CHAPMAN & HALL/CRC CYBER-PHYSICAL SYSTEMS

Intelligent Security Solutions for Cyber-Physical Systems

Edited by Vandana Mohindru Sood, Yashwant Singh, Bharat Bhargava, and Sushil Kumar Narang

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Intelligent Security Solutions for Cyber-Physical Systems

A cyber-physical system (CPS) is a computer system in which a mechanism is controlled or monitored by computer-based algorithms and involves transdisciplinary approaches, merging theories of cybernetics, mechatronics, design, and process science. This text mainly concentrates on offering a foundational theoretical underpinning and a comprehensive and coherent review of intelligent security solutions for cyber-physical systems.

Features:

- Provides an overview of cyber-physical systems (CPSs) along with security concepts like attack detection methods, CPS failures, and risk identification and management.
- Showcases cyber-physical systems (CPSs) security solutions, lightweight cryptographic solutions, CPS forensics, etc.
- Emphasizes machine learning methods for behavior-based intrusion detection in cyber-physical systems (CPSs), resilient machine learning for networked CPS, fog computing industrial CPS, etc.
- Elaborates classification of network abnormalities in Internet of Things–based cyber-physical systems (CPSs) using deep learning.
- Includes case studies and applications in the domain of smart grid systems, industrial control systems, smart manufacturing, social network and gaming, electric power grid and energy systems, etc.

Chapman & Hall/CRC Cyber-Physical Systems

Series Editors:

Jyotir Moy Chatterjee, Lord Buddha Education Foundation, Kathmandu, Nepal

Vishal Jain, Sharda University, Greater Noida, India

Cyber-Physical Systems: A Comprehensive Guide
By: Nonita Sharma, L K Awasthi, Monika Mangla, K P Sharma, Rohit Kumar

Introduction to the Cyber Ranges
By: Bishwajeet Pandey and Shabeer Ahmad

Security Analytics: A Data Centric Approach to Information Security
By: Mehak Khurana, Shilpa Mahajan

Security and Resilience of Cyber Physical Systems
By: Krishan Kumar, Sunny Behal, Abhinav Bhandari, Sajal Bhatia

Cyber Security Applications for Industry 4.0
By: R Sujatha, G Prakash, Noor Zaman Jhanjhi

Cyber Physical Systems: Concepts and Applications
By: Anupam Baliyan, Kuldeep Singh Kaswan, Naresh Kumar, Kamal Upreti, Ramani Kannan

Intelligent Security Solutions for Cyber-Physical Systems
By: Vandana Mohindru Sood, Yashwant Singh, Bharat Bhargava, Sushil Kumar Narang

For more information on this series please visit: https://www.routledge.com/Chapman--HallCRC-Cyber-Physical-Systems/book-series/CHCPS?pd=published,forthcoming&pg=1&pp=12&so=pub&view=list?pd=published,forthcoming&pg=1&pp=12&so=pub&view=list

Intelligent Security Solutions for Cyber-Physical Systems

Edited by
Vandana Mohindru Sood
Yashwant Singh
Bharat Bhargava
Sushil Kumar Narang

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Front cover image: metamorworks/Shutterstock

First edition published 2024
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 978-1-032-52152-7 (hbk)
ISBN: 978-1-032-52319-4 (pbk)
ISBN: 978-1-003-40610-5 (ebk)

DOI: 10.1201/9781003406105

Typeset in Times
by SPi Technologies India Pvt Ltd (Straive)

Contents

About the Editors

Dr. Vandana Mohindru Sood is an assistant professor in the Department of Computer Science and Engineering (Artificial Intelligence) at Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India, since 2021. She has more than 11 years of experience in teaching and research. She completed her PhD in Computer Science and Engineering from Jaypee University of Information Technology, Himachal Pradesh, India. Dr. Vandana is a renowned researcher in the areas of the Internet of Things, Wireless Sensor Networks, Security, Blockchain, Cryptography, UAV, and Machine Learning. She has published more than 30 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, etc. She has 376 citations and a H-Index of 13. She has organized international conferences and chaired various sessions during IEEE and Springer conferences. She has published 10 utility patents, 4 design patents granted, and edited 3 books.

Prof. Yashwant Singh is a professor and head of the Department of Computer Science & Information Technology at the Central University of Jammu since 2017. He completed his PhD at Himachal Pradesh University, Shimla. His research interests lie in the Internet of Things, Wireless Sensor Networks, and ICS/SCADA Cyber Security, ranging from theory to design to implementation. He has collaborated actively with researchers in several other disciplines of Computer Science, particularly Machine Learning, Electrical Engineering, and Cyber-Physical Systems. He has served on 30 International Conferences and Workshop Programs as a committee member. He currently serves as a coordinator of the Kalam Centre for Science and Technology (KCST), Computational System Security System Vertical at the Central University of Jammu established by DRDO. Yashwant has published more than 80 research articles in international journals, international conferences, and book chapters of repute. He has 1,468 citations and a H-Index of 20. He is executing a research project on IoT vulnerability worth Rs. 46.32 Lakhs sponsored by DRDO and another project on cybersecurity worth 12.19 lakhs sponsored by the National Commission for Women. He is a visiting professor at Jan Wyzykowski University, Polkowice, Poland.

