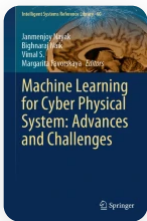


Home > [Machine Learning for Cyber Physical System: Advances and Challenges](#) > Chapter


An In-Depth Analysis of Cyber-Physical Systems: Deep Machine Intelligence Based Security Mitigations

| Chapter | First Online: 12 April 2024

| pp 27–55 | [Cite this chapter](#)



[Machine Learning for Cyber Physical System: Advances and Challenges](#)

[B. K. Tripathy](#) , [G. K. Panda](#) & [Ashok Sahu](#)



 Part of the book series: [Intelligent Systems Reference Library](#) ((ISRL,volume 60))

 50 Accesses

Abstract

Cyber Physical Systems (CPS) is a complex system whose components are both physical and software being intertwined has emerged as a crucial domain and is capable of exhibiting multiple and distinct behavioral modalities handling real-world applications. Over the past two decades, they have evolved into a cornerstone for research and industrial applications, embodying a convergence of physical, biological, and engineered components governed by a computational core. It is a network of interacting elements with physical input and output devices. These systems heavily rely on advanced sensor nodes, communication technologies and control units. Addressing the challenge of deploying sensors in spatially-distributed processes, wireless sensor networks (WSNs) have taken center stage in CPS. WSNs offer a cost-effective solution for monitoring a diverse range of applications, from battlefield surveillance to environmental oversight. The integration of sensor devices within CPS is pivotal in ensuring precision in control and enhancing reliability. Several transdisciplinary approaches like merging theory of cybernetics, mechatronics, design and process science

are involved in a CPS and the process is called as embedded system. Concurrently, technological progress has given rise to sophisticated cyber threats, necessitating ongoing vigilance from researchers to safeguard both physical and virtual systems. This necessitates security mitigation to take measures for reducing these harmful effects or hazards. Deep machine intelligence means machine intelligence based upon deep learning techniques and is most recent AI techniques. This chapter delves into the challenges faced from the security aspects of CPS and their solutions based upon deep machine intelligence, presenting experimental findings through an intrusion detection dataset.

 This is a preview of subscription content, [log in via an institution](#)  to check access.

Access this chapter

Log in via an institution

Chapter

EUR 29.95

Price includes VAT (Pakistan)

Available as PDF

Read on any device

Instant download

Own it forever

Buy Chapter →

eBook

EUR 149.79

Hardcover Book

EUR 179.99

Tax calculation will be finalised at checkout

Purchases are for personal use only

[Institutional subscriptions](#) →

References

1. <https://www.nsf.gov/pubs/2008/nsf08611/nsf08611.htm> [Accessed on 12th Nov 2023]

2. Lee, E.A.: Cyber physical systems: Design challenges. In: Proceedings of the 11th IEEE Intl symposium on object oriented real-time distributed computing (ISORC), pp. 363–369. IEEE, (2008)

[Google Scholar](#)

3. Wu, F.J., Kao, Y.F., Tseng, Y.C.: From wireless sensor networks towards cyber physical systems. *Pervasive Mob. Comput.* **7**(4), 397–413 (2011)

[Article](#) [Google Scholar](#)

4. Jamwal, A., Agrawal, R., Manupati, V.K., Sharma, M., Varela, L., Machado, J.: Development of cyber physical system based manufacturing system design for process optimization. *IOP Conf. Series: Mater. Sci. Eng.* **997**, 012048 (2020)

[Google Scholar](#)

5. Ribeiro, M.T., Singh, S., Guestrin, C.: Why should i trust you? Explaining the predictions of any classifier. In: Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, (2016). <https://doi.org/10.1145/2939672.2939778>

6. Nazarenko, A.A., Safdar, G.A.: Survey on security and privacy issues in cyber physical systems. *AIMS Electron. Electr. Eng.* **3**, 111–143 (2019)

[Article](#) [Google Scholar](#)

7. Hukkeri, G.S., Goudar, R.H.: IoT:issues, challenges, tools, security, solutions and best practices. *Intl J Pure Appl Math*, **120**(6), 12099–12109 (2019)

[Google Scholar](#)

8. Tripathy, B.K., Panda, G.K.: A new approach to manage security against neighborhood attacks in social networks. In: 2010 Intl Conf on advances in social networks analysis and mining, pp.264–269. IEEE, (2010)

[Google Scholar](#)

9. Panda, G.K., Mitra, A., Singh, A., Gour, D., Prasad, A.: Applying l -Diversity in anonymizing collaborative social network. Int. J. IJCSIT 8(2), 324–329 (2010)

[Google Scholar](#)

