Detection of Anomalies in Industrial IoT Systems by Data Mining: Study of CHRIST Osmotron Water Purification System

Mohammad Sadegh Sadeghi Garmaroodi, Faezeh Farivar, Senior Member, IEEE, Mohammad Sayad Haghighi, Senior Member, IEEE, Mahdi Aliyari Shoorehdeli, Senior Member, IEEE, Alireza Jolfaei, Senior Member, IEEE

Abstract—Industry 4.0 will make manufacturing processes smarter but this smartness requires more environmental awareness, which in case of Industrial Internet of Things, is realized by the help of sensors. This article is about industrial pharmaceutical systems and more specifically, water purification systems. Purified water which has certain conductivity is an important ingredient in many pharmaceutical products. Almost every pharmaceutical company has a water purifying unit as a part of its interdependent systems. Early detection of faults right at the edge can significantly decrease maintenance costs and improve safety and output quality, and as a result, lead to the production of better medicines. In this paper, with the help of a few sensors and data mining approaches, an anomaly detection system is built for CHRIST Osmotron® water purifier. This is a practical research with real-world data collected from SinaDarou Labs Co. Data collection was done by using six sensors over two-week intervals before and after system overhaul. This gave us normal and faulty operation samples. Given the data, we propose two anomaly detection approaches to build up our edge fault detection system. The first approach is based on supervised learning and data mining e.g. by support vector machines. However, since we cannot collect all possible faults data, an anomaly detection approach is proposed based on normal system identification which models the system components by artificial neural networks. Extensive experiments are conducted with the dataset generated in this study to show the accuracy of the data-driven and model-based anomaly detection methods.

Index Terms—Data Mining, Machine Learning, Industrial IoT, Anomaly Detection, Fault Detection, Dataset Generation, Edge Processing, System Identification, Water Purification System.

I. INTRODUCTION

Water is one of the important raw materials in pharmaceutical drug manufacturing process. Control and monitoring of water purification process, including production, storage, distribution and microbiological and chemical quality checking is taken very seriously both for public and pharmaceutical consumptions [1–3]. Generally, in dependable automated systems, quick and precise fault detection, identification and tolerant compensation [4, 5] at the edge are essential for equipment reliability, reduction in the number of off-products as well as maintenance costs. Timely detection of anomalies or faults can also prevent failures cascade that might happen due to the interconnections between industrial systems. [6].

In water purification systems, anomalies and faults may be caused by over-voltage, over-current, overloading in high-pressure pumps, failure or malfunctioning of PLC cards and sensors, pipes leakage, sedimentation in pipes, or even deliberate cyber attacks [6]. Since any malfunction in medicine-related systems can be hazardous and affect public health, irregularities are taken seriously. Purified water is an important ingredient in many pharmaceutical products. Malfunctioning of water purification systems can result in poor water quality, reduced output or even plant shutdown.

There are many non-expensive and non-intrusive techniques for anomaly detection which are classified into model-based and data-driven groups [7, 8]. Model-based approaches work based on the model of physical systems, and can be further divided into observer-based and system identification-based subgroups [9]. Modeling of industrial processes is a critical issue because most real-world industrial systems are non-linear, multi-input and multi-output, and due to interrelated parameters and noises, they have un-modelled dynamics and uncertainty [10, 11]. If the basic model of a process is not well represented, the fault detection or diagnostic system will not be sufficiently robust in the presence of noise and disturbance. This implies that a model-driven fault/anomaly detection mechanism suits the cases in which the process is simple, low dimensional or can be accurately described by mathematical relations [12, 13].

When the system behavior is unknown and too complex, or its model is incomplete and unavailable, applying data-driven methods are prescribed. There are two main approaches for data driven fault/anomaly detection; unsupervised and supervised learning [14].

This paper develops two anomaly detection approaches in industrial Internet of Things (IoT) and more specifically, for water purification systems, both of which are based on Machine Learning (ML) and data mining. The proposed methods are tested on a CHRIST Osmotron® water purification...
The main contributions of this paper are as follows:

- Real-world data collection from a CHRIST Osmotron\textsuperscript{®} system at SinaDarou Lab Co. to record and store sensors’ information for anomaly detection.
- Designing data-driven and model-driven edge anomaly/fault detectors for industrial water purification systems based on data mining and machine learning.