Prof. Bharat Bhargava is a professor of the Department of Computer Science with a courtesy appointment in the School of Electrical & Computer Engineering at Purdue University. Professor Bhargava is conducting research on security and privacy issues in distributed systems. Professor Bhargava is a recipient of seven best paper awards at various international computer science conferences. Professor Bhargava is a Fellow of the Institute of Electrical and Electronics Engineers and the Institute of Electronics and Telecommunication Engineers. He serves on seven editorial boards of international journals. He also served on the IEEE Computer Society on Technical Achievement award and Fellow committees. Professor Bhargava is the founder of the IEEE Symposium on Reliable and Distributed Systems, IEEE Conference on Digital Library, and the ACM Conference on Information and Knowledge Management.

Dr. Sushil Kumar Narang is an associate professor and Dean in the Department of Computer Science and Engineering (Artificial Intelligence) at Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India. He completed his Ph.D. at Panjab University, Chandigarh, India. His research on "Feature Extraction and Neural Network Classifiers for Optical Character Recognition for Good Quality Handwritten Gurmukhi and Devnagari Characters" focused on various image processing, machine as well as deep learning algorithms. His research interests lie in programming languages, ranging from theory to design to implementation, Image Processing, Data Analytics, and Machine Learning. Dr. Sushil has published technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, etc. He has collaborated actively with researchers in several other disciplines of computer science, particularly machine learning on real-world use cases. He is a certified Deep Learning Engineer.

Contributors

Bibhudendra Acharya
Department of ECE
National Institute of Technology Raipur
Chhattisgarh, India

Krishnashree Achuthan
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Kerala, India

Sangeeta Arora
KIET Group of Institutions
Delhi-NCR, India

Ankit Ashish
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Devershi Pallavi Bhatt
Department of Computer Applications
Manipal University
Jaipur, India

Moushumi Das
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Kamal Deep Garg
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Hitakshi
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Mohammad Reza Hosenkhan
Faculty of Information and Communication Technology
Universite Des Mascareignes, Mauritius

J. Jithish
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Kerala, India

Gurleen Kaur
Department of Computer Science & Engineering
Chandigarh Group of Colleges
Punjab, India

Gurpreet Kaur
Department of Law
Guru Kashi University
Punjab, India

Tripat Kaur
School of Commerce and Management
GSSDGS Khalsa College
Patiala, India

Veerpal Kaur
Department of Computer Applications
Manipal University
Jaipur, India

Himanshu Khajuria
Amity Institute of Forensic Sciences
Amity University
Uttar Pradesh, India

Neha Koul
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Neerendra Kumar
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Suprava Ranjan Laha
Department of Computer Science and Engineering, FET-ITER
Siksha 'O' Anusandhan (Deemed to be) University
Odisha, India

Sheikh Imroza Manzoor
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Kapil Mehta
Department of Computer Science & Engineering
Chandigarh Group of Colleges
Punjab, India

Meenakshi
Dept. of Computer Science & Technology
Central University of Punjab
Bathinda, Punjab

Zeesha Mishra
Department of ECE
Chhattisgarh Swami Vivekanand Technical University
Chhattisgarh, India

Sushil Kumar Narang
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Debasish Swapnesh Kumar Nayak
Department of Computer Science and Engineering, FET-ITER
Siksha 'O' Anusandhan (Deemed to be) University
Odisha, INDIA

Biswa Prakash Nayak
Amity Institute of Forensic Sciences
Amity University
Uttar Pradesh, India

Binod Kumar Pattanayak
Department of Computer Science and Engineering, FET-ITER
Siksha 'O' Anusandhan (Deemed to be) University
Odisha, India

Saumendra Pattnaik
Department of Computer Science and Engineering, FET-ITER
Siksha 'O' Anusandhan (Deemed to be) University
Odisha, India

G Krishna Pranav
Department of ECE
National Institute of Technology Raipur
Chhattisgarh, India

Saumya Rajvanshi
Department of Computer Science & Engineering
Chandigarh Group of Colleges
Punjab, India

Indranath Roy
Dr. Shakuntala Misra National Rehabilitation University
Lucknow, U.P., India

Asadullah Safi
Dept. of Computer Science & Technology
Central University of Punjab
Punjab, India

Sriram Sankaran
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Kerala, India

Aditya Sharma
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Zakir Ahmad Sheikh
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Chintan Singh
Amity Institute of Forensic Sciences
Amity University
Uttar Pradesh, India

Satwinder Singh
Central University of Punjab, Bathinda
Pune, India

Yashwant Singh
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Vandana Mohindru Sood
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India

Sumegh Tharewal
Symbiosis Institute of Computer Studies and Research (SICSR),
Symbiosis International (Deemed) University (SIU),
Pune, India

Pradeep Kumar Tiwari
Dr. Vishwanath Karad MIT World Peace University
Pune, India

Narinder Verma
Department of Computer Science and Information Technology
Central University of Jammu
Jammu, India

Preface

The concept of cyber-physical systems (CPS) emerges as a cornerstone of contemporary technological breakthroughs in this age where the digital domain closely interleaves with the physical sphere. These systems are radically transforming industries, from smart grids to healthcare, by fusing computing and physical processes together. Yet, with great potential comes great responsibility. As CPS gets more eminent, protecting it against numerous vulnerabilities becomes both a necessity and an intellectual challenge. By going deeply into the core of CPS security, this book, *Intelligent Security Solutions for Cyber-Physical Systems*, seeks to answer this challenge and provides a thorough guide for researchers, experts, and enthusiasts alike.

