EVOLUTION OF MACHINE LEARNING IN CYBER PHYSICAL SYSTEM

Prof. Megha Wankhade, Assistant Professor,
NCRD's Sterling Institute of Management Studies Nerul, Navi Mumbai
meghasw@gmail.com

Dr.Suhasini Vijaykumar, Principal,
Bharati Vidyapeeth's Management and Technology,
Sector-8, CBD Belapur,
Navi Mumbai.

ABSTRACT
Machine learning (ML), which has been studied since the 1950s, is a branch of artificial intelligence that allows machines to adapt and learn from data rather than being programmed. In more recent times, ML has been used in systems including robotics, autonomous vehicles, smart power grids, and process control. These kinds of systems directly affect human safety and life. Their ML models must therefore be protected from adversaries that aim to damage users or compromise their privacy. The many advantages that machine learning has provided for security and CPS/IoT, both generally and specifically, including the improvement of intrusion detection systems and decision accuracy in CPS/IoT. CPS stands for Cyber-Physical Systems. High-tech sensors combined with actual physical places make up cyber-physical systems (CPS). In the context of CPS systems, these intimate couplings of sensors with communication infrastructure that are inextricably linked to society's Crucial Infrastructures (C.I.) are more frequently observed.
The use of adversarial machine learning research to cyber-physical systems (CPS) like autonomous vehicles and healthcare is examined in this paper. As a result, this study will provide as a springboard for further investigation into adversarial ML and CPSs. Providing a deeper grasp of this new trans disciplinary methodology is the goal of this study. The characteristics of CPSs are discussed.
Keywords: Machine Learning, ML, Cyber Physical System, CPS

Introduction

The internet has played a significant role in the digital revolution, enabling platform similar to bank, edification, online exchange, , medical, and government services. Wireless communication, mobile devices, and other technological advancements like parallel/distributed computing, cloud computing, and nanotechnology have contributed to this progress. With the advent of wireless sensors, the internet has expanded to incorporate hardware devices that connect to it, giving rise to the Internet-of-Things (IoT) and wireless sensor networks (WSN). This development has pressed the frontiers of study in field like manufacturing, transportation, healthcare, and security, among others. To ensure the stability and reliability of extensive and organically distributed cyber-physical systems, a variety of system requirements engineering approaches should be implemented, focused on both hardware and software. Machine learning has emerged as a ubiquitous tool to analyze complex network data without being explicitly programmed and is increasingly used to analyze CPS systems. However, CPS systems face increasing security challenges as attacks may come from both cyber and physical interfaces, making conventional cyber security methods ineffective. It is suggested that the organized pathway for large-scale and organically dispersed cyber-physical systems be steady and reliable with extremely composite distributed as well as central control. There are many different system requirements engineering methodologies, and both software and hardware should be given priority. (Wankhade, 2020).

Literature Review

AzadS ,Sabrina , Wasimi (2019) Systems typically refer to the integration of vehicular systems with computational and communication capabilities, allowing them to communicate with other vehicles and infrastructure to enhance safety, efficiency, and convenience.

Bomfim (2020)performed a temporal study of the most studied areas in which machine learning has been applied beginning with the year that the gathered materials were published. The aim was to identify the increasing pattern in research between 2010 and 2019. The study highlights the subjects that have received the most attention recently and offers insights into the implementation of machine learning in the CPS field. Synopsis of a study or research report that analyses.

The study also notes that different algorithms have different sensitivities to system size and imbalanced data. For example, KNN may execute improved in small-sized systems but worse in large-sized systems, while SVM performs better in large-scale systems. The study also observes a phase change that is the smallest amount of capacity accessible to attackers to construct unobservable attacks.

Chandramohan, Poel, Meijerink, & Heijenk (2019) discusses the importance of timely and accurate incident response to mitigate the impact of attacks and prevent further damage to the vehicular system. It also notes the significance of regulatory compliance and standards in ensuring the security and safety of cyber-physical vehicular systems.

Goodfellow, Shlens, & Szegedy(2014) It is particularly well-liked since producing adversarial examples is so simple. utilized to gauge the effectiveness of most users at first, but was later discovered to be a relatively weaker type of adversarial attacks.