The rest of this paper is organized as follows. In Section II, we briefly review related studies. Section III introduces the process and CHRIST Osmotron\textsuperscript{®} unit for water purification. In Section IV, machine learning-based approaches are developed for anomaly detection. Results are presented in Section V. Finally, the paper is concluded in Section VI.

II. RELATED WORK

Traditional methods for anomaly/fault detection are based on occasional inspection of the system or machine. For instance, overheating of an electric motor can be diagnosed as a fault. But the inefficiency of people, longtime high-intensity work, and random inspection make the traditional methods unreliable [15]. A variety of data-driven anomaly detection techniques have been developed and employed in automatic control systems. These methods can discover meaningful rules to represent the information in system variables e.g. by using the time series data. Recently, anomaly detection has become one of the active research topics aiming to increasing the safety and reliability of dynamic systems.

Because of the importance of water quality in medicine manufacturing and water supply companies, several studies have tried to address the issue of anomaly detection in these systems. In [16], an anomaly detection algorithm is designed to check the water quality by dual time-moving windows. The algorithm works based on an autoregressive linear model. It has been tested on PH data of water. In [17], Support Vector Machine (SVM) and artificial neural networks are used for determining the water quality. In [18], least squares support vector machine (LS-SVM) and particle swarm optimization methods have been applied to predict the water quality. This paper applied recurrent neural networks to a dynamic system. Moreover, they modelled the problem with multiple input variables. This can be useful in time series forecasting in which classical linear methods struggle to adapt to multivariate or multiple input problems. Paper [1] presented a survey of machine learning methods in anomaly detection for the quality of drinking-water. According to the authors, the review encompasses both traditional ML and deep learning (DL) approaches. Having fair comparisons between published studies is difficult because of the difference in dataset, models, parameters, etc. DL is suggested mainly because of its advantages in feature learning accuracy. In [2], anomaly detection in water quality data is studied with different approaches, e.g. logistic regression, linear discriminant analysis, SVM, artificial neural network, deep neural network, recurrent neural network, and long short-term memory. The applied methods are compared by using the F-Score metric. In [3], machine learning and statistic learning approaches have been studied to solve the problem of anomaly detection in water quality data. Different machine and static learning methods for time series (like local outlier factor, isolation forest, robust random cut forest, seasonal hybrid extreme studentized deviate, and exponential moving average) have been used for anomaly detection in a wastewater treatment plant. Comparison results have been presented to show the power of each method.

In a broader view, the number of studies on IoT, Cyber Physical Systems (CPS), and Networked Control Systems (NCS) has increased. IoT helps with the interconnection of CPSs. It facilitates distributed traffic exchange, especially the heterogeneous and dynamic data at the edge. In [19], a transmission architecture is developed for wired/wireless fieldbus networks and wireless sensor networks (WSNs) in smart factories. For a typical IoT application, i.e. environment monitoring by WSNs, reference [20] employed two clustering algorithms, in centralized (cloud-based) and distributed (edge-based) approaches. Advantages of the proposed algorithms are in computation, communication, and energy consumption. Paper [21] proposed an automatic anomaly detection method in WSNs by coupling edge and cloud data analyses. The algorithm employed unsupervised artificial neural networks and the multi-parameterized edit distance algorithm for edge and cloud data, respectively. Reference [22] explored an agent-based computing paradigm in order to support IoT design, implementation, and analysis. Specifically, agent-based cooperating smart object methodology and middleware were studied. CPSs as well as collective and dynamic services are named as opportunistic IoT services which are modelled and simulated using Aggregate Computing in [23].
normal or abnormal behaviour and flag irregular behaviour as possibly anomalous. For instance, papers [27, 28] studied anomaly detection algorithms in the context of CPS security. Such algorithms can also be used in other areas like aviation [29], network infrastructure in smart cities [30], fault detection and tolerant control of nonlinear dynamic systems [31, 32], electric power and smart grid systems [33, 34].