Section I introduces the foundational concepts and components of CPS. This section elucidates CPS-related layers, components, models, and challenges after providing a broad overview of its design. This primer provides the necessary background for individuals who are new to the field so that the next sections can be contextualized in their proper perspective.

However, without considering the security considerations that go along with CPS, a thorough knowledge of the technology would be incomplete. The security ideas built into CPS are the emphasis of Section II, which also explores the threats and vulnerabilities inherent to these systems. This section presents a comprehensive view of the security landscape surrounding CPS, from assessing potential attack routes to simplifying security policies and risk management techniques.

The focus of Section III of the narrative is on securing the cyber-physical systems against the vulnerabilities described in Section B. Here, we explore the CPS-specific frameworks, solutions, and cryptographic safety measures. This section offers readers tools to not only prevent security breaches but also to identify them, fix them, and prevent them from transpiring again. Topics covered here range from forensics to lightweight cryptographic solutions.

But in the rapidly transforming world of technology, conventional security measures occasionally fall short. The synergy between ML and CPS security is explored in Section IV. This section explains how the power of ML may be utilized to strengthen CPS security with chapters devoted to intrusion detection, fog computing, and big data analytics. Furthermore, subjects like explainable unsupervised ML and reinforcement learning give a preview of what intelligent CPS security solutions will look like in the future.

Finally, Section V focuses on real-world CPS applications across a diversity of fields, including the possibilities of blockchain-enabled CPS and smart grids and healthcare systems. In addition to highlighting the difficulties in each field, the chapters also discuss current trends and speculate on potential future directions.

Our goal in writing this book is dual: First, to present a comprehensive analysis of CPS and the security issues that are inherently present and, second, to provide cutting-edge, intelligent solutions that can be modified and applied in a variety of contexts. This book will act as both a guide and a spark, inspiring you to break new

boundaries in the development of intelligent security solutions for cyber-physical systems.

To the future, where the digital and physical realms coalesce harmoniously and securely, welcome to the world of Intelligent Security Solutions for Cyber-Physical Systems.

Editors

Section I

Introduction to Cyber-Physical Systems

1 Cyber-Physical Systems and Their Emergence in Machine Learning

Moushumi Das and Vandana Mohindru Sood

Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India

1.1 INTRODUCTION: BACKGROUND AND DRIVING FORCES

The cyber-physical system (CPS) is a representation of an Industry 4.0 device that may combine both virtual and physical environments by delivering data processing in real time. A CPS helps any physical system to be equipped with some simulated systems such as a monitor, allowing information about the real world to be studied in the virtual world and choices to be taken to impact the course of the actual world (Duo et al. 2022).

CPS makes information integration, communication, and collaboration easier along with real-time monitoring and worldwide network optimization (Liu et al. 2022). CPSs are built as a system of computing units that communicate around their surroundings using practical inputs as well as output mechanisms. CPSs are a new type of engineering system with sophisticated processing and communication capabilities that execute specific duties within strict real-time constraints (Wu et al. 2023).

Data is frequently exchanged in real time among the many CPS components. All the necessary demands are essential for satisfying their operational demands, allowing the computer system to regulate itself and become conscious, which is especially important in real-time applications (Malik and Saleem 2022).

This is also one of the essential elements of the IIoT and will play an important part in Industry 4.0 enabling intelligent services and programs to execute precisely. They are built on the real-time interchange of various forms of data and sensitive information between cyber and physical systems. CPS development is being pursued by both academics and industry. Given CPS' immense economic potential, implementing CPS into Industry 4.0 will increase German gross value by 267 billion euros by 2025 (Chen et al. 2022).

This is an embedded system network consisting of three fundamental essential components: Sensors, aggregators, and actuators. CPS systems may also observe their environment, adapt, and manage the physical world (Wang et al. 2022a). The major components of cyber-physical systems are depicted in Figure 1.1.

Machine learning is critical for improving the capabilities of CPS by allowing them to learn from data, adapt to changing surroundings, and make intelligent