10. Tripathy, B.K., Panda, G.K., Kumaran, K.: A rough set based efficient l -diversity algorithm. Intl. J. Adv Applied Sci, 302–313 (2011)

[Google Scholar](#)

11. Rad, C.R., Hancu, O., Takacs, I.: Olteanu, G. Smart monitoring of potato crop: A cyber-physical system architecture model in the field of precision agriculture. Agric. Agric. Sci. Procedia 6, 73–79 (2015)

[Google Scholar](#)

12. Ahmad, I., Pothuganti, K.: Smart field monitoring using toxtrac: a cyber-physical system approach in agriculture. In: Proceedings of the 2020 Intl conf on smart electronics and communication (ICOSEC), Trichy, India, pp.10–12 (2020)

[Google Scholar](#)

13. Abid, H., Phuong, L.T.T., Wang, J., Lee, S., Qaisar, S.: V-Cloud: vehicular cyber-physical systems and cloud computing. In: Proc of 4th Intl symposium on applied sciences in biomedical and communication technologies, Spain, (2011)

[Google Scholar](#)

14. Work, D., Bayen, A., Jacobson, Q.: Automotive cyber physical systems in the context of human mobility. In: Proceedings of the national workshop on high-confidence cyber-physical systems, Troy, Miss, USA, (2008)

[Google Scholar](#)

15. Dafflon, B, Moalla, N, Ouzrout, Y.: The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. Int. J. Adv. Manuf. Technol. 113, 2395–2412 (2021)

[Google Scholar](#)

16. He, G., Dang, Y., Zhou, L., Dai, Y., Que, Y., Ji, X.: Architecture model proposal of innovative intelligent manufacturing in the chemical industry based on multi-scale

integration and key technologies. Comput. Chem. Eng. **141**, 106967 (2020)

[Article](#) [Google Scholar](#)

17. Ren, S., Feng, D., Sun, Z., Zhang, R., Chen, L.: “A framework for shop floor material delivery based on real-time manufacturing big data. J. Ambient. Intell. Humaniz. Comput. **10**, 1093–1108 (2019)

[Article](#) [Google Scholar](#)

18. Majeed, A., Lv, J., Peng, T.: A framework for big data driven process analysis and optimization for additive manufacturing. J. Rapid Prototyp. **24**, 735–747 (2018)

[Google Scholar](#)

19. Sampigethaya, K., Poovendran, R.: Aviation cyber–physical systems: foundations for future aircraft and air transport. Proc. of IEEE **101**, 1823–1855 (2013)

[Article](#) [Google Scholar](#)

20. Ying, D.S.X., Venema, D.S., Corman, D.D., Angus, D.I., Sampigethaya, D.R.: Aerospace cyber physical systems–challenges in commercial aviation, Cyber-Physical Systems Virtual Organization

[Google Scholar](#)

21. Sampigethaya, K., Poovendran, R.: Aviation cyber–physical systems: Foundations for future aircraft and air transport. Proc. IEEE **101**, 1834–1855 (2013)

[Article](#) [Google Scholar](#)

22. Huang, Y., Zhao, M., Xue, C.: Joint WCET and update activity minimization for cyber–physical systems. ACM Transactions, TECS **14**, 1–21 (2015)

[Google Scholar](#)

23. Broo, D.G., Boman, U., Törngren, M.: Cyber–physical systems research and education in 2030: Scenarios and strategies. J. Ind. Inf. Integr. **21**, 100192 (2021)

[Google Scholar](#)

24. Perry-Hazan, L., Birnhack, M.: Privacy CCTV and school surveillance in the shadow of imagined law. *Law Soc. Rev.* **50**, 415–449 (2016)

[Article](#) [Google Scholar](#)

25. Singh, K., Sood, S.: Optical fog-assisted cyber-physical system for intelligent surveillance in the education system. *Comput. Appl. Eng. Educ.*, 692–704 (2020)

[Google Scholar](#)

26. Marwedel, P., Engel, M.: Flipped classroom teaching for a cyber-physical system course-an adequate presence-based learning approach in the internet age. In: *Proc of the 10th European Workshop on Microelectronics Education (EWME)*, Tallinn, Estonia, pp.14–16 (2014)

[Google Scholar](#)

27. Taha, W., Hedstrom, L., Xu, F., Duracz, A., Bartha, F.Y., David, J., Gunjan, G.: Flipping a first course on cyber-physical systems: An experience report. In: *Proc of the 2016 workshop on embedded and cyber-physical systems education*. Association for Computing Machinery, New York, NY, USA (2016)

[Google Scholar](#)

28. Singh, V.K., Jain, R.: Situation based control for cyber- physical environments. In: *Proc of the IEEE military communications conf (MILCOM '09)*, Boston, Mass, USA, (2009)