This study only focuses on machine learning-based anomaly detection for CHRIST Osmotron® water purification system which is used in pharmaceutical companies. In the next section, we present a brief description of the system, and then we propose our framework for this aim. Evaluation of the proposed framework comes after.

III. DESCRIPTION OF CHRIST OSMOTRON® WATER PURIFICATION SYSTEM

The aim of any water purification system is preventing microbrial growth and removing particles, organic and inorganic substances, dissolved gases, and microbes. Every phase of production from pretreatment to quality control of the water, storage and distribution is a major concern in the pharmaceutical industry. In general, there are different processes of water purification according to the United States Pharmacopoeia (USP) and European Pharmacopoeia (EP) requirements, including: distillation, reverse osmosis (RO), deionization, and ultrafiltration.

CHRIST Osmotron® system makes purified water by using reverse osmosis and deionization processes and consists of three units which are osmosis, cold and hot loops. The main process of water purification occurs in the osmosis unit, and cold and hot loops are used for storage and distribution of purified water (PW) and water for injection (WFI). The osmosis unit reduces the potable water conductivity from about 700 $\mu$m/cm to less than 1 $\mu$m/cm by passing water through the softening membranes and the electro-deionize column. The purified water in the outlet of this unit flows to the cold and hot loops.

The internals of CHRIST Osmotron® water purification system are shown in Fig. 1. Potable water first passes through a filter (F270.1.1) to remove any particles that may be in the water. The filter has a 100 $\mu$m rating. In the next part, a water softener operates based on ion-exchange principle and softens the incoming water. It consists of two filters (F270.2.1-3.1) connected in series. Calcium and magnesium are replaced by sodium. When the filters become saturated with hard agents, they have to be regenerated with the aid of sodium chloride (common salt). The softened water is then led to the reverse osmosis. The reverse osmosis unit (B270.5.2-5.4) tries to demineralize the soft water. The soft water first passes through a fine filter (F270.5.1) that removes any particles which may still be in the water. The filter has a 5$\mu$m rating. Then the filtrated water is pumped, at a high pressure generated by the frequency-regulated pump (P270.5.1), into the permeators. Some of this water passes through the membrane, leaving dissolved substances behind. This is so called the permeate. The permeate from the reverse osmosis unit enters the EDI SEPTRON modules (B270.6.1-6.3). Each of these consists of two chambers, separated by a special membrane. The pure-water chamber is filled with an ion-exchanger resin. As the permeate flows through the pure-water chamber, almost all of the ions remaining in it are removed. The ions removed from the permeate are collected in the concentration chamber. They are later removed by the rinsing water circulated by the frequency-regulated pump (P270.6.2). The resulting dilute is flowed through the pipes to the pure water storage tank (B560.1.1), and then to the consumers.

Each of the aforementioned subsystems can malfunction. In the next subsection, two artificial intelligence-based strategies are developed for anomaly detection in CHRIST Osmotron® water purification system.
IV. ANOMALY DETECTION BY USING ARTIFICIAL INTELLIGENCE

Accuracy in detection and reaction timeliness are important issues in anomaly detection. Reaction time is critical to prevent process failures and cascaded damages in dependable and controllable things. Early detections increase the chance to maintain the system performance. We propose two specific approaches, both based on machine learning techniques, to make an anomaly or fault detection system in CHRIST Osmotron® water purification systems. The first one is based on supervised data driven methods that make detection of specific faults using classification methods possible. The second approach is generic and model-based with which any fault can be detected.

A. Approach #1: Data-Driven Anomaly/Fault Detection

Supervised classification is a machine learning-based technique which is popularly used for detection of previously-seen errors. This is the same technique that is so called signature-based detection in the cyber security domain [34]. In this approach, a labelled training set of normal and faulty samples is created first and then, the data are fed to a classifier to find a proper boundary that best separates the samples. If there are multiple faults or anomalies of known kind, this method can well detect and separate them. However, similar to any signature-based scheme, the drawback is that if there is a previously unseen fault or anomaly, the detector might not classify it correctly, or even mistake it for normal sample.