DOI: 10.1201/9781003406105-2

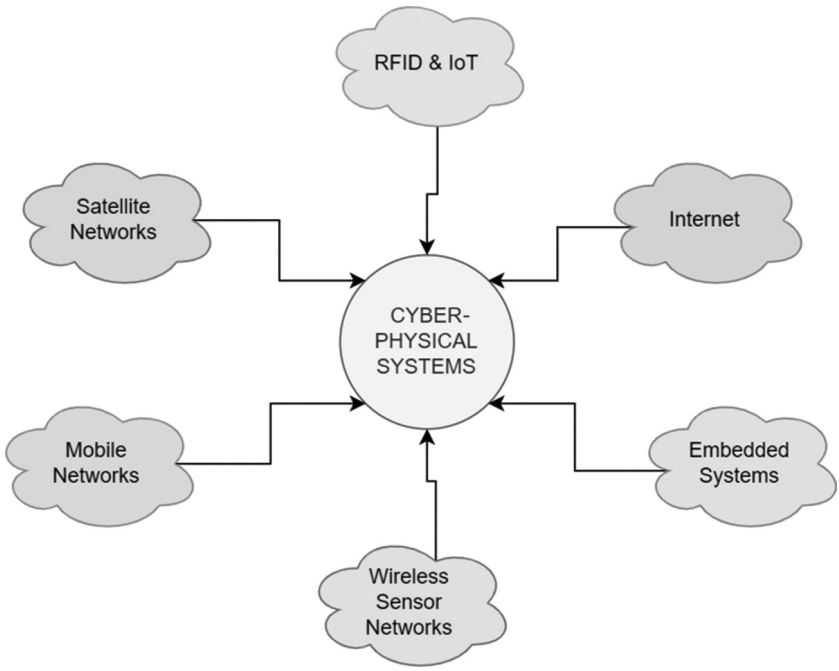

FIGURE 1.1 Components of cyber-physical systems.

judgments. Machine learning algorithms in CPS extract important insights from sensor data, historical knowledge, and real-time observations to allow autonomous decision-making (Ryalat et al. 2023).

In addition, machine learning provides predictive analytics in CPS, where models may estimate system behavior, performance, or demand based on previous data. These forecasts aid in optimizing resource allocation, energy management, and system operation scheduling, resulting in increased efficiency and cost savings. Furthermore, machine learning enables CPS to optimize control techniques. For example, reinforcement learning approaches can develop optimum control policies by exploring the environment and receiving feedback based on preset goals. This enables CPS to change control actions dynamically based on real-time circumstances, resulting in increased system stability, energy economy, and reaction times (Yu et al. 2022).

Furthermore, machine learning facilitates decision-making by evaluating massive volumes of data and finding significant patterns or insights. Machine learning algorithms may aid in decision support, risk assessment, and anomaly classification by training models on historical data and expert knowledge and helping operators and decision-makers to make educated choices in complicated CPS settings. Figure 1.2 depicts many uses of machine learning in cyber-physical systems.

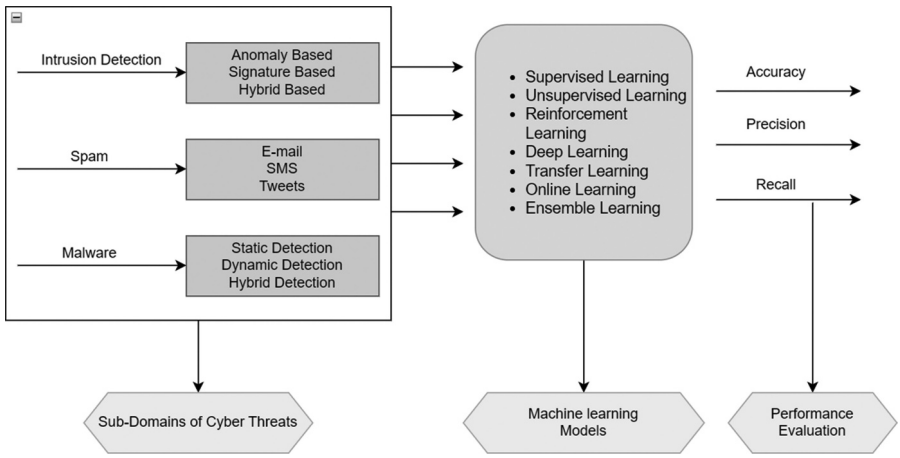

FIGURE 1.2 Machine learning-based applications in cyber-physical systems.

Data play an important part in operating CPSs, especially given that CPSs might have serious effects if choices are generated from information of poor quality. It also may jeopardize safety limitations if inaccurate data is received, time deadlines are missed, or key sensor readings are not received in real time (Rachmawati 2022).

CPSs improve interaction among intelligent manufacturing entities and cyber computer resources. Wearable sensors are often used for recognizing human activity and are a vital aspect of CPS since they are capable of directly and effectively tracking body mobility. CPSs are generated when computing, networking, and physical processes come together. Communication is used in CPSs to exchange information between objects and people. The dependability, latency, and bandwidth of these exchanges are studied. The interplay of items and calculations results in sophisticated IoT implementation (Wang et al. 2022b).

CPSs are widely utilized in the industrial, healthcare, distribution, and transportation industries, as well as in buildings. No doubt CPS is an important part of life, but it is something in need of security for priority, and for that various technologies have been introduced working on the basis of machine learning and deep learning algorithms and some of them have given satisfying results even but still, there is a lot of need for much more improvements in the coming time. A huge amount of data is being generated through CPS; in this stage, machine learning can act as a better technology for working with the data and processing it which also enables CPS to work in a dynamic environment along with intrusion detection (Patel et al. 2023).

Machine learning algorithms may modify models and adapt to changing settings by continuously learning from data, ensuring CPS stays dynamic and robust (Malikopoulos 2023). As CPS evolves, advances in machine learning will play an increasingly important role in determining the future of intelligent, linked systems. The combined application of machine learning and edge computing in CPS decreases latency and bandwidth needs, allowing important applications to make real-time

decisions. The synergistic interaction between machine learning and CPS will lead to breakthrough developments with ramifications in a variety of disciplines (Lee and Kundu 2022; Lee et al. 2020).