Hoel, Wolff & Laine (2018) In self-driving cars, a DQN is trained to make decisions on its own. High level inputs are also subjected to a CNN to expedite learning and enhance the performance of the agent.

Ozay , Esnaola, Tunay & Kulkarni (2015), the study suggests that machine learning algorithms can be effective in detecting attacks, and the choice of algorithm should be based on the system size, data imbalance, and the type of attack being targeted.

Pan, Zheng, Chen, Luan, Bootwala, & Batten (2017) covers different types of attacks on vehicular systems, including denial-of-service attacks, intrusion attacks, and physical attacks. It discusses various approaches to prevent and detect these attacks, including using cryptographic techniques, intrusion detection systems, and anomaly detection techniques. The paper also highlights the importance of secure communication protocols and secure data storage mechanisms to prevent unauthorized access and data breaches.

Radanliev , Roure , Kleek M ,Santos O & Ani U.(2021) In this research, a new hierarchical cascading framework is presented that proposes methods for modeling imperative mechanisms in linked, complex, interconnected systems. It describe the links and interdependencies between components to both external and internal IoT services and CPS in summary maps in crucial environments for AI, such as IoT. The imperative categories for the development of artificial cognition in CPS are identified by the summary map.

Overall, the paper emphasizes the need for a comprehensive and multi-faceted approach to prevent and detect attacks on vehicular systems, combining technical solutions, best practices, and regulatory compliance.

CPES, being mission-critical components of power grid infrastructure, are particularly vulnerable to attacks that can result in disastrous consequences. To enhance the security of CPES, it is suggested to leverage tested capabilities to simulate power system operating conditions, identify security flaws, create security measures, and assess grid operation in fault-induced or maliciously created scenarios. This can help identify and mitigate potential risks before they result in actual harm to the power grid infrastructure.

Xing, Su, Zhang, Peng, Pu, & Luo (2019) An incentive system based on Q-learning to persuade autonomous vehicles to disclose hazards in order to increase their trust values and utilities.
Zografopoulos , Ospina , Liu , & Konstantinou(2021) are discussing the importance of Cyber-Physical Systems (CPS) and the potential risks associated with attacks on these systems, particularly Cyber-Physical Energy Systems (CPES) within power grid infrastructure. CPS is designs that interact with the physical world by using both analogue and digital components as well as communication and computing resources.

Objectives of study

Machine learning (ML) and CPS are two unified fields with diverse applications across several domains. The integration of ML techniques in CPS has opened up new avenues for research, development, and innovation. In this paper, we focus primarily on how the ML paradigm impacts for these two fields.

Domain Specific Modeling

Researchers have recently looked into a number of model-based design techniques for cyber-physical systems, including event modeling, physical modeling, and real-time assurance. Model-based software design techniques like domain-specific modeling, model-integrated computing, and model-driven development (MDD) employing the Unified Modeling Language (UML) have been widely used in CPS design. Domain-specific modeling involves creating tailored models using specialized modeling languages or tools that are designed to capture the unique characteristics and requirements of a specific domain. An example of DSM design flow abstractions is exposed in Figure 1. These model-based design techniques have also been applied to embedded systems blueprint and have shown promise in improving system reliability and reducing development time and costs. However, challenges and limitations must be considered and addressed during the design process.

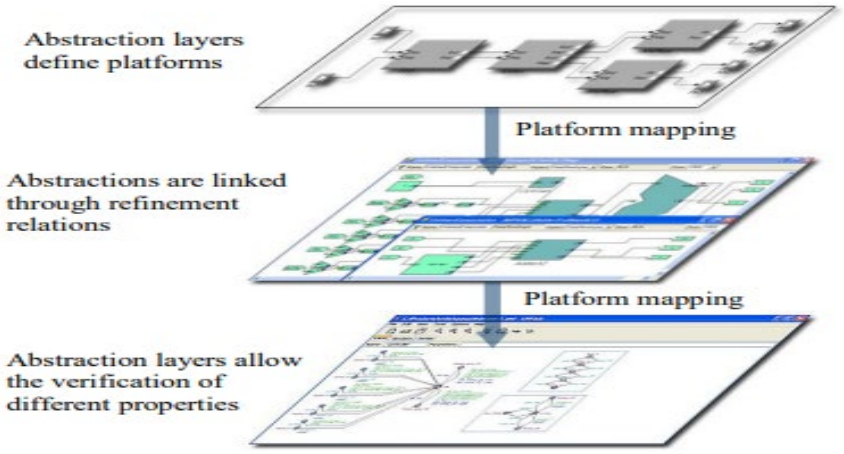

Figure.1 Design flow for DSM (Source: https://www.semanticscholar.org)