Fig. 2 depicts the first approach for anomaly detection in CHRIST Osmotron®. All the steps of this approach, except pre-training with labelled samples, have been illustrated in this figure. In the results section, we will show how the real-world data collected from a machine before and after overhauling are used to train classifiers like SVM or neural networks.

B. Approach #2: Model-based Anomaly / Fault Detection

Signature-based detection of Approach #1 is certainly effective if the anomaly or fault attributes/features are known beforehand. However, it is almost impossible to collect samples of every possible type of fault in a complex interconnected industrial system. The best practices suggest building a normal model of the system instead, which comes to help when one wants to monitor/study the behavior of the system. This approach is generally referred to as anomaly detection in the domain of cybersecurity [27, 35].

As mentioned before, we collected real-world data from an Osmotron in normal and faulty conditions. However, in this approach, we put the faulty samples aside and only focus on the ones collected during the system’s normal operation.

An identifier, which is an artificial neural network, learns the system dynamics under normal conditions. Then, given the input, the developed normal model is used to generate an output estimate and a residual signal \((Y_{out} - Y_{nn})\) which form the basis of our decision making. Note that \(Y_{out}\) and \(Y_{nn}\) are the system and normal model outputs, respectively.

In this study, we suggest using fixed as well as adaptive thresholds to detect anomalies based on the residue. During the training/learning phase, the system and the identifier outputs form a residual \((Y_{out} - Y_{nn})\) based on which the anomaly detection system determines the detection threshold. The modelling errors collected from the plant/system during the training interval make the threshold for anomaly detection. To calculate the fixed threshold, it is assumed that the residue is an approximation of Gaussian distribution whose mean \((m)\) and standard deviation \((v)\) of the the residual signal \(N(m, v)\) determine a fixed threshold \(T\) as follows:

\[
T = m \pm \zeta v
\]

where \(\zeta\) is a (constant) coefficient.

In practice, because of measurement noise and modelling uncertainty, it is essential to make a larger threshold to avoid false alarms. It leads to reduce sensitivity in fault detection. Therefore, the threshold should be chosen such that it compromises between sensitivity of fault decision and rate of the false alarm. Because of mentioned reason, it is recommended to apply adaptive thresholds for industrial applications. Like before, it is assumed that the residual is an approximation of the normal distribution. The mean and standard deviation are calculated over the past \(n\) samples as follows:

\[
m(k) = \frac{1}{n} \sum_{i=k-n}^{k} r(i)
\]

\[
v(k) = \frac{1}{n-1} \sum_{i=k-n}^{k} (r(i) - m(k))^2
\]

Fig. 3. The second approach for anomaly/fault detection. This approach is more applicable when the samples of different system faults are scarce.
where $0 < n < k$. The adaptive threshold is obtained as:

$$T(k) = m(k) \pm \zeta v(k) \quad (4)$$

This threshold is calculated using the estimations of statistical parameters of previously-observed residuals. It is assumed that the residual distribution is normal in this case. Thresholds are adjusted for the selected window of length $n$ based on the mean and standard deviation values, according to Eq. (4). This continues for the whole procedure to the last window.

Notice that it is important to choose an appropriate length for the time window. If $n$ is too small, the threshold quickly adapts to any change in the residual e.g. disturbances, noises or faults. If $n$ is too large, the threshold acts as if it is constant, which leads to sensitivity reduction in decision making [36].

The second approach can be used in an online manner. The proposed scheme for the second approach of anomaly detection in CHRIST Osmotron® system is demonstrated in Fig. (3). As shown, the plant is the Osmotron water purification system. As mentioned before, the artificial neural network modelled the normal behaviour of the main system and is then employed as an intelligent identifier. A residual generator calculates differences between the outputs of the main system and those of the model. Then, the adaptive thresholds we explained in this section are employed for anomaly detection and decision making regarding the system operation situation. If the system works with anomalies, the operator is alerted.