However, incorporating machine learning into CPS presents its own set of issues. Furthermore, controlling the computational and communication needs of machine learning algorithms within a resource-constrained CPS context is crucial (Zhang et al. 2021).

1.2 LITERATURE REVIEW

Wiśniewski et al. (2022) provided a novel method for creating a Petri-net-based CPS. This recommended method shortened the time and expense of CPS prototyping by identifying faults in the structure during the early defining stage. The idea was shown with a case investigation into a traffic light intersection in real life. The system was developed, researched, constructed, and eventually confirmed within the FPGA device (Virtex-5 family).

(Amro et al. 2023). In order to exploit encoded common knowledge and make attack expression easier, a new risk assessment method supplemented with specific semantics and MITRE ATT&CK framework components has been presented. The recommended method is then shown by doing a risk analysis for a communication architecture customized for APSs. Furthermore, we present a set of measures based on graph theory for assessing the effect of the detected hazards.

NIRVANA is an innovative technique for prediction validation via uncertainty metrics (Catak et al. 2022). They first utilized prediction-time dropout-based neural networks, and the second was utilized as input for a support vector machine to forecast erroneous labels, and to construct an extremely discriminatory prediction validator model with unpredictable values.

Alohali et al. (2022) suggested a methodology that first conducts data preprocessing. Furthermore, the the fish swarm optimization-based feature selection (IFSO-FS) approach is employed for feature selection. To circumvent the local optima problem, the IFSO approach incorporates the Levy Flight (LF) notion for the searching process of the standard FSO algorithm.

Lee and Kundu (2022) proposed the 5C-CPS framework including a reference structure for DL and DT integration. It provides a complete path for developing and implementing smart manufacturing with enhanced openness, cooperation, and efficiency.

Mishra et al. (2023) proposed a generic NG-CPS framework that included all design components. The smart city was also built as an NG-CPS using the standard NG-CSP architecture. To aid network designers in networking, a cutting-edge protocol framework for smart city NG-CPS was also available.

Thus, Table 1.1 summarizes the various models and techniques presented by many authors and researchers, as well as the research gap between all of them, from which it is concluded that even after the introduction of many new technologies, certain improvements in the models are still required for much better results.

TABLE 1.1
Summary of the Related Work

References	Year	Model/Techniques Proposed	Dataset/Algorithm Used	Advantage	Research Gap
Wiśniewski et al. (2022)	2023	Petri-net-based cyber-physical system	Traffic light crossroad example	Error detection in the systems.	The absence of deadlocks needs to be checked.
Amro et al. (2023)	2023	Risk assessment approach	FMECA	The need for expert judgment was reduced	Estimation of countermeasure effectiveness.
Catak et al. (2022)	2022	NIRVANA (uNcertaInty pRediction ValidAtor iN Ai)	Four real-world CPS datasets	Showed a negative correlation between uncertainty quantification and prediction accuracy.	Prioritization to test DL models
Alohali et al. (2022)	2022	AIMMF-IDS	IFSO algorithm	The performance was enhanced.	Intrusion detection performance is to be boosted.
Lee and Kundu (2022)	2020	Reference architecture for the integration of DL and DT	5C-CPS structure	Better efficiency	Need for improvement in the design of components.
Mishra et al. (2023)	2020	Generic NG-CPS framework	Big data (a large amount of heterogeneous, unstructured data)	Covered all the protocols stack.	Various emerging technologies can be used for better performance.

1.3 ARCHITECTURE

The following is the architecture with functions that are performed by each of the components of cyber-physical systems. Figure 1.3 depicts the architecture of cyber-physical systems (Wu et al. 2023).

a) **Sensors**: The sensors in cyber-physical systems are used to collect data in real time.
b) **Actuators**: Control commands are carried out by matching actuators in order to achieve the intended physical actions (Rai and Sahu 2020).
c) **Computing and Control Centre**: This is in charge of receiving data from sensors. The control center makes matching control choices based on the incoming data to guarantee that physical operations are carried out correctly (Olowononi et al. 2020).
d) **Communication Network**: A communication platform between the command and control center, as well as the physical system is provided by this component. The communication network transmits control signals or choices from the control center to actuators (Luo et al. 2021).

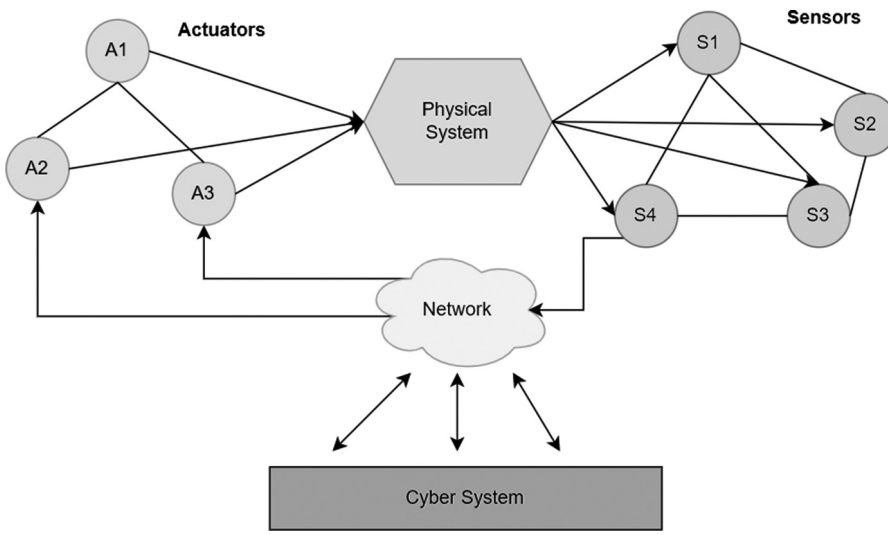

FIGURE 1.3 Architecture of cyber-physical systems.

