Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 583-590
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.5540

# Review of machine learning and deep learning mechanism in cyber-physical system

V. Padmajothi[a,b,*], J. L. Mazher Iqbal[c]

[a]ECE, Vel Tech Rangarajan Dr. Sagunthala R& D Institute of Science and Technology, Avadi, Chennai, Assistant Professor, ECE, SRM Institute of science and technology, Kattankulathur, Chennai, India
[b]ECE, SRM Institute of science and technology, Kattankulathur, Chennai, India
[c]ECE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India

(Communicated by Madjid Eshaghi Gordji)

**Abstract**

Cyber-Physical Systems are one of the emerging technologies which involve the integration of cyber system physical and control systems. This Cyber-physical System automates the industrial process like manufacturing, monitoring and control. Since the system involves three different cyber, physical and control optimization domains, such systems are complex in nature and cannot be done with a traditional optimization mechanism. Machine learning and deep learning are efficient mechanisms to model the behavior of such complex systems for design and optimization. In this work, the application of machine learning mechanisms in the cyber-physical system for various purposes like security, re-organization, and scheduling. This systematic review will give more insight into the latest application and mechanism of machine learning and deep learning for the cyber-physical system.

*Keywords:* Anomalous detection; cyber-physical system; deep learning; fault analysis; machine learning; security; scheduling

## 1. Introduction

A Cyber-Physical System (CPS) is nothing but integrated system with computer system, control system and physical system. Those algorithms are computer based ones. In cyber-physical systems both the physical components and the non-physical components like software are strongly tied together. The main challenges in Cyber-Physical Systems according to Industry 4.0 are safe guarding and safe keeping of the data, inadequate amount of beneficial quantities, top management prioritization is insufficient, Industrial broadband structure, sabotaging and non-production due to the data

*Received:* June 2021 *Accepted:* September 2021

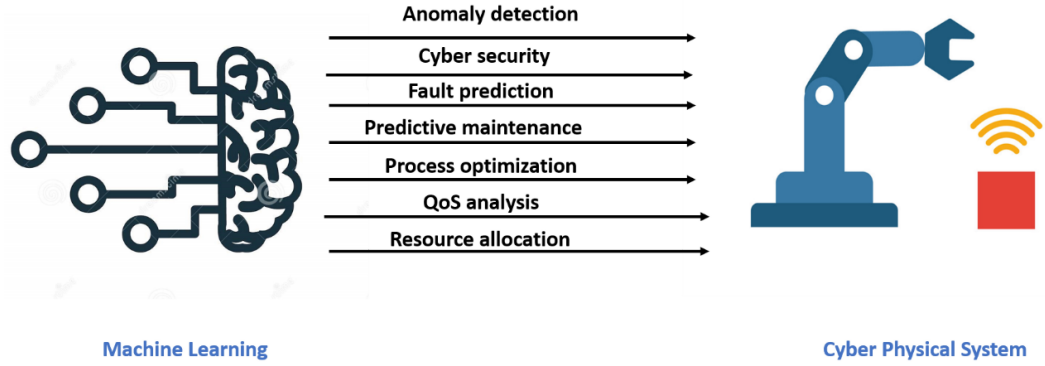


Figure 1: Application of Machine Learning in Cyber-Physical System

unavailability.

Figure 1 shows the various application of ML in cyber-physical systems. From the figure, we can observe the following applications are mainly implemented using machine learning mechanism:
1. Anomaly detection, 2. Cybersecurity, 3. Fault prediction, 4. Predictive maintenance 5. Process optimization, 6. QoS analysis and 7. Resource allocation
Anomaly detection involves detecting abnormal behavior in CPS using sensor data analysis. It could be used for security attack detection, failure of the gaget etc. Cybersecurity involves the detection of various communication attacks, which may result in a malfunction of the physical system, thereby spoil the deployed objective of the physical system. In this article detecting security attack using several type of ML approach which is reported in current literature is presented. Fault prediction is the process of prediction of error occurrence of the component, which could be used to avoid failure of the system and thereby unwanted catastrophic events and also large loss can be avoided. Predictive is closely connected with fault prediction, where the outcome of fault prediction could be used as input data for predictive maintenance. Process optimization is connected with the cyber system, where the entire operation of the system is divided into a number of processes/tasks. ML: mechanism can be applied to individual process control. On the other aspect, an intelligent scheduler can be designed for effectively managed task allocation and computation to meet the real-time constraints of CPS. In this direction, a broad review of various intelligence scheduling algorithms developed using ML/DL algorithms is reported. QoS analysis involves accessing QoS-related data from various CPS subsystems and analyzing them to verify the required QoS are met or not. Resource allocation is tightly is tied up with QoS analysis. And resource allocation and various communication, computational resource required for effective CPS operation are dynamically allocated with the ML algorithm. The intelligent task scheduling also will come under this category, which is also reviewed in this article