V. IMPLEMENTATION RESULTS & DISCUSSION

Both approaches for anomaly detection described in the previous section (illustrated in Fig. (2) and Fig. (3)) are applied on CHRIST Osmotron® water purification system here.

A. Data Gathering

CHRIST Osmotron® water purification system was installed by its experts in Sina Darou Laboratories Co. in 2006. The device input capacity is 2000 $\text{lit}/\text{h}$, which under normal conditions should produce 1500 $\text{lit}$ of purified water with a conductivity of less than 1 $\mu\text{m/cm}$.

Decrease in the output volume of the purified water, as well as increase in the conductivity of the water at the system outlet were two major problems that the device faced at the time of the project launch. Hence, the possible causes and factors of these problems were examined. As mentioned in Section III, membrane filters and EDI ion exchange resins play an important role in the quality and capacity of purified water, so in the first step, membrane filters and then and EDI resins were also replaced during overhaul.

The basic repair and service of the device were included activities such as replacing some O-rings and sealing washers, washing and cleaning the water movement paths, replacing some valves and actuators, calibrating the sensors, replacing some input and output cards of the device controller (PLC), and so on. Moreover, the replacement of the mentioned filters and resins provided the desired performance of the system. Fig. 4a and Fig. 4b show an example of sensors and PLC cards used in this work, respectively.

In this study, six sensors have been selected and positioned in the Osmotron unit as shown in Fig. 1, which are as follows:

- PT270.5.1: Pressure of before frequency regulated pump.
- PT270.5.4: Pressure of after frequency regulated pump.
- QE270.5.1: Conductivity after RO.
- QE270.6.2: Conductivity of concentrate.
- PT270.6.3: Pressure of EDI.
- QE270.6.1: Conductivity of EDI to tank.

Regarding the challenge of data gathering, a data recorder with six-channels and sampling frequency of one minute has been installed in CHRIST Osmotron® system. A Jumo recorder from the LOGOSCREEN 500 series was installed on the Osmotron unit as depicted in Fig. 4c. As shown in Fig. 4d, the recorder can record and store values measured by the mentioned sensors. Then, both normal and faulty data were collected. Faulty data were recorded in the earlier days of the study when the system was suffering from an undesirable performance, and the normal data refers to the data collected after overhaul of the system by manufacturer experts.

A sample of faulty data and normal data (which were collected one week and three months after the system repair) is depicted in Fig. 5. As observed, faulty data is marked in green and corresponds to one month before the experts repair the system, while the normal data is shown in blue and collected at intervals of one week and three months after repairing the system. Notice that sampling was done in one-minute intervals because of the system variations. After gathering data, the information was transferred from the recorder to the computer.

B. Data Preprocessing

In this study, preprocessing of data consists of three steps; cleansing, normalization, and noise removal.

- **Data Cleansing.** Sometimes either the device was shut down for service and filter replacement, or the electricity was cut off, therefore, some data could be irrelevant or lost. It is important to clean such samples off the dataset.
- **Normalization.** Since the range of variations in the measured data was large, the data have been normalized to lie between zero and one.
• **Noise Removal.** To remove and reduce noise effects on the collected data, a low-pass filter, which was Savitzky-Golay filter, was employed. It is a digital smoothing filter.

In the next subsection, the two developed machine learning-based approaches for anomaly detection (illustrated in Fig. 2 and Fig. 3) are applied on CHRIST Osmotron®.

### C. Results of Approach #1 (Data-driven)

Whenever we know the faults we are looking for, supervised signature-based classification can be used. Since we could not deliberately induce different kinds of faults in a sensitiveustrial machine like our pharmaceutical water purification system to collect their signatures (or data samples), we merely collected data from the system that had gone faulty mostly because of aging and not being calibrated. Normal samples were collected after overhauling.