Dimensions of Machine Learning Schemes

This paper provides a brief review of different machine learning schemes categorized into reinforcement, unsupervised, and supervised learning. Based on their results, machine learning techniques can also be divided into classification, regression, dimensionality reduction, clustering, and density estimation categories. In supervised learning, input-output pairs that have been labeled during training serve as the basis for learning a function or model that maps inputs to outputs. Depending on whether the target labels are discrete or numeric, it can also be further divided into classification and regression.

Classification deals with a restricted set of definite classes, which can be binary or multitudinous, while regression focuses on numeric outputs.

Regression: The objective of regression, a sort of supervised learning, is to forecast a continuous output variable from input characteristics. The output variable can take any value within a certain range, not just probabilities like in your example. In the case of binary classification, where there are only two possible output values (e.g., malware or not malware), the problem is often formulated as logistic regression, which predicts the probability of the positive class.

Unsupervised Learning: The goal in unsupervised learning is to discover models or structure in the facts devoid of using some explicit labels or targets. This can include tasks like clustering, where the aim is to group similar instances together, or dimensionality decrease, where the goal is to reduce the number of features while holding as a great deal in order as probable. The evaluation of unsupervised learning models can be more challenging because there are no clear targets to compare the predictions against, but there are still various ways to assess their performance, such as measuring how well the model captures the underlying data distribution or how well it aids in downstream tasks like classification.

In fact, reinforcement learning involves an agent interacting with its environment, acting, and then receiving rewards or punishments based on its actions. Learning a policy that maximizes the cumulative reward over time is the aim.

About policy search and value function approximation, the two primary reinforcement learning techniques. Whereas value function approximation approximates the expected benefits of each action in each state, policy search directly seeks the best course of action. The state-action value function, which calculates the expected cumulative reward of performing a specific action in a specific state and then applying the best course of action, is the quality function.

Policy Search: Policy search is a category of reinforcement learning algorithm that directly optimizes the policy, i.e., the mapping from states to actions, without estimating a value function. There are various methods for policy search, including gradient-based methods that utilize the gradient of the predictable incentive by means of to the policy parameters to revise the policy, and gradient-free methods that search for the optimal policy without using gradients. Examples of gradient-based policy search algorithms include policy gradient methods such as REINFORCE, while examples of gradient-free methods include evolutionary algorithms such as genetic algorithms (Gibney2016).

Value Function Approximation: Value function approximation is another type of reinforcement learning algorithm that estimates the expected cumulative reward of taking each action in each state. This can be done using various techniques, such as Monte Carlo methods or temporal difference learning. Examples of value function approximation algorithms include Q-learning and SARSA(Arulkumaran, Deisenroth, Brundage, & Bharath 2017).

Application Domain

CPS are utilized in a wide range of applications, including engineering tools for robots and biological systems, traffic, safety, automobiles, manufacturing and development controls, energy efficiency, environmental monitoring and administration, etc (SultanovsE, Skorobogatjko A.,& Romanovs A. 2016). At the moment, CPSs combine intelligent roadways with unmanned vehicles. WSN and embedded/real-time system advancements have opened up new possibilities for unmanned vehicle applications.