Figure 2 shows the use case for predictive control of machine learning between the sensor and the activator. In this use case ML model, the sensor data are captured and used for training the ML model. After training, the model can have the behavior of the physical system and which could be used for predictive control of activators
Thus the machine learning mechanisms are widely used in CPS systems for various applications. This paper presents a review of the application of machine learning in CPS systems. The remaining part of the article is organized as follows: Section 2 deals with machine learning applications for

*Corresponding author
*Email addresses:* padmajov@srmist.edu.in (V. Padmajothi), drmazheriqbal@veltechuniv.edu (J. L. Mazher Iqbal)

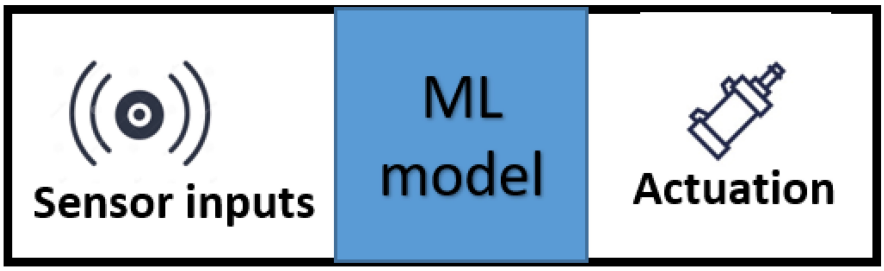


Figure 2: ML model for predictive control between the sensor and the activator

security. Section 3 presents Machine Learning-based Scheduling in CPS, section 4 gives the Fault Analysis in CPS using Machine Learning, section 5 concludes the article with a summary.

## 2. Machine Learning Security Application in CPS

Safeguarding the Cyber-Physical Systems (CPSs) is very much essential for preserving sensitive information. In CPS, the sensor data are transmitted to the actuator through wireless communication, which has various security issues, so in CPS there is a need to address these issue. In past few years, the CPS security issues were addressed and over came with help the of machine learning based algorithm.

A wide range of surveying the connections between resilient Cyber-Physical Systems (CPS) via the help of Machine Learning (ML) is presented [11]. ML, when applied in CPS, it has been ensured. From this article, the readers can identify the advancement of detection of security using ML, and also, they have countermeasures.

In [5], the necessity of integrated security in CPS is presented. Moreover, it highlights the different security challenges associated with CPS. They have also mentioned the techniques and countermeasures that are available and based upon ML and Deep Learning (DL), which falls in the Artificial Intelligence (AI) and data science category. This literature review clearly shows that data science perception is appropriate for safe-guarding CSP and comes with adaptive strategies that are vital. They have provided insights useful or related to security analysis of CPS via ML, which helps the reader to move furthermore in investigating & realizing of security framework which safeguards CPS from both external and internal cyber-attacks.

The co-existence abnormality, faults and security attacks are analysed [15]. In this literature, they observed and learned from scratch the inter-communication environmental system called Energy Aware Smart Home (EASH). Also, they have differentiated and defined the problems like a component failure and network attacks, which are revised and evaluated based on communication behaviour effect or outcome. They generally show us the link between abnormality sources and ML-based Framework for differentiating the problem. The framework was evaluated through simulation or VR and in a real-time demonstration & testbed environment through which they got about 85% of accuracy in classification. Thus the classification accuracy increases, it was verified by an experimental result and a detail analysis is provided in consideration of classes and features utilized in this implemented approach.