We used the classic linear support vector machine (SVM) (as well as neural network and decision tree) as a binary classifier to separate the normal and abnormal samples. Bear in mind that abnormal samples constitute only one kind of fault in this experiment. The six sensors created a set of samples in the 6-dimensional space. Slices of this space in which the input-output relation of important Osmotron components is visible have been depicted in Fig. 6. It is rather easy to find out that the normal operation areas in the majority of these slices are quite distinct from the faulty ones. That is exactly why all of the classic classifiers, including linear SVM, could classify normal and faulty samples with 100% accuracy.

### D. Results of Approach #2 (Model-based)

As mentioned before, since it is almost impossible to have a dataset of all possible faults, we adopt anomaly detection approaches in which only normal operation behavior of the system is learned. This is a common approach in anomaly and intrusion detection of industrial cyber physical systems.

Since we have multiple sensors inside the system, we have access to inputs and outputs of almost every important component. Therefore, rather than identifying the whole system as a black-box based on its inputs and outputs, we can have more granularity and learn each important component behavior separately. For example, let us take the frequency regulated water pump (P270.5.1 in Fig. 1) whose task is to receive water at variable pressures and create an almost constant pressure (around 15 bars) at its output end.

For identification, we took a neural network with two hidden layers. We set the number of neurons at the input layer, the two hidden layers, and the output layer to 5, 22, 20, and 1, respectively. We used 1500 samples in this experiment from which 75% were used in training and the rest were used in the test. The network was trained by back propagation.

Fig. 7 shows the identification residues \((Y_{out} - Y_{nn})\) of the pump, reverse osmosis, and EDI SEPTRON when a sequence of test samples (from the normal dataset) is fed to the trained network. It also shows thresholds. For the water pump example, one can see that the maximum estimation error (under normal circumstances) for the pump (Fig. 7a) does not exceed 0.13 bar. If a fixed threshold is to be used for operation anomaly detection, 0.13 can be a good candidate. To see how a
faulty system performs, we used the samples of PT270.5.1 and PT270.5.4 before overhauling and plotted the residue found by the same neural network trained by the non-faulty overhauled system. Fig. 7d shows the residue along with the thresholds. It can be seen that a faulty system eventually crosses the threshold and the alarm is raised. While fixed thresholds are handy and easy to find for each system component, they are less sensitive to violations that might happen at certain working points. Therefore, we also tested adaptive thresholds that were updated according to Eq. (4). Fig. 7 plots also the adaptive threshold boundaries for P270.5.1 (the water pump), reverse osmosis and EDI SEPTRON.

It should be emphasized that unlike the first approach, this detection approach does not rely on previously-seen faulty samples and thus, is more probable to catch unseen anomalies.

We further discuss and summarize the results of the two approaches employed in this study. The first data-driven approach that we used was a binary SVM classifier that could separate normal and abnormal classes of data. To train the classifier, we studied the input-output data for each subsystem. As the Osmotron unit contains four subsystems, we plotted their input-output functional maps under normal and faulty conditions in Fig. 6. The figure clearly shows the workspaces of the subsystems under normal and faulty condition are different.

This explains why a linear classifier like the binary SVM that we used is able to achieve high accuracies. The second method was the model-based approach that we founded on the basis of residual signals and adaptive thresholds. Fig. 7 demonstrates the residual signals for each component of the Osmotron unit along with the thresholds applied for anomaly detection. This approach does not require faulty training samples. We can compare the performance of this approach to that of the first one if we merge the signals of component-based anomaly detection systems by an OR operation and make a system-wide anomaly detection flag.

VI. CONCLUSION

In this paper, we used two machine learning-based approaches for detecting anomalies or faults in a real-world industrial automation system, i.e. CHRIST Osmotron® water purifier. By adding a few sensors and using machine learning techniques, we injected intelligence to this interconnected industrial system and made spotting anomalies and faults possible. A prominent part of this research was collecting real-world data from CHRIST Osmotron® before and after overhauling using six sensors. Aging created a kind of fault from which 15000 samples were collected. The same number of samples were collected after overhauling, which represented
the system’s normal operation attributes. We first used classic supervised classifiers to detect the fault based on the six sensors readings. However, since detection of different or perhaps unknown faults was not easy, we proposed to detect anomalies based on learning the normal behavior of the system and putting the faulty samples aside. Both fixed and adaptive thresholds were tested, and the results showed that while the supervised machine-learning approach is effective, its counterpart has this additional feature that can be used to detect unknown and unseen anomalies. As a future work, we intend to spot the location of faulty component based on a rough functional model of the system and the data collected from a minimum number of sensors.