As illustrated in Figure 2, we can research various views using this prototype platform

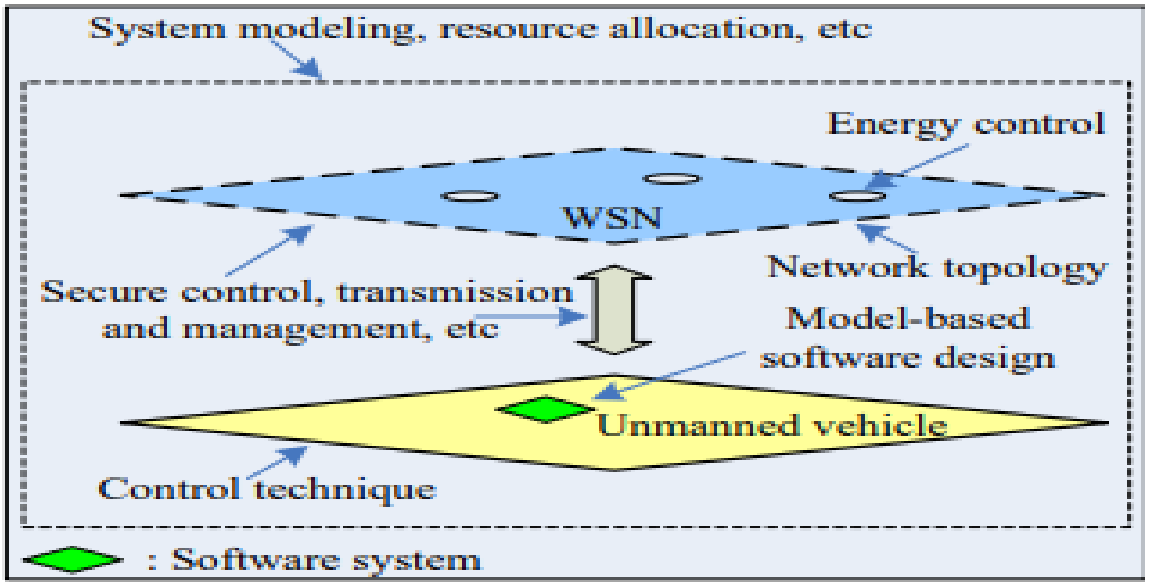

Figure 2 Study from different perspective (Source: https://www.semanticscholar.org)

In contrast to use in these other fields, cyber-physical systems in medicine must have the most exact, succinct, and extremely minimal likelihood of error. Technologies that are intended to help people cannot hurt their fitness. Also, people should have access to trustworthy, safe, and efficient CPS healthcare. CPS offers a variety of applications in the field of healthcare, including assisted living, hospitals, and aged care.

Machine Learning Applied For CPS System

Although they are linked, AI and ML are not the same. The design of intelligent systems that can carry out activities that traditionally require human intelligence, including speech recognition or making decisions based on complex data, is covered within the broader topic of AI. The goal of machine learning (ML), on the other hand, is to teach computers how to learn from data and make predictions or judgments based on that data.

The two primary categories of ML algorithms are supervised learning and unsupervised learning. With supervised learning, each data point is connected to the appropriate output, and the system is trained on a labeled dataset. This dataset is used by the algorithm to train a function that converts inputs into outputs. The algorithm in unsupervised learning is responsible with finding patterns or relationships in a dataset that is left unlabeled.

There are several real-world uses for AI and ML in industries including healthcare, banking, transportation, and manufacturing. For instance, AI and ML algorithms can be used to improve quality control in manufacturing, forecast credit risk in lending, and diagnose diseases from medical pictures. Although there are a lot of potential advantages of AI and ML, there are also worries about the ethical and societal ramifications of these technologies, such as the possibility of bias and discrimination in algorithms used for decision-making. As a result, it's critical that these technologies be developed responsibly and openly. Specific uses, system complexity, and building necessities necessitate particular design. Figure3. An example of CPS.

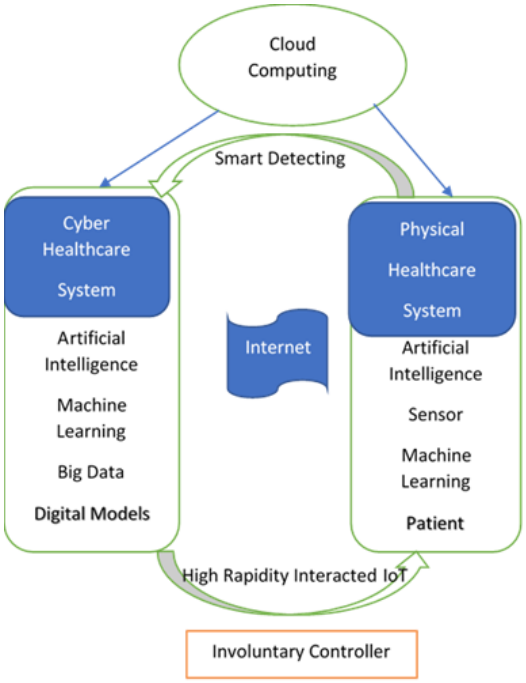

Figure 3. Illustration of Cyber Physical System in healthcare(Source:https://www.igi-global.com)