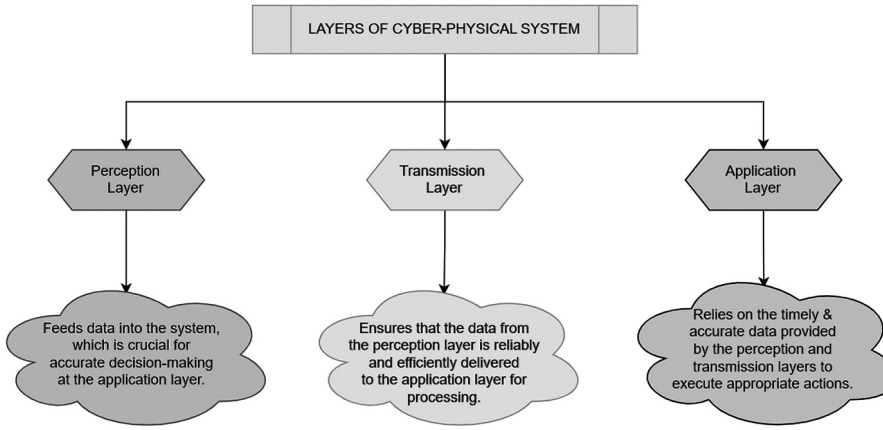

FIGURE 1.4 Various layers of cyber-physical systems.

1.3.1 Different Layers of Cyber-Physical Systems

The perception, transmission, and application layers are the three primary layers in the architecture of cyber-physical systems. Figure 1.4 is a representation of all three layers.

- **Perception Layer**
  It goes by several names, such as the identification layer and the sensing layer. To enable the monitoring, tracking, and analysis of the physical world, these technologies gather data in real time. Information on the quantity of electricity consumed, the temperature, the location, the chemistry, and the biology are some examples of the data that can be gathered depending on the type of sensor. Real-time data generated by these sensors are accessible through both wide-reaching and local network domains. It is often referred to as the sensing layer or the identifying layer. Depending on the type of sensor, data such as electrical consumption, heat, location, chemistry, and biology are also obtained, as are sound and light signals. Real-time data are generated by these sensors over large and local network domains, which the application layer aggregates and analyzes (Hussain et al. 2020).
- **Transmission Layer**
  This layer is considered to be the second layer in the cyber-physical systems (CPS) architecture. This stratum facilitates the processing and transmission of data and facilitates the transmission and exchange of data across the Internet. To handle the proliferation of devices connected to the internet, various protocols, including IPv6, are employed.

  These technologies play a crucial role in facilitating the storage, processing, and transmission of data in a networked environment. Cloud computing platforms enable users to access and utilize computer resources, such as storage and computational power, over the internet (Rathore and Park 2020).

- **Application Layer**
  This is the third layer and exhibits a higher level of interactivity compared to previous layers. The function of this process is to assess the data obtained from the data transfer layer and subsequently give instructions to physical components, including sensors and actuators. The attainment of this objective is accomplished by the utilization of intricate decision-making algorithms that rely on aggregated data. The aforementioned layer further collects and analyzes data collected by the perception layer prior to determining the requisite automated actions.

  To safeguard and preserve privacy, private data must be kept private and not released. Furthermore, this layer needs a robust multifactor authentication method to avoid unauthorized access. The magnitude of produced data has become a serious concern. As a result, safeguarding large data needs effective security systems capable of processing massive volumes of data in a fast and efficient manner (Liu et al. 2022; Liu et al. 2020).

1.3.2 Components of Cyber-Physical Systems

CPS components are utilized to detect information or control signals. CPS components are divided into two types given as following:

a) **Sensing Components**: These components are generally located in the perception layer which usually consists of sensors enabling the information collection which is further transferred to the aggregators. Also, the data are forwarded to the actuators that process it for guaranteeing the decision.
   The primary CPS sensor components are listed below:
   - **Sensors**: Capture and preserve real-world information using a "calibration" technique that helps in assessing the collected data to check its correctness. The sending of data from here is considered a crucial step.
   - **Aggregators**: These are generally located near the transmission layer and are in-charge of processing data received from sensors prior to issuing the corresponding decisions.
   - **Actuators**: The aggregators, as per their decisions, are responsible for ensuring the availability of information to the surrounding environment at the application level (Zhou et al. 2021).

b) **Controlling Components**: The aforementioned components are employed for the purpose of signal regulation, and they have significance in the control, monitoring, and management of signals. Their primary objective is to attain heightened levels of accuracy and safeguard against potential threats such as deliberate signal disruption, extraneous noise, and interference. Moreover, these components are employed to mitigate signal jamming, noise, and interference. The essentiality of Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs), along with their constituent components (such as Operational Technology/Information Technology (OT/IT), Control Loop/Server, and Human–Machine Interface (HMI)/Graphical User Interface (GUI)), has emerged as a direct consequence (Tran et al. 2019).