ACKNOWLEDGEMENT

We are thankful to SinaDarou Laboratories Company, and specifically its CEO, Dr. Mohammad Hasan Vasefi, and the Manager of Engineering and Technical Department, Mr. Ali Naghi Mansubi, for their supports during this study.

REFERENCES

[1] E. Dogo, N. I. Nwulu, B. Twala, and C. Aigbavboa, “A survey of machine learning methods applied to anomaly detection on drinking-water quality data,” Urban Water Journal, vol. 16, no. 3, pp. 235–248, 2019.
[2] F. Muharemi, D. Logofatu, and F. Leon, “Machine learning approaches for anomaly detection of water quality on a real-world data set,” Journal of Information and Telecommunication, vol. 3, no. 3, pp. 294–307, 2019.
[3] Y. Yan, “Anomaly detection for water quality data,” Ph.D. dissertation, 2019.
[4] F. Farivar and M. Aliyari Shoorehdeli, “Fault tolerant synchronization of chaotic heavy symmetric gyroscope systems versus external disturbances via lyapunov rule-based fuzzy control,” ISA transactions, vol. 51, no. 1, pp. 50–64, 2012.
[5] F. Farivar and M. A. Shoorehdeli, “Fault tolerant synchronization of chaotic heavy symmetric gyroscope systems via gaussian rbf neural network based on sliding mode control,” in IEEE International Conference on Mechatronics, 2011, pp. 300–305.
[6] M. S. Haghighi and K. Mohamedpour, “Neighbor discovery: Security challenges in wireless ad hoc and sensor networks,” in Trends in telecommunications technologies, 2010.
[7] Y. Zhang, Y. Yang, S. X. Ding, and L. Li, “Data-driven design and optimization of feedback control systems for industrial applications,” IEEE Transactions on Industrial Electronics, vol. 61, no. 11, pp. 6409–6417, 2014.
[8] Z. Chen, S. X. Ding, H. Luo, and K. Zhang, “An alternative data-driven fault detection scheme for dynamic processes with deterministic disturbances,” Journal of the Franklin Institute, vol. 354, no. 1, pp. 556–570, 2017.
[9] A. Slimani, P. Ribot, E. Chanthey, and N. Rachedi, “Fusion of model-based and data-based fault diagnosis approaches,” IFAC-PapersOnLine, vol. 51, no. 24, pp. 1205–1211, 2018.
[10] S. Yin, G. Wang, and H. R. Karimi, “Data-driven design of robust fault detection system for wind turbines,” Mechatronics, vol. 24, no. 4, pp. 298–306, 2014.
[11] M. R. Kandroodi and B. Moshiri, “Identification and model predictive control of continuous stirred tank reactor based on artificial neural networks,” in International Conference on Control, Instrumentation and Automation, IEEE, 2011, pp. 338–343.
[12] W. Hongm, C. Tian-You, D. Jin-Liang, and M. Brown, “Data driven fault diagnosis and fault tolerant control: some advances and possible new directions,” Acta Automatica Sinica, vol. 35, no. 6, pp. 739–747, 2009.
[13] S. Simian, “Chemical system dynamic identification with application to sensor fault detection,” IFAC Proceedings Volumes, vol. 38, no. 1, pp. 87–92, 2005.
[14] M. Grbovic, W. Li, N. A. Subrahmanya, A. K. Usadi, and S. Vucetic, “Cold start approach for data-driven fault detection,” IEEE Transactions on Industrial Informatics, vol. 9, no. 4, pp. 2264–2273, 2013.
[15] T. Wang, M. Qiao, M. Zhang, Y. Yang, and H. Snoussi, “Data-driven prognostic method based on self-supervised learning approaches for fault detection,” Journal of Intelligent Manufacturing, pp. 1–9, 2018.
[16] J. Zhang, X. Zhu, Y. Yue, and P. W. Wong, “A real-time anomaly detection algorithmor water quality data using dual time-moving windows,” in Int. conference on innovative computing technology, 2017, pp. 36–41.