On using deep Convolutional Neural Networks (CNNs) and the original network data a merged framework is formed to detect Distributed Denial of Service (DDoS) attacks as soon as possible is presented [4], in order to take over the control in that malicious device, DDoS attacks were arranged or mobilized by a botnet. These malicious devices targets messages or SMS, internet, call or blending of these services in order to cause a group of massive DDoS attack in a cell, which can interrupt CPS's

process. Through demonstration, their framework has achieved more than 91% detection accuracy in normal circumstances and under-attack.
In [9], the authors have probed the latest advancement in Deep Learning (DL) and how it could cover these security problems with enhanced accuracy in Android-based CPS systems. In common, the DL engine is implemented for the detection of sensitive app behaviours, which are classified by a system information patterns like available space in storage and transmitted package volume are identified by an encoder which uses a custom Deep Neural Network. In mean time, for resource limitations purpose, ResNet is used to operate on typical devices such as Cyber-Physical System and Internet of Things. Sparse learning is implemented to decrease the quantity of acceptable guidelines in the trained neural network. Estimations shows that the model outperforms well with a finet set of guideline on time series organization for identifying the behaviour of an sensitive app with background noises and the targeted behaviours are certainly intersecting
Security issues in Additive Manufacturing (AM) methods are also reported in [3]. In this article, they inspected the standard features of AM supply chain and based on the industry's nature three types of AM chain models have been implemented. Their summary of their model constitutes on acquiring a full view of the AM supply chain and which contains the raw material, printer hardware and the virtual supply chain. All the way throughout the lifetime of extra manufactured products, it was found out that on when a digital thread virtual supply chain interweaving with physical supply chain, it automatically makes the AM process a cyber-physical system (CPS) due to their functions or operations. Moreover, this technology comes with the benefits of CPS and also along with the class of attack area vectors. So they have provided an advanced risk classification scheme based on the possible attacks (printer, raw material and design level), risks (reverse engineering, counterfeiting and theft). They concluded that the old cybersecurity methods need to be enhanced and improved to solve this new variant attack vector, which is a treat to AM supply chain, in considering the old solutions, which helped to address the attacks' threats and the danger. In full view of the AM supply chain, the correlation of the process is presented and clarified the local vectors attacks' effect. Then the gap in the existing security method which needs to be filled for AM security is discussed.
Security in IoT-based CPS is presented in [12]. Even a small fault or failure could lead to an overflow of failures inside the interdependent networks in CPS. So this paper focuses on to shrink or decrease overflow of failures between the interdependent networks and also to reduce the losses. Vigorness of the system is highlighted for a random attack, and in entire network function size of the component were calculated during the time of the attack. The alteration of the inter-links topology of the coupled networks were done improve the consistency of the system. Through which they got a more efficient swapping strategy for the advancement of the vigorness of the Cyber-Physical System in compared to the former revisions. Therefore, the altered systems' structures give greater performance in swapping the inter link-strategies, thereby increasing the consistency of networks. Furthermore, this article could be considered as a guide on optimizing a Cyber-Physical System topology by decreasing the effect of overflow of the failures.

### *2.1. Anomalous Detection*

Intrusion detection and anomalous attack detection is another type of security attack detection in CPS.
A violation detecting system in CPS for IEEE 1815.1- power system network is reported in [7]. The author has summarized the following points in his work: at first, they have implemented an app method to detect the insertion in the system, then for anomaly detection, they have implemented a neural network based on bidirectional recurrent for IEEE 1815.1- network and finally he has done a demonstration to verify these implemented techniques by utilizing several attack data of power sys-