Following that, we outline the many types of control systems utilized in CPS:

- **Programmable Logic Controllers (PLC)**: To replace the hard-wired layers, initially PLCs are used, but now, they are considered as industrial digital computers governing the production processes.
- **Distributed Control Systems (DCS)**: These are the controlling systems allowing independent controllers for dispersion across the system. The offsite surveillance and oversight approach improves the reliability of the DCS while lowering the installation cost (Leong et al. 2020).
- **Remote Terminal Units (RTU)**: The phrase "Remote Telemetry Unit" refers to microprocessor-controlled electrical equipment, MTU. They do not have any kind of control loops or control algorithms, unlike PLCs. As a result, they tend to be better for wireless communications across broader geographic telemetry zones (Dreossi et al. 2019).

1.4 MODELS OF CYBER-PHYSICAL SYSTEMS

- **Timed Actor CPS**: The functional features of behavior and accuracy, in addition to the nonfunctional characteristics of efficiency and time, are the emphasis of this paradigm. There is a theory that limits specific behavioral sets, enhancing efficiency while lowering complexity. It has a purpose and a classical modification (Jayaratne et al. 2021).
- **Event-Based CPS**: Before actuation decisions can be made in such models, an event must be identified by the appropriate CPS components. Contrarily, individual component time limits vary depending on the nondeterministic system delay brought on by the various CPS processes.
- **Lattice-Based Event Model**: Events are represented in this CPS by event type, as well as both external and internal event characteristics. In the case that these occurrences are collated, they may be used to build a spatiotemporal feature of the particular incident to recognize every observer of the event (Hu et al. 2023).
- **Hybrid-Based CPS Model**: These interactive systems are heterogeneous systems made up of discrete-state and continuous-state interactive systems. Hybrid CPS, in contrast to earlier types, connect over a network, causing delays. Additionally, hybrid CPS systems are incompatible with concurrent system simulation and do not enable hierarchical modeling. As a consequence, the limitations of hybrid system models created by CPS were examined (Latif et al. 2022).

1.5 MACHINE LEARNING IN CYBER-PHYSICAL SYSTEM

Machine learning is critical in cyber-physical systems because it enables real-time data evaluation and adaptive decision-making. Learning patterns from interconnected physical and digital components improves system efficiency, predictive maintenance, and resilience. This synergy enables CPS to evolve intelligently, successfully linking the virtual and physical worlds.

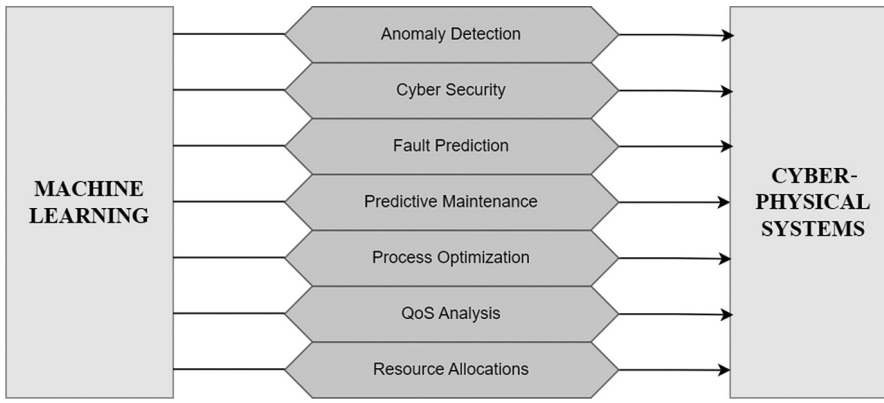

FIGURE 1.5 Various machine learning techniques.

1.5.1 Machine Learning Techniques Useful for Cyber-Physical Systems

CPS applications include driverless cars, industrial control systems, smart grids, healthcare systems, and others. Here are several machine learning approaches that are very beneficial in CPS, as represented in Figure 1.5.

- **Supervised Learning**: Anomaly detection, classification, and regression are all tasks that require supervised learning techniques in CPS. To generate predictions or choices, these algorithms learn from labeled training data. In autonomous cars, for example, supervised learning may be used to recognize things on the road and make judgments based on them.
- **Unsupervised Learning**: CPS uses unsupervised learning approaches to uncover patterns and correlations in data that lacks tagged training samples. To discover groups of similar data points, clustering methods such as k-means and hierarchical clustering can be utilized. This can be useful in discovering abnormalities in CPS or identifying anomalous behaviors.
- **Reinforcement Learning**: Reinforcement learning (RL) is a strong approach in CPS, notably for decision-making and control problems. To maximize a reward signal, RL algorithms learn through contact with the environment. RL may be utilized in CPS to develop optimum policies for tasks such as path planning, resource allocation, and scheduling (Tang et al. 2023).
- **Deep Learning**: Deep learning approaches, particularly deep neural networks, have demonstrated exceptional performance in a variety of CPS applications. Convolutional neural networks (CNNs) are often used for image and video analysis, but recurrent neural networks (RNNs) are better suited to sequential data processing applications like time series analysis or natural language processing.
- **Online Learning**: Online learning algorithms are ideal for CPS applications that use streaming data or operate in dynamic situations. As fresh data becomes available, online learning allows models to adapt and update in