[17] M. R. Kandroodi, S. Shabanuddin, C. K. Chang, N. A. Zakaria, A. Ab Ghani, and N. W. Chan, “Prediction of water quality index in constructed wetlands using support vector machine,” Environmental Science and Pollution Research, vol. 22, no. 8, pp. 6208–6219, 2015.
[18] Y. Xiang and L. Jiang, “Water quality prediction using is-svm and particle swarm optimization,” in 2009 Second International Workshop on Knowledge Discovery and Data Mining. IEEE, 2009, pp. 900–904.
[19] Y. Luo, Y. Duan, W. Li, P. Pace, and G. Fortino, “A novel mobile and hierarchical data transmission architecture for smart factories,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3534–3546, 2018.
[20] C. Savaglio, P. Gerace, G. Di Fatta, and G. Fortino, “Data mining at the iot edge,” in International Conference on Computer Communication and Networks (ICCCN). IEEE, 2019, pp. 1–6.
[21] F. Cauteruccio, G. Fortino, A. Guerrieri, A. Liotta, D. C. Mocanu, C. Perra, G. Terracina, and M. T. Vega, “Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance,” Information Fusion, vol. 52, pp. 15–30, 2019.
[22] G. Fortino, W. Russo, C. Savaglio, W. Shen, and M. Zhou, “Agent-oriented cooperative smart objects: From iot system design to implementation,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 11, pp. 1939–1956, 2017.
[23] R. Casadei, G. Fortino, D. Piainini, W. Russo, C. Savaglio, and M. Viroli, “Modelling and simulation of opportunistic iot services with aggregate computing,” Future Generation Computer Systems, vol. 91, pp. 252–262, 2019.
[24] A. Cook, G. Misirl and Z. Fan, “Anomaly detection for iot time-series data: A survey,” IEEE Internet of Things Journal, vol. 7, no. 7, 2020.
[25] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security: A survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.
[26] M. A. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, “A review of novelty detection,” Signal Processing, vol. 99, pp. 215–249, 2014.
[27] F. Farivar, S. Barchinezhad, M. S. Haghhighi, and A. Jolfaei, “Detection and compensation of covert service-degrading intrusions in cyber physical systems through intelligent adaptive control,” in 20th IEEE International Conference on Industrial Technology, 2019.
[28] S. Barchinezhad and M. Sayad Haghhighi, “Compensation of linear data-driven fault detection scheme for dynamic processes with deterministic disturbances,” Journal of the Franklin Institute, vol. 354, no. 1, pp. 556–570, 2017.
[29] F. Farivar and M. N. Ahmadabadi, “Compensated fault-tolerant control for a class of unknown nonlinear systems,” Applied Soft Computing, vol. 37, pp. 702–714, 2015.
[30] M. Sayad Haghhighi, F. Farivar, A. Jolfaei, and M. H. Tadayon, “Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack,” The Journal of Supercomputing, vol. 76, no. 4, pp. 3063–3085, 2020.
[31] M. Martimelli, E. Tronci, G. Dippoppa, and C. Balducelli, “Electric power system anomaly detection using neural networks,” in International Conference on Knowledge-Based and Intelligent Information and Engineering Systems. Springer, 2004, pp. 1242–1248.
[32] M. S. Haghhighi, F. Farivar, and A. Jolfaei, “A machine learning-based approach to build zero false-positive ips for industrial iot and cps with a case study on power grids security,” IEEE Transactions on Industry Applications, in press, 2020.
[33] F. Farivar, M. S. Haghhighi, A. Jolfaei, and M. Alazab, “Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber physical systems and industrial iot,” IEEE transactions on industrial informatics, vol. 16, no. 4, 2020.
[34] K. Patan, Artificial neural networks for the modelling and fault diagnosis of technical processes. Springer, 2008.