuracy. In (Stefanidis and Voyiatzis, 2016), for detecting intrusions in ICS, especially in SCADA systems, interconnected using TCP/IP, an IDS architecture based on the Hidden Markov Model (HMM) algorithm was proposed.

However, despite the popularity of using ML in intrusion detection models, there are not enough standard datasets for training and testing these models. This leads to the impossibility of developing reliable ML models for detecting anomalies in ICS. Datasets play an important role in ML and determine learning outcomes. Having a good dataset is a guarantee of successful training of an ML model. Most of the available data sets, especially in the context of SCADA, do not contain all types of cyber-attacks, so it is difficult to assess the performance and accuracy of an intrusion detection model.

Some researchers have tried to create datasets for anomaly detection in SCADA. Oak Ridge National Laboratories created three sets of transmission system data (Pan et al., 2015, Pan et al., 2015). These datasets contain many measurements including normal behavior, attack behavior, log data from Snort and the relay network. In (Goh et al., 2016), the authors collected datasets from a water treatment system that may represent a real industrial water treatment plant. The data set contains the physical properties and network traffic during the attack and in normal mode. In (Morris et al., 2015) created a dataset from a gas pipeline that contains data from normal activities and more than 30 different attacks. Simulators are used in (Antoine and José, 2016) to set up an electrical network and create malicious traffic with real attack tools, although the data set cannot reproduce a real industrial control network. These datasets can be a good basis for testing and evaluating anomaly detection models and algorithms.

Intrusion detection methods based on traditional ML algorithms such as SVM decision tree, NN (Neural Network), etc., cannot effectively deal with massive, multi-dimensional, time-related network traffic data in an ICS. To solve this problem, the work (Chen et al., 2019) proposes a method for detecting intrusions in ICSs based on a recurrent neural network. The authors use the update gate and reset gate of the Gated Recurrent Unit to store information about the data in the time dimension, which made it possible to explore the features of the data and to optimize the gradient learning process of the

neural network for which used Adam algorithm. Comparative experiments were carried out with intrusion detection methods based on SVM algorithms, decision tree, NN, RNN, LSTM, etc. The results showed that the proposed method has a higher classification accuracy than SVM, decision tree, NN, and RNN, and the accuracy is the same as LSTM, but the training time is reduced.

Most of the existing classification techniques are hard to deploy in a real environment since they cannot deal with the open set problem. In (Wang et al., 2021) proposed NN based-methodology to solve this problem, the openmax layer is used instead of the traditional softmax layer, which overcomes the limitations of softmax, allowing NN to detect unknown attack classes. For training new loss function termed center loss is implemented to improve detection ability. The NN model learns better feature representations with the combined supervision of center loss and softmax loss. The NN was evaluated on NF-BoT-IoT-v2 and Gas Pipeline datasets. The experiments show that the proposed method is comparable with the current algorithm in terms of detecting unknown classes and has better overall classification performance.

Most IDS do not consider the imbalanced nature of ICS datasets, thus suffering from low accuracy and high False Positive Rates when being put to use. (Cao et al., 2022) proposes the NCO–double-layer DIFF_RF–OPFYTHON intrusion detection method for ICS, which consists of NCO modules, double-layer DIFF_RF modules, and OPFYTHON modules. Detected traffic is divided into three categories by the double-layer DIFF_RF module: known attacks, unknown attacks, and normal traffic. The known attacks are classified into specific attacks by the OPFYTHON module according to the feature of attack traffic. The NCO module uses to improve the model input and enhance the accuracy of the model. The results show that the proposed method outperforms traditional intrusion detection methods, such as XGboost and SVM. The accuracy of the used dataset reaches 98.13%. The detection rates for unknown attacks and known attacks reach 98.21% and 95.1%, respectively.

6. Conclusion

The number of ICS cyber threats and their complexity is increasing significantly year by year. Under such conditions, ensuring cyber security of ICS is one of the main problems of national and international security. Therefore, it is necessary to improve the methods of ensuring the cybersecurity of ICS, which are currently used.