[Google Scholar](#)

29. Meng, W., Liu., Xu, W., Zhou, Z.: A cyber-physical system for public environment perception and emergency handling. In: *Proc of the IEEE Intl Conf on high performance computing and communications*, (2011)

[Google Scholar](#)

30. Hackmann, G., Guo, W., Yan, G., Sun, Z., Lu, C., Dyke, S.: Cyber-physical code sign of distributed structural health monitoring with wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **25**, 63–72 (2013)

[Article](#) [Google Scholar](#)

31. Lin, J., Yu, W., Yang, X., Yang, Q., Fu, X., Zhao, W.: A real-time en-route route guidance decision scheme for transportation-based cyber physical systems. *IEEE Trans. Veh. Technol.* **66**, 2551–2566 (2016)

[Article](#) [Google Scholar](#)

32. Kantarci, B.: Cyber-physical alternate route recommendation system for paramedics in an urban area. In: *Proc of the 2015 IEEE Wireless Communications and Networking Conf (WCNC), USA*, (2015)

[Google Scholar](#)

33. Ko, W.H., Satchidanandan, B., Kumar, P.: Dynamic watermarking-based defense of transportation cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.* **4**, 1–21 (2019)

[Article](#) [Google Scholar](#)

34. Raisin, S.N., Jamaludin, J., Rahalim, F.M., Mohamad, F.A.J., Naeem, B.: Cyber-Physical System (CPS) application-a review. *REKA ELKOMIKA J. Pengabdi. Kpd. Masy.* **1**, 52–65 (2020)

[Google Scholar](#)

35. Wang, J., Abid, H., Lee, S., Shu, L., Xia, F.: A secured health care application architecture for cyber-physical systems. *Control Eng Appl Inform* **13**(3), 101–108 (2011)

[Google Scholar](#)

36. Lounis, A., Hadjidj, A., Bouabdallah, A., Challal, Y.: Secure and scalable cloud-based architecture for e-health Wireless sensor networks. In: *Proc of the Intl Conf on Computer Communication Networks (ICCCN '12), Munich, Germany*, (2012)

[Google Scholar](#)

37. Bocca, M., Tojvola, J., Eriksson, L.M., Hollmen, J., Koivo, H.: Structural health monitoring in wireless sensor networks by the embedded goertzel algorithm. In: *Proc of the IEEE/ACM 2nd Intl Conference on Cyber-Physical Systems (ICCPs '11)*, pp.206–214. Chicago, Ill, USA (2011)

[Google Scholar](#)

38. Jindal, A., Liu, M.: Networked computing in wireless sensor networks for structural health monitoring. In: Proceeding of the IEEE/ACM transactions on networking (TON '12), vol. 20. pp.1203–1216 (2012)

[Google Scholar](#)

39. Akter, F., Kashem, M.A., Islam, M.M., Chowdhury, M.A., Rokunojjaman, M., Uddin, J.: Cyber-Physical System (CPS) based heart disease's prediction model for community clinic using machine learning classifiers. *J. Hunan Univ. Nat. Sci.* **48**, 86–93 (2021)

[Google Scholar](#)

40. Feng, J., Zhu, F., Li, P., Davari, H., Lee, J.: Development of an integrated framework for cyber physical system (CPS)-enabled rehabilitation system. *Int. J. Progn. Health Manag* **12**, 1–10 (2021)

[Google Scholar](#)

41. Liu, J., Wang, P., Lin, J., Chu, C.H.: Model based energy consumption analysis of wireless cyber physical systems. In: Proc of 3rd IEEE Intl Conf on Big data security on cloud, IEEE Intl Conf on High Performance and Smart Computing (Hpssc), and IEEE Intl Conf on intelligent data and security, pp. 219–224. China (2017)

[Google Scholar](#)

42. Panda, G.K., Tripathy, B.K., Padhi, M.K.: Evolution of social IoT world: security issues and research challenges, *Internet of Things (IoT)*, pp.77–98. CRC Press, (2017)

[Google Scholar](#)

43. Panda, G.K., Mishra, D., Nayak, S.: Comprehensive study on social trust with xAI: techniques, evaluation and future direction, (Accepted), explainable, interpretable and transparent AI system, pp.1–22 (Ch-10). CRC Press, (2023)

[Google Scholar](#)

44. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient MAC protocol for wireless sensor networks. In: 21st Annual joint Conf of the IEEE computer and communications societies, vol. 3. pp.1567–1576 (2002)

[Google Scholar](#)

