Association for Computing Machinery

ACM Transactions on Internet Technology– Special Issue on

Deep Learning Algorithms and Systems for Enhancing Security in Cloud Services

Special Issue Guest Editors

Dr. Gunasekaran Manogaran
(Corresponding GE)
University of California, Davis, USA
gmanogaran@ucdavis.edu

Dr. Hassan Qudrat-Ullah
York University, Toronto, Canada
hassanq@yorku.ca

Dr. Qin Xin
University of the Faroe Islands, Faroe Islands
qinx@setur.fo

Dr. Latifur Khan
The University of Texas at Dallas,Texas, USA
lkhan@utdallas.edu

Important Deadlines

- Manuscript submission: January 30, 2021
- First notification: April 1, 2021
- Submission of revised manuscript: June 1, 2021
- Final notification: July 3, 2021
- Final submission (camera-ready): September 15, 2021

ACM TOIT Editor-in-Chief

Prof. Ling Liu
School of Computer Science, Georgia Institute of Technology
ling.liu@cc.gatech.edu

Cloud services are used in many industries and organizations for management of shared resources with convenient access. They enable various distributed computational data handling proposals and solutions, which benefit both the developers and the users. Despite the growth of cloud services, the security of cloud data has been a primary area where many challenges and threats have been observed. Although advanced cryptographic models and algorithms can be used to overcome certain security threats, the amount of time, space and memory used remain high. To combat these issues and to enhance the security of cloud services, introducing a deep learning-based system will be a flexible solution.

Deep learning has been used in many organizations recently because of its extraordinary pattern recognition and prediction power. Since deep learning uses multimode neural network concepts to simulate activities similar to the working model of the brain, it can be induced and managed in a cloud-based environment. Using deep learning algorithms to train on huge datasets in the cloud environment will make the overall process of computing more effective with low latency. Significant threats such as malware detection, network intrusion, data privacy, and trust issues can be monitored using deep learning algorithms in real time. Unlike other traditional security enhancers, deep learning models are self-taught and have intelligent capabilities of providing disruptive results in identifying threats and enhancing cloud security in the ever-increasing competitive world.

This special issue invites researchers and academicians to discuss and provide various security measures and solutions for intrusion detection, trust enhancement, network penetration prevention, and data theft in cloud services; and also to enhance cloud security by inducing deep learning algorithms and systems into the cloud environment.

Topics of interest include, but are not limited to:

- Deep learning to address location privacy in distributed cloud environment
- Emerging soft computing methodologies in deep learning for enhancing cloud security
- Deep learning for end-to-end secure communications in cloud services
- Deep learning-based cloud strategies for security audit
- Risk assessment for cloud security using deep learning
- The future of deep learning for enhancing cloud security services
- Deep learning to avoid external influences in time series forecasting and analysis
- Deep learning models for countering vulnerabilities in real-time analysis of cloud environment
- Deep learning algorithms and trends to handle big data and cloud security
- Confidential computing environments for enhanced security
- New cloud-based confidential security features developed by major cloud service providers
- Minimizing security, integrity and privacy threats of cloud computing using deep neural network methods

Submission Instructions:
Please refer to http://dl.acm.org/journal/toit/author-guidelines
Please select “Special Issue on Deep Learning Algorithms and Systems for Enhancing Security in Cloud Services” in the TOIT Manuscript Central website.