The use of ML methods, in ensuring the cybersecurity of ICS is a new research area. ICS cybersecurity approaches based on ML methods are promising and show clear advantages over existing approaches.

There are many ML methods in the literature, and the choice of ML methods to ensure the cybersecurity of ICS is an urgent task. The correct choice of ML methods for solving certain cybersecurity tasks of ICS depends on many criteria, including the type of system protected.

This article analyzed approaches to ICS intrusion detection based on various methods of ML. The analysis carried out can help in the correct choice of ML methods for solving intrusion detection problems ICS, used in various industries.

Acknowledgments

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

References

Antoine L, José M. (2016). Providing SCADA network data sets for intrusion detection research. In: 9th USENIX workshop on security experimentation and test.

Ashok A., Hahn A., and Govindarasu M. (2014). Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment, J. Adv. Res., vol. 5, pp. 481–489.

Bonnie Z., and Sastry S. (2010). SCADA-specific intrusion detection/prevention systems: a survey and taxonomy, Proc. of the 1st Workshop on Secure Control Systems (SCS).

Brenner J. F. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems," Bull. At. Sci., vol. 69, p. 15.

Cao Y., Zhang L, Zhao X., Jin K. and Chen Z. (2022). An Intrusion Detection Method for Industrial Control System Based on Machine Learning, Information, 13(7), 322; https://doi.org/10.3390/info13070322

Case D. (2016). Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) 388.

Chen T., Lin P. and Ling J. (2019). An Intrusion Detection Method for Industrial Control System Based on Gate Recurrent Unit, Journal of Physics: Conference Series, 1302 022016, https://doi.org/10.1088/1742-6596/1302/2/022016

Dhirani L, Armstrong E., and Newe T. (2021). Industrial IoT Cyber Threats, and Standards Landscape: Evaluation and Roadmap, Sensors (Basel). 21(11): 3901, https://doi.org/10.3390/s21113901

Fovino, I. N. (2014). SCADA system cyber security. In K. Markantonakis & K. Mayes (Eds.), Secure smart embedded devices, platforms and applications (pp. 451–471). New York, NY: Springer Science + Business Media. https://doi.org/10.1007/978-1-4614-7915-4_20.

Gao W. and Morris T. H. (2014). On Cyber Attacks and Signature Based Intrusion Detection for MODBUS Based Industrial Control Systems. Journal of Digital Forensics, Security and Law, vol. 9, 1, 37–56.

Ghanem K., Aparicio-Navarro F.J., Kyriakopoulos K.G., Lambotharan S., Chambers J.A. (2017). Support Vector Machine for Network Intrusion and Cyber-Attack Detection, Institute of Electrical and Electronics Engineers (IEEE), 1(1), https://core.ac.uk/works/18504183

Goh J., Adepu S., Junejo K.N. (2016). A dataset to support research in the design of secure water treatment systems. In: 11th international conference on critical information infrastructures security. Springer, Cham.

Helm, J. M., Swiergosz, A. M., Haeberle, H. S.,Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. Current reviews in musculoskeletal medicine, 13(1), 69-76.

Hemavati Er. and Aparna R. (2019). A Survey on Intrusion Detection System using Machine Learning and Deep Learning, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(2), https://doi.org/10.32628/CSEIT195264

Hu Y., Yang A., Li H., Sun Y., and Sun L. (2018). A survey of intrusion detection on industrial control systems, International Journal of Distributed Sensor Networks, 14(8):155014771879461, https://doi.org/10.1177/1550147718794615

Igure, V., Laughter, S., & Williams, R. (2006). Security issues in SCADA networks. Computers and Society, 25 (7), 498–506.

Jiang D., and Zhao J. (2019). Machine Learning in Industrial Control System Security: A Survey, Proceedings of 2019 Chinese Intelligent Systems Conference, pp. 310-317, https://doi.org/10.1007/978-981-32-9698-5_35

Junejo K. N. (2020). Predictive safety assessment for storage tanks of water cyber physical systems using machine learning. Sadhana 45, 1 (2020), 1–16.