45. Van, T.D., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: Proc of the 1st Intl Conf on embedded networked sensor systems, pp. 171–180. ACM, New York, USA (2003)
- [Google Scholar](#)
46. Liu, Z., Elhanany, I.: RL-MAC: A reinforcement learning based MAC protocol for wireless sensor networks. Intl. J. Sensor Networks 1(3), 117–124 (2006)
- [Article](#) [Google Scholar](#)
47. Shen, Y.J., Wang, M.S.: Broadcast scheduling in wireless sensor networks using fuzzy hopfield neural network. Expert Syst. Appl. 34(2), 900–907 (2008)
- [Article](#) [Google Scholar](#)
48. Kim, M., Park, M.G.: Bayesian statistical modeling of system energy saving effectiveness for MAC protocols of wireless sensor networks. In: Software engineering, artificial intelligence, networking and parallel/distributed computing, studies in computational intelligence, vol. 209, pp. 233–245. Springer. (2009)
- [Google Scholar](#)
49. Chu, Y., Mitchell, P., Grace, D.: ALOHA and q-learning based medium access control for wireless sensor networks. In: Intl symposium on wireless communication systems, pp. 511–515 (2012)
- [Google Scholar](#)
50. Sha, M., Dor, R., Hackmann, G., Lu, C., Kim, T.S., Park, T.: Self adapting MAC layer for wireless sensor networks. Technical Report WUCSE-2013–75, Washington University in St. Louis. Tech Rep (2013)
- [Google Scholar](#)
51. Dash, S., Saras, K., Lenka, M.R., Swain, A.R.: Multi-token based MAC-Cum-routing protocol for WSN: A distributed approach. J. Commun. Softw Syst., 1–12 (2019)
- [Google Scholar](#)
52. Kumar, L.S., Panda, G.K., Tripathy, B.K.: Hyperspectral images: A succinct analytical deep learning study. In: Deep learning applications in image analysis. Studies in big

53. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G.: A survey on jamming attacks and countermeasures in WSNs. *IEEE. Commun. Surv & Tutor.* **11**(4), 42–56 (2009)

[Article](#) [Google Scholar](#)

54. Yin, D., Zhang, L., Yang, K.: A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access* **6**, 24694–24705 (2018)

[Article](#) [Google Scholar](#)

55. Buduma, N., Locascio, N.: *Fundamentals of deep learning: Designing next-generation machine intelligence algorithms*. O'Reilly Media, Inc., O'Reilly (2017)

[Google Scholar](#)

56. Sarker, I.H.: Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN Comput. Sci.* **2**, 420 (2021)

[Article](#) [Google Scholar](#)

57. Irvine The UCI KDD Archive, University of California. KDD Cup 1999 Data, <http://www.kdd.ics.uci.edu/databases/kddcup99/kddcup99/html/> [Accessed 20 April 2023]

Author information

Authors and Affiliations

School of Computer Science Engineering and Information Systems, VIT, Vellore, Tamil Nadu, 632014, India

B. K. Tripathy

MIT School of Biotechnology, Bhubaneswar, Odisha, 751024, India

G. K. Panda

Research Scholar, Utkal University, Bhubaneswar, Odisha, 751004, India

Ashok Sahu

Corresponding author

Correspondence to [B. K. Tripathy](#).

Editor information

Editors and Affiliations

Department of Computer Science, MSCB University, Baripada, India

Janmenjoy Nayak

Department of Computer Application, Veer Surendra Sai University of Technology,

Sambalpur, India

Bighnaraj Naik

Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering,

Coimbatore, Tamil Nadu, India

Vimal S

Institute of Informatics and Telecommunications, Reshetnev Siberian State University of

Science and Technology, Krasnoyarsk, Russia

Margarita Favorskaya

Rights and permissions

[Reprints and permissions](#)

Copyright information

© 2024 The Author(s), under exclusive license to Springer Nature Switzerland AG

About this chapter

Cite this chapter

Tripathy, B.K., Panda, G.K., Sahu, A. (2024). An In-Depth Analysis of Cyber-Physical Systems: Deep Machine Intelligence Based Security Mitigations. In: Nayak, J., Naik, B., S, V., Favorskaya, M. (eds) Machine Learning for Cyber Physical System: Advances and Challenges. Intelligent Systems Reference Library, vol 60. Springer, Cham. https://doi.org/10.1007/978-3-031-54038-7_2

[.RIS](#)↓ [.ENW](#)↓ [.BIB](#)↓

DOI

https://doi.org/10.1007/978-3-031-54038-7_2

Published

12 April 2024

Publisher Name

Springer, Cham

Print ISBN
978-3-031-54037-0

Online ISBN
978-3-031-54038-7

eBook Packages
Intelligent Technologies
and Robotics
Intelligent Technologies
and Robotics (R0)

Publish with us

Policies and ethics 