Conclusion

It is important to note that while machine learning can provide significant benefits to CPS systems; it is not a silver bullet for all cyber security challenges. Efficient cyber security involve a versatile advances which take in together practical clarifications and human factors like training as well as awareness. In addition, there is a need for regulatory frameworks and industry standards to ensure that security is built into CPS systems from the outset. As machine learning continues to evolve, it is crucial that we keep pace with its developments and integrate it into our cyber security strategies in a responsible and effective manner. By doing so, we can reap the benefits of these technologies as reducing the hazards. The integration of ML in CPS has opened up new avenues for research and development, enabling the creation of more intelligent, efficient, and reliable systems. With the rising accessibility of information as well as proceeds in ML techniques, we can expect to see further innovation and growth in these areas in the future.

References

Arulkumaran K., Deisenroth M. ,Brundage, and Bharath A (2017), "Deep reinforcement learning: A brief survey," IEEE Signal Processing Magazine, vol. 34, no. 6, pp. 26–38, 2017. (1)

Azad S ,Sabrina F, Wasimi S(2019) , 'Transformation of Smart Grid using Machine Learning'29th Australasian Universities Power Engineering Conference (AUPEC)

BomfimT. (2020) 'Evolution of Machine Learning in Smart Grids',IEEE 2020 , International Conference on Smart Energy Grid Engineering

Chandramohan A., Poel M, Meijerink B & Heijenk (2019), "Machine learning for cooperative driving in a multi-lane highway environment," Wireless Days (WD), pp. 1–4 .

Gibney E. (2016), "Google ai algorithm masters ancient game of go," Nature News, vol. 529, no. 7587, p. 445, 2016.(5)

Goodfellow J., Shlens J, and Szegedy C. (2014), "Explaining and harnessing adversarial examples," arXiv preprint arXiv:1412.6572

Hoel K., Wolff & Laine L (2018), "Automated speed and lane change decision making using deep reinforcement learning," 21st International Conference on Intelligent Transportation Systems (ITSC), pp. 2148–2155, IEEE

Liang , William H. , Liao W , Gao W, and Wei Yu(2019) , "Machine Learning for Security and the Internet of Things: the Good, the Bad, and the Ugly Fan"(8)

Ozay M., Esnaola, Tunay & Kulkarni S. (2015), "Machine Learning Methods for Attack Detection in the Smart Grid" ,IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS

Pan L, Zheng X., Chen, Luan, Bootwala, and Batten(2017),"Cyber security attacks to modern vehicular systems," Journal of Information SecurityandApplications

Radanliev P. Roure D. Kleek M ,Santos O & Ani U.(2021) ," Artificial intelligence in cyber physical systems" AI Soc . 2021;36(3):783-796. doi: 10.1007/s00146-020-01049-0. Epub 2020 Aug 27.

Wankhade M. & Vijaykumar S. (2020) "Cyber Physical System Framework: An Apropos Study " Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC 2020) IEEE Xplore Part Number: CFP20J06-ART; ISBN: 978-1-7281-2813-

Wan J, Yan H, Suo H and Fang Li, &Caufeng Z, 2021, "Advances in Cyber-Physical Systems Research " TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 5, NO.

Wankhade M. & Kottur S. 2021, "Healthcare and Cyber Physical Systems",www.igi-global.com/chapter/healthcare-and-cyber-physicalsystems/288817?camid=4v1

Xing, Z. Su, N. Zhang, Peng, H. Pu, and J. Luo (2019), "Trustevaluation-based intrusion detection and reinforcement learning in autonomous driving," IEEE Network, vol. 33, pp. 54–60, Sep. 2019

Zografopoulos I , Ospina J , Liu X, & Konstantinou C(2021) , "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies " IEEE

