Call for Book Chapter
Convergence of Deep Learning in Cyber-IoT Systems and Security

To be published under Book Series
Artificial Intelligence And Soft Computing For Industrial Transformation

Scrivener - Wiley Publishing
USA

Indexed by Scopus

And offered to Web of Science

Editors

Dr. Rajdeep Chakraborty
Assistant Professor,
Dept. of CSE, Netaji Subhash Engineering College, Kolkata, India.
E-mail:-
rajdeep.research@gmail.com

Dr. Anupam Ghosh,
Professor,
Dept. of CSE, Netaji Subhash Engineering College, Kolkata, India.
E-Mail:-
anupam.ghosh@rediffmail.com

Dr. J.K. Mandal, Professor,
Dept. of CSE, University of Kalyani, Kalyani, West Bengal, India.
E-mail:-
jkm.cse@gmail.com

Dr. S. Balamurugan, SMIEEE, ACM Distinguished Speaker,
Founder & Chairman - Albert Einstein Engineering and Research Labs (AEER Labs)
Vice Chairman- Renewable Energy Society of India (RESI), India.
Email:-
sbnbala@gmail.com

Scope of the book:

Deep learning is an extended family of machine learning particularly uses artificial neural network for increasing learning capacity of an AI system. So, scope of this book is to integrate deep learning in the area of Cyber Systems, IoT based Systems and Cyber Physical systems including security solutions in all areas. Cyber system technology is a Computer technology especially that which involves the Internet or Cyberspace and Cyber Security includes assessments and penetration testing; provide development and implementation of secure network solutions by architecting and engineering trusted systems into secure systems, and manage audit/intrusion and security technology systems. The Internet of Things (IoT) is a technological concept of connecting multiple devices that have the possibility of switching on and off the web in order to use software and automation processes for smart living. IoT is an innovation that changes the way we organize our lives at home and at work, as well as the way we move and use transportation means and manage industrial machinery. Any object, even people, in terms of smart-phones and wearable's, can be a part of the IoT grid. Internet of Things security focuses on protecting your internet-enabled devices that connect to each other on wireless networks. IoT security is the safety component tied to the Internet of Things, and it strives to protect IoT devices and networks against cybercrime. Cyber-Physical Systems (CPS) is integrations of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. Cyber physical systems are intelligent system that combine hardware and software and are connected through a network as the physical world merges with the virtual world into cyberspace. Cyber-Physical systems have various security challenges.

Multidisciplinary Application areas are also accepted in this book such as control, automation, robotics, Computational Biology and system biology which must focus on Cyber-IoT systems using deep learning techniques.

Therefore, your unpublished work is invited for this book as book chapter publication on listed topics but not limited to.

Tentative Chapters/Topics:

1. **Introductory Chapters on Deep Learning, Deep Learning for IoT systems, Deep Learning for Cyber-Physical System and security aspects.**
2. **Convolution Neural Networks, Recurrent Neural Networks and Deep Belief Networks**
3. **Long Short Term Memory, Deep and restricted Boltzmann Machines and Deep Reinforcement Learning.**
4. **Deep Learning based AI modelling.**
5. **Intrusion detection**
6. **Malware detection**
7. **Detection and categorization of domain names generated by Domain Name generation algorithms (DGAs).**
8. **Spam detection**
9. **Traffic Analysis and Binary Analysis.**
10. **Protocols for IoT Security.**
11. **Authentication Mechanism in IoT Security.**
12. **Distributed, reliable and efficient management of Cyber-Physical Systems.**
13. **Cyber-Physical System Engineering**
14. **Cognitive Cyber-Physical Systems**
15. **Security issues in Cyber-Physical Systems**
16. **Multidisciplinary Application areas**
17. **Case studies and student projects on Deep Learning for Cyber-IoT systems, Cyber-Physical System and Security**

Are very much welcome for this book.

Important Date

Abstract Submission Last Date:

30th April 2021

Acceptance Notification of Abstract:

15th May 2021

Full Paper Last Date:

31st July 2021

Acceptance Notification of Full Chapter:

30th September 2021

Final Camera Ready Submission:

31st October 2021

Deposition of final matter to the publisher:

31st December 2021

For more information and updates you may contact editors or follow the following links.

Important Links

Book Flyer and Website: http://cdlciss2021.in

Book Series: http://www.scrivenerpublishing.com/series.php?id=Artificial%20Intelligence%20and%20Soft%20Computing%20for%20Industrial%20Transformation

Book Chapter Submission and Information: https://easychair.org/conferences/?conf=cdlciss-2021