real time. This is useful in scenarios requiring real-time decision-making, such as adaptive control systems or anomaly detection in quickly changing contexts (Jamal et al. 2023).
- **Ensemble Learning**: The process of merging different models to create more accurate predictions or judgments is known as ensemble learning. Ensemble approaches in CPS can improve system dependability and resilience by pooling predictions from many models or algorithms. To increase the accuracy and robustness of CPS applications, ensemble methods like Random Forests, Boosting, and Bagging can be applied.

These machine learning approaches, together with CPS developments, continue to push the frontiers of numerous disciplines. They allow for intelligent decision-making, real-time monitoring, and adaptive control, which results in more efficient, dependable, and secure cyber-physical systems (Li et al. 2020).

1.5.2 Application of Machine Learning in Cyber-Physical Systems

Cyber-physical systems (CPS) are systems that combine physical and computer components to monitor, control, and optimize physical processes in real time. Machine learning techniques might be used to analyze and learn from CPS data, which could then be used to improve performance and optimize processes. Here are some examples of CPS machine learning applications (Presekal et al. 2023):

- **Smart Grids**: Machine learning algorithms can be used to analyze data from power grid sensors and estimate real-time power demand and supply. This information might be used to optimize electricity distribution, eliminate energy waste, and reduce carbon emissions.
- **Autonomous Vehicles**: In autonomous vehicles, machine learning algorithms may be used to evaluate data from sensors and cameras, allowing them to make real-time driving decisions such as spotting obstructions, anticipating traffic patterns, and correctly altering speed and direction.
- **Industrial Monitoring**: Machine learning algorithms have the ability to improve industrial operations like production and logistics. These algorithms can analyze sensors and other data to detect equipment faults, optimize production schedules, and boost productivity (Throne and Lăzăroiu 2020).
- **Healthcare Monitoring**: Machine learning algorithms are capable of monitoring vital signs and other health metrics in real time and providing early warnings of potential health risks. This is especially true for chronic diseases like diabetes, where early detection and intervention are critical (Schneble and Thamilarasu 2019).
- **Building Automation**: Machine learning algorithms may help HVAC systems, lighting systems, and other building systems. By utilizing data from sensors and other sources, these algorithms can estimate energy demand, optimize energy usage, and improve overall building comfort and efficiency (Alsufyani et al. 2023).

- **Traffic Management**: Machine learning algorithms can be used to analyze real-time data from traffic sensors and cameras to optimize traffic flow. This can lead to fewer traffic, faster travel times, and better safety.
- **Environmental Monitoring**: Machine learning algorithms may be used to analyze data from sensors and other sources to monitor environmental aspects such as air quality, water quality, and weather patterns. This can aid in the identification of possible threats and the implementation of timely measures to protect public health and the environment (Mohindru et al. 2019).
- **Robotics**: Machine learning algorithms may assist robots in real-world scenarios such as manufacturing, logistics, and healthcare. Robots can adapt to changing situations and make judgments in real time by evaluating data from sensors and cameras, resulting in increased efficiency and production (Mohindru et al. 2020).

1.6 VARIOUS CHALLENGES FACED IN CYBER-PHYSICAL SYSTEMS

- **Privacy**: The CPS is continually collecting massive amounts of data, which most individuals are unaware of. An individual, therefore, has the right to access their own data and know what kind of information is obtained about them by those who gather data and to whom this information is transferred or sold.
- **Dependability**: Through the early implementation of fault-tolerance mechanisms, if the intelligent physical worlds (IPW) can guarantee the CPS's behavior of adaptation, the CPS will be more reliable and offer a sufficient Quality of Service (QoS). While dependability is built on the capacity to react to changing situations in order to overcome and recover from any potential interruption, whether cyber or physical (Kumar et al. 2021).
- **Resiliency**: CPS must be tough to survive accidents and violent assaults. As a result, cybersecurity risks exist in CPS's logical and physical systems. If any of the elements are unreliable, a multiview editor would be appointed to make the appropriate modifications (Rathore et al. 2021).
- **Interaction and Coordination**: These are necessary to maintain the CPS operational at all times. The aspects of the cyber world, on the other hand, are formed on sequences with no chronological significance. In addition, two key approaches to investigating and assessing this issue are explained.

REFERENCES

Alohali, Manal Abdullah, Fahd N. Al-Wesabi, Anwer Mustafa Hilal, Shalini Goel, Deepak Gupta, and Ashish Khanna. "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment." *Cognitive Neurodynamics* 16, no. 5 (2022): 1045–1057.

Alsufyani, Abdulmajeed, Youseef Alotaibi, Alaa Omran Almagrabi, Saleh Ahmed Alghamdi, and Nawal Alsufyani. "Retracted article: Optimized intelligent data management framework for a cyber-physical system for computational applications." *Complex & Intelligent Systems* 9, no. 3 (2023): 2957–2957.