tem, which also includes CPS network traffic used by actual power system, CPS Malware Behaviour (CMB), False Data Injection (FDI), and Disabling Reassembly (DR) attacks. Therefore three types of FDI, DR attacks and five types of CMB attacks were detected by this implemented techniques
Another anomaly detection framework known as PPAD-CPS (Privacy-Preserving based Anomaly Detection for Cyber-Physical Systems) is presented in [6]. This framework is proposed to power systems for safeguarding non-public information and also to track down the malicious activities and the network traffic of them. Then the framework is sub-divided into two main modules. The first module is used to filter and convert the actual data format into another format through which privacy preservation is achieved. The second module is also known as the anomaly detection module, which is implemented using the Gaussian Mixture Model (GMM) and Kalman Filter (KF) to accurately evaluate the later chances of legalized and abnormal events. Two public datasets are used to calculate the PPAD-CPS framework's performance. Power System and the UNSW-NB15 dataset are the two public datasets. Compared to the four recent techniques to achieve a high privacy level, this framework is more effective. This is shown through an experimental result. Overall in terms of detection rate, false-positive rate, and computational time this framework performs well than the other seven peer abnormal detection methods.

## 3. Machine Learning-based Scheduling in CPS

Scheduling is used in CPS for task scheduling for real-time performance and also sensor scheduling for the data transmission from them for distant state evaluation of the physical system, which is scattered.
An estimate of the study of sensor transmissions scheduling to find out the state of active processes at remotes is presented [8]. A central wireless gateway is implemented to monitor and collect information from different sensors. These sensors need to be appropriately scheduled for better estimation at the gateway. For example, every-time the quick one or the first one needs to decide which sensor should have access to the network and which shouldn't. In order to overcome this problem, they have formulated an associated Markov Decision Process (MDP). MDP solves the problem by utilizing a Deep Q-Network, which is the latest deep learning algorithm. The proposed mechanism has highly measureable and model-free. The DL algorithm for scheduling has equivalency to other widespread scheduling algorithms like round-robin, reduced waiting time, etc. and also outperforms well than these algorithms in many scenarios.
"Age of Information" consists of transmission delay of the packet & inter-arrival time of the packet. In a CPS an enhanced real-time system. A scheduling mechanism for optimal transmission of the packet to make the freshness of the information with less age is presented [14]. The main theme of this article is to achieve the optimized scheduling strategy for transmission in order to preserve the novelty of the information in industrial CPS at present/real-time. Cyber and physical units are made to co-exist together. Their requirement is to give a quality service which is a challenging one to handle. For this purpose, Deadline aware Highest Latency First policy is implemented. This paper gives a systematic evidence for better optimization and claims the validation through a performance comparison with other scheduling strategy in an extensive simulation.
Integrated complexity is presented among scheduling and supervising the CPS, particularly in actuators. An event-driven model is proposed in [10] to satisfy the required amount of control accuracy and to conserve the actuator's energy consumption with limited action delay. The authors found out two challenging problems; they are 1. Actuator scheduling and 2. Output control. To overcome this two challenging problem, the author proposed a two-step optimization technique. Those two steps are 1. The problems are sub-divided into two sub-problems, those problems are actuator's

