Call for Chapter(s)

Machine Learning for Security and Privacy in Internet of Healthcare Things

to be published by **Wiley-Scrivener Publishing, USA**

Dear Colleagues

It is our pleasure to invite you to submit a chapter for inclusion in the edited book "Machine Learning for Security and Privacy in Internet of Healthcare Things" to be published by Wiley-Scrivener Publishing, USA. The submitted proposal should have 1-2 page and include sufficient details to be useful for Security and Privacy in Internet of Healthcare Things educators, Industrialists and Readers having security to privacy ranging from basic to recent advances.

Scope of the book

IoT is expanding worldwide in recent years, it also provides new challenges and opportunities related to the cyber security risk in IoT healthcare sector. IoHT devices diagnose the diseases very easily in less time with more accuracy but with the lack of network segmentation, insufficient access control on legacy system as well as enhance the vulnerable surface area that can be exploited by cyber attackers. Most common threats that IoHT devices poses is of data privacy and security. As IOT device transmit and receive data in real time. Cybercriminals attack the system and steal the Personal Health Information (PHI) of both doctors as well as patients. Later on cybercriminal misuse these data to generate fake IDs to buy medical equipment and drugs, which they sell later. Hacker also files false medical Insurance claim on patient's name. Another more significant threat is an integration of multiple network devices which causes hindrance in the implementation of IoT in the healthcare sector. The huge amount of data generated by IoT healthcare devices disrupts the decision making of doctors to diagnose the diseases.

This is an edited book. The main topics for the chapters of this book are:

- Introduction of Internet of Healthcare Things (IoHT).
- Machine Learning and Security challenges in IoHT.
- Case studies of trust in IoHT and Machine Learning.
- Secure Data Transmission network model for IoHT.
- Authentication and Authorization mechanism for IoHT.
- Data Security and Privacy Concern in HealthCare System.
- Security Enhancements in cloud computing based Healthcare System.
- Fog computing based security platform for IoHT.
- Security and Privacy Issue related to IoT based ubiquitous Healthcare System.
- BlockChain for IoHT.
- Big data and Machine learning based secure e-Healthcare System.

All chapters must be original and not simultaneously submitted to another book project, journal or conference. The following important dates will be considered for the submissions:

- **Proposal Submission: ~~August 31, 2020~~ October 15, 2020**
  (1-2 page proposal explaining the work; with single or double-spaced Times New Roman 11 pt. size text)
- **Full Chapter Submission for the Accepted Proposals: ~~September 30, 2020~~ October 31, 2020**
  (details for full paper preparation will be given to the authors)
- **First Round Review Reports: ~~Oct. 15, 2020~~ Nov. 15, 2020**
- **Revised Full Chapter Submission: ~~Oct. 31, 2020~~ Nov. 30, 2020**

Submission Link:

EasyChair
The world for scientists

https://easychair.org/conferences/?conf=mlspioht2021

Inquiries and submissions (Word document) can be forwarded by mail to:

kavitasharma_06@yahoo.co.in and yogitagigras@ncuindia.edu

Editors

Dr. Kavita Sharma, Department of CSE, G. L. Bajaj Institute of Technology and Management, Greater Noida, India.
Email: *kavitasharma_06@yahoo.co.in*

Dr. Yogita Gigras, Department of CSE and IT, The NorthCap University, Gurugram, India.
Email: *yogitagigras@ncuindia.edu*

Dr. D. Jude Hemanth, Department of ECE, Karunya University, Coimbatore, India.
Email: *judehemanth@karunya.edu*

Dr. Ramesh Chandra Poonia, Department of ICT and Natural Sciences, Norwegian University of Science and Technology, Norway.
Email: *rameshcpoonia@gmail.com*