CALL FOR PAPERS- Federated Learning for Cybersecurity in Internet of Things

In traditional machine learning, the data from different sources has to be moved to a central location, where the machine learning models will get trained to understand the patterns existing in the data. Due to the increased applications of Internet of Things (IoT) based applications, sensitive data collected by IoT devices is being transferred to the cloud for training machine learning algorithms to understand the patterns in the data. The sensitive nature of these data can attract malicious users into hacking attempts. The solution to this problem is a machine learning model which gets trained at the source of the data, instead of being trained at central locations like the cloud. Federated Learning is a recent advancement of machine learning, where, instead of moving the data to the central cloud, the machine learning model itself is moved to the source of the data. Hence, Federated Learning has the potential to solve several issues regarding cyber security in IoT based applications.

This special issue solicits high quality research papers on the application of Federated Learning for cybersecurity in Internet of Things. Experimental results or literature review articles on federated learning for cybersecurity in IoT are welcome. The topics for the special issue include but are not limited to:

- Federated learning for intrusion detection in IoT Federated learning with edge computing for cybersecurity in IoT
- Federated learning with blockchain for cybersecurity in IoT Federated learning for security and privacy in IoT
- Federated learning for anomaly detection in IoT
- Big data analytics with federated learning for cybersecurity in IoT
- Federated learning cybersecurity in smart grids
- Federated learning cybersecurity in Industrial IoT
- Federated learning for energy efficiency in IoT
- Federated learning for privacy preservation of the users in social media apps.
- Federated learning for cybersecurity in 5G and beyond

Guest Editors:

1. Dr. Thippa Reddy Gadekallu
   Vellore Institute of Technology, India
   Email: thippareddy.g@vit.ac.in

Short Bio:

Dr. Thippa Reddy Gadekallu is currently working as Associate Professor in School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India. He obtained his B.Tech. in CSE from Nagarjuna University, India, M.Tech. in CSE from Anna University, Chennai, Tamil Nadu, India and completed his Ph.D in VIT, Vellore, Tamil Nadu, India. He has more than 14 years of experience in teaching. He has published more than 80 international/national publications. Currently, his areas of research include Machine Learning, Internet of Things, Deep Neural Networks, Blockchain, Computer Vision.

Google Scholar: https://scholar.google.com/citations?user=nQFCxmkAAAAJ&hl=en&oi=ao

Researchgate: https://www.researchgate.net/profile/Thippa_Gadekallu

2. Dr. Mamoun Alazab
Charles Darwin University, Australia
Email: alazab.m@ieee.org

Short Bio:

Dr Mamoun Alazab is an Associate Professor at the College of Engineering, IT and Environment at Charles Darwin University, Australia. He received his PhD degree in Computer Science from the Federation University of Australia, School of Science, Information Technology and Engineering. He is a cyber security researcher and practitioner with industry and academic experience. Alazab's research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research papers in many international journals and conferences, such as IEEE transactions on Industrial Informatics, IEEE Transactions on Industry Applications, IEEE Transactions on Big Data, IEEE Transactions on Vehicular Technology, Computers & Security, and Future Generation Computing Systems. He delivered many invited and keynote speeches, 24 events in 2019 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), the Australian Communications and Media Authority (ACMA), Westpac, United Nations Office on Drugs and Crime (UNODC), and the Attorney General's Department. He is a Senior Member of the IEEE. He is the Founding chair of the IEEE Northern Territory (NT) Subsection.

3. Dr. Praveen Kumar Reddy
Vellore Institute of Technology, India
Email: praveenkumarreddy@vit.ac.in

Short Bio:

Praveen Kumar Reddy Maddikunta is currently working as Assistant Professor in School of Information Technology and Engineering, VIT, Vellore, Tamil Nadu, India. He was a visiting professor in Guangdong University of Technology, China in 2019. He had worked as Software Developer for Alcatel-Lucent, IBM. He obtained his B. Tech in Computer Science and Engineering from JNT University, A.P and MTech. in Computer Science and Engineering from VIT, Vellore, Tamil Nadu, India and Ph.D Computer Science and Engineering from VIT, Vellore, Tamil Nadu, India. He has published a total of 25 papers in high-status journals (SCI). Currently, Dr. Praveen Kumar Reddy

is working in the area of Energy Aware Applications for Internet of Things (IoT) and High-Performance Computing.

4. Weizheng Wang
Research Associate, City University of Hong Kong, Hong Kong
Email: weizheng.wang@ieee.org

Short Bio:

Weizheng Wang received the B.S. degree in software engineering from Yangzhou University, Yangzhou, China, in 2019, the M.S. degrees in computer science and engineering from the University of Aizu, Aizu-Wakamatsu, Japan, in 2021. Now he is a Research Associate in University of Aizu and pursuing the Ph.D. degree at the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include applied cryptography, blockchain technology and IoT system.

Important Dates:

Submission Deadline: May 31, 2022

First Round Review Due: August 15, 2022

Revision Due: October 15, 2022

Acceptance Notification: January 30, 2023

Final Manuscript Due: February 15, 2022

Publication Date: March 2022

References:

1. Alazab, M., RM, S. P., Parimala, M., Reddy, P., Gadekallu, T. R., & Pham, Q. V. (2021). Federated learning for cybersecurity: concepts, challenges and future directions. IEEE Transactions on Industrial Informatics.
2. Taheri, R., Shojafar, M., Alazab, M., & Tafazolli, R. (2020). FED-IIoT: A robust federated malware detection architecture in industrial IoT. IEEE Transactions on Industrial Informatics.
3. Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated Learning-based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal.
4. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.

5. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., ... & Gadekallu, T. R. (2021). Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions. arXiv preprint arXiv:2106.09527.
6. Pham, Q. V., Dev, K., Maddikunta, P. K. R., Gadekallu, T. R., & Huynh-The, T. (2021). Fusion of federated learning and industrial internet of things: a survey. arXiv preprint arXiv:2101.00798.