scheduling and action time allocation. Then after sub-dividing the problems are solved in iteration method in which one solution is used in another. The algorithm concurrence also proven.; 2. In order to evaluate the errors and respectively to alter the results according to it, an online method is implemented. The effectiveness of the implemented method is shown through a demonstration.
The dynamic and irregular release of tasks arrives from the regular interaction between the cyber and physical systems. An investigation of the dynamic scheduling of criticality functions in CPS is presented in [1]. This article inspects the dynamic scheduling of mixed-critical functions; an acyclic graph is used to model each function with no assumptions in its short period of time between successive arrivals. The old methodologies are inactive, explains the mixed-criticality and gives us a cure or solution when deadline misses are noticed, which leads to a High Deadline Ratio (HDM), and which is unfortunate, especially for functions of high criticality. So the author proposed a different scheduling approach, which uses active strategies (ASDYS), in which mixed-criticality is vigorously handled until the end of the scheduling progress. For illustration purposes, automotive CPSs are used. Through experiment, it's found out that this method is far better and advanced than the previous methods in both DMR of high criticality field and in entire system DMR fields. A multiple-attackers schedule problem in cyber-physical systems (CPSs) is presented in [17]. In this article, the author contemplates multi-attackers who cause scheduling problems against remote state evaluation in CPSs. In relation with the existing results where it focuses on only one type of attacker, but here the author wishes to inscribe two type of attackers namely the Denial of service (DoS) attacker and the linear deception attackers, who exist in CPSs concurrently. With the less amount of resources in hand, the two attackers need to cooperate with each other, decides whether to initiate the attack or call off the attack and which kind of attack needs to be injected and reaming steps are optimally planned over a fixed amount of time, in order to reduce system's performance at major level. At first, the development of distant evaluation of state and error variance, during the attack the schedule is derivative and they consider error and terminal error as system's performance index and in order to find out the optimal attacking scheduling scheme, they analyse the core properties. At the end, in order to witness the their theoretical result an illustration is shown
In CPS the automatic decision making are mandatory for active production scheduling. Various digital twins were aggregated to present a new framework; a global digital twin is used to make autonomous decision & also to perform a manufacture plan is offered [16]. The fuzzy inference system used to perform decision-making. In workstations local digital twins is utilized to predict the condition of the assets and the rate of the production, which is assured on the shop floor.
This paper represents a Cyber-Physical Production System (CPPS) framework for reorganizing and cohesive decision-making for re-scheduling. The validation and proof of this implemented method are shown in the assembly process of the Industry 4.0 in pilot line. We can find that the implemented framework can detect the changes during the process of manufacture and creates a suitable decision for re-scheduling purpose, as demonstrated through an experiment.

## 4. Fault Analysis in CPS using Machine Learning

Fault detection in CPS is required to predict the malfunctioning in the system. In recent years, there is considerable work carried out for fault diagnosis and prediction. In this direction, the author of [2] has invented the idea of parametric hybrid automata (PHA) to outline the complexity of these CPSs. Until the runtime, the PHA parameter values are unidentified. However, the ordinary offline checking model is infeasible. So instead of that, they have proposed an online checking PHA model as a fault recognition tool. Its utilization is a challenging one, which consumes more time to reach the state of verification and which is the conservative focus of model checking. In order to describe

this difficult, they implemented that the model checking can focus on online scenario reachability validation. Then they injected a mechanism to compose/decompose the plot or scenarios. They have achieved polynomial-time cost by exploiting linear programming through their plot or scenario reachability validation. The evaluation gives the results from over one h to approximately 200 ms. In this study is based on the condition of CPS. K-means clustering analysis is based on the fault case big data machine learning is implemented for examination of the fault recognition of the rotating machinery without any help of an external expert. K-means cluster-based fault identification model, it contains k-means cluster analysis module, fault mode - fault cluster centroid knowledge base module and fault identification module has been created. A detailed study of fault feature extraction and fault eigenvectors transmission is done. The urge, rubbing, misalignment and normal status of the centrifugal compressor in industrial plants these vibration data were helpful in train the k -means cluster fault recognition model and also to verify them. The recognition accuracy rate result is obtained and resulted as follows: 94% - surge faults, 100% - rubbing faults and 80% - misalignment faults. In the future, the effect of this cluster analysis of the vibration data will be studied for five or more operating states.

### *4.1. Predictive Maintenance*

Predictive maintenance can be considered as a subcategory of fault diagnosis, which involves finding the status of equipment through fault diagnosis. There are few works that reported Predictive Maintenance using machine learning. In this direction, two innovative ideas are reported in [13]. The reported creative ideas are: 1) a predictive maintenance machine learning model in manufacturing system based on the status indication of the machine and 2) semi-Double-loop machine learning, an ML-based high-level environment for predictive maintenance execution on the basis of intelligent Cyber-Physical System (I-CPS). Focusing only on the status information of a machine gives us a quick implementation and an enhanced predictive maintenance prototype/paradigm investment cost is very low, especially in the case of SMEs. Thus the model is valid for real-life scenarios and also explores different techniques and algorithms for the purpose of learning the predictive maintenance models. The results show a very high accuracy of prediction level.