Kanade V. (2021). What Is Advanced Persistent Threat? Definition, Lifecycle, Identification, and Management Best Practices, https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-advanced-persistent-threat/

Stoufler K., Lightman S. and Abrams M. (2014). Guide to industrial control systems Security, NIST special publication 800-82.May.

Koay A., Ko R., Hettema H. and Radke K. (2022). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges, Journal of Intelligent Information Systems, 60, pp. 377-405.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

Liu Y., Ning P., and Reiter M. K. (2011). False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur., vol. 14, pp. 1-33.

Maglaras L. A., Jiang J. (2014). Intrusion Detection in SCADA Systems Using Machine Learning Techniques, Science and Information Conference (SAI), pp. 626-631.

Mitchell R. and Chen I.-R. (2015). Behavior Rule SpeciŠcation-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. Dependable and Secure Computing, IEEE Transactions on 12(1), pp.16–30.

Morris T, Zach T, Ian T. (2015). Industrial control system simulation and data logging for intrusion detection system research. In: 7th annual southeastern cyber security summit.

Mubarak S., Habaebi M., Islam R., Rahman F. and Tahir M. (2021). Anomaly Detection in ICS Datasets with Machine Learning Algorithms, Computer Systems Science & Engineering, , https:// doi.org/10.32604/csse.2021.014384

Nicolas F., Murchu L. O , and Chien E. (2014). W32.Stuxnet Dossier, Symantec.

Nicolas F., Murchu L. O. (2011). W32.Stuxnet Dossier. Cupertino, CA, USA: Symantec. Retrieved November 8, 2015 https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Pan S, Morris T, Adhikari U. (2015). Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. 11th IEEE Trans Ind Inf 11(3), pp.:650–662.

Pan S, Morris T, Adhikari U. (2015). Developing a hybrid intrusion detection system using data mining for power systems. IEEE Trans Smart Grid 6(6):1

Pasqualetti F., Dorfler F., and Bullo F. (2015). Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," IEEE Control Syst., vol. 35, no. 1, pp. 110–127.

Pasqualetti F., Dörfler F., and Bullo F. (2013). Attack Detection and Identi fi cation in Cyber-Physical Systems, IEEE Trans. Automat. Contr., vol. 58, no. 11, pp. 2715–2729.

Pinto A., Herrera L.-C., Donoso Y., and Gutierrez J. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure, Sensors, 23(5), 2415, https://doi.org/10.3390/s23052415

Reaves, B., and Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5 (3-4), 154–174. doi: 10.1016/j.ijcip.2012.10.001

Russel, J. (2015). A brief history of SCADA/EMS, http://scadahistory.com/

Smith R. S. (2011). .A decoupled feedback structure for covertly appropriating networked control systems, in IFAC Proceedings Volumes (IFAC-PapersOnline), vol. 18, pp. 90–95.

Stefanidis K., Voyiatzis A. G. (2016). An HMM-Based Anomaly Detection Approach for SCADA Systems, in IFIP International Conference on Information Security Theory and Practice, pp. 85-99, Springer International Publishing.

Truong T. C., Diep Q. B., Zelinka I. (2020). Artificial Intelligence in the Cyber Domain: Offence and Defense, Symmetry, 12(3):410. https://doi.org/10.3390/sym12030410

Van Der Zwan E. (2010). Security of Industrial Control Systems, What to Look For, ISACA J. Online, 4(10), pp. 1-9.

Wang C., Wang B., Sun Y., Wei Y., Wang K., Zhang H.,and Liu H. (2021). Intrusion Detection for Industrial Control Systems Based on Open Set Artificial Neural Network, Security and Communication Networks, 4027900, https://doi.org/10.1155/2021/4027900

Yasakethu S. L. P., Jiang J. (2013). Intrusion Detection via Machine Learning for SCADA System Protection, in Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, pp. 101-105.

Zakarya D., Ahmed S., Olivier V. (2015). Analysis of Cyber Security for Industrial Control Systems, International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC).

Zhang Y. G., Zhang W., Xue X. R., Yang X. J. (2013). SCADA Intrusion Detection System Based on Self-Learning Semi-Supervised One-Class Support Vector Machine, Metallurgical Industry Automation, vol. 37(2), pp. 1-5.