## 5. Conclusions

The cyber-physical system involves an automated system that deals with physical components like industries manufacturing units. This system needs to be secured from any type of attack. So, security measure on the CPS is essential. Security attack detection is the primary step in securing the CPS system where machine learning plays a vital role. A review of such mechanism is reported in this paper. Similarly, machine learning-based scheduling for dynamic changes in the environment of CPS were also presented. Fault prediction and predictive maintenance is another essential factor to be realized in CPS. The work involved with fault diagnosis and predictive maintenance is also resented in the presented work.

## References

[1] Y. Bai, Y. Huang, G. Xie, R. Li and W. Chang, *ASDYS: Dynamic scheduling using active strategies for multi-functional mixed-criticality cyber–physical systems*, IEEE Trans. Indust. Inf. 17(8) (2020) 5175–5184.

[2] L. Bu, Q. Wang, X. Ren, S. Xing and X. Li, *Scenario-based online reachability validation for CPS fault prediction*, IEEE Trans. Computer-Aided Design Integ. Circuits Syst. 39(10) (2019) 2081–2094.

[3] N. Gupta, A. Tiwari, S.T. Bukkapatnam and R. Karri, *Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks*, IEEE Access 8 (2020) 47322–47333.

[4] B. Hussain, Q. Du, B. Sun and Z. Han, *Deep learning-based DDoS-attack detection for cyber–physical system over 5G network*, IEEE Trans. Indust.Inf. 17(2) (2020) 860–870.
[5] A.A. Jamal, A.A.M. Majid, A. Konev, T. Kosachenko and A. Shelupanov, *A review on security analysis of cyber physical systems using Machine learning*, Materials Today: Proc. (2021).
[6] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu and I. Khalil, *An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems*, IEEE Trans. Sustainable Comput. 6(1) (2019) 66–79.
[7] S. Kwon, H. Yoo and T. Shon, *IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for the cyber-physical system*, IEEE Access 8 (2020) 77572–77586.
[8] A.S. Leong, A. Ramaswamy, D.E. Quevedo, H. Karl and L. Shi, *Deep reinforcement learning for wireless sensor scheduling in cyber–physical systems*, Automatica 113 (2020) 108759.
[9] H. Ma, J. Tian, K. Qiu, D. Lo, D. Gao, D. Wu, C. Jia and T. Baker, *Deep-learning–based app sensitive behavior surveillance for Android powered cyber–physical systems*, IEEE Trans. Indust. Inf. 17(8) (2020) 5840–5850.
[10] L. Mo, P. You, X. Cao, Y. Song and A. Kritikakou, *Event-driven joint mobile actuators scheduling and control in cyber-physical systems*, IEEE Trans. Indust. Inf. 15(11) (2019) 5877–5891.
[11] F.O. Olowononi, D.B. Rawat and C. Liu, *Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps*, IEEE Communic. Surv. Tutor. 23(1) (2020) 524–552.
[12] H. Peng, C. Liu, D. Zhao, H. Ye, Z. Fang and W. Wang, *Security analysis of CPS systems under different swapping strategies in IoT environments*, IEEE Access 8 (2020) 63567–63576.
[13] G.D. Putnik, V.K. Manupati, S.K. Pabba, L. Varela and F. Ferreira, *Semi-Double-loop machine learning-based CPS approach for predictive maintenance in manufacturing system based on machine status indications*, CIRP Ann. 70(1) (2021) 365–368.
[14] D. Sinha and R. Roy, *Deadline-aware scheduling for maximizing information freshness in industrial cyber-physical system*, IEEE Sensors J. 21(1) (2020) 381–393.
[15] G. Tertytchny, N. Nicolaou and M.K. Michael, *Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning*, Microproc. Microsyst. 77 (2020) 103121.
[16] A. Villalonga, E. Negri, G. Biscardo, F. Castano, R.E. Haber, L. Fumagalli and M. Macchi, *A decision-making framework for dynamic scheduling of cyber-physical production systems based on digital twins*, Annual Rev. Cont. 51 (2021) 357–373.
[17] J. Zhang and J. Sun, *Optimal cooperative multiple-attackers scheduling against remote state estimation of cyber-physical systems*, Syst. Cont. Lett. 144 (2020) 104771.