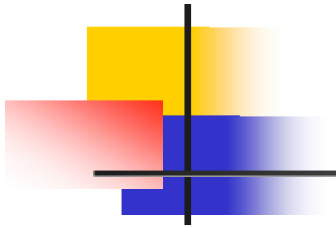


CSE 543

Information Assurance and Security

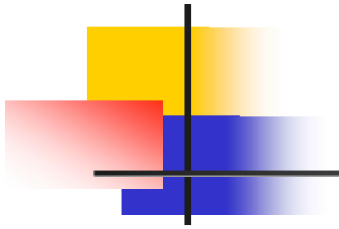
Machine Learning in IA Applications

Professor Stephen S. Yau

Fall 2022

Areas Enabling AI Applications

- Computing paradigms and systems
  - Architecture, hardware, software, ...
- Algorithms
- Smart and big data
- Internet and mobile networks
- Sensing devices
- Semiconductor technologies
- …



IEEE World Congress On Services

September 5-11, 2021 (virtual).

https://conferences.computer.org/services/2021/

July 11-15, 2022 (hybrid) Barcelona, Spain

https://conferences.computer.org/services/2022/

Major Applications of Machine Learning

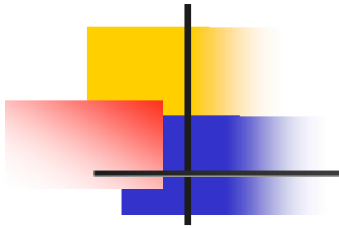
- **Cybersecurity**
- **Speech recognition**
- **Customer service**
- **Pattern recognition**
- **Finances**
- **Healthcare**
- **Transportation**
- **Smart city**
- **…**

Applications of Machine Learning Algorithms to Cybersecurity

- Cloud Systems
- IoT Networks
- Social Networks
- Smart Cities
- Cyber Threat Identification
- Attacks Prediction
- Trusted Coordination of Collaborative Services for Effective Space-Air-Ground-Water Computing and Communications
- …

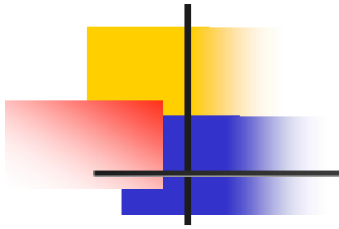
What Is Machine Learning?

Machine learning focuses on the use of ***relevant data and powerful algorithms*** to imitate ***humans*** to learn and improve the accuracy of the ***recognition process*** of applications.



Machine Learning Methods

- Supervised
- Unsupervised (clustering)
- Reinforcement
- Data mining
- Deep Learning
- Statistical machine learning
- …



Neural Networks

- Neural Network is inspired by and resembles the human nervous system and the structure of the human brain.
- It consists of processing units (nodes) organized in input and output layers. The nodes in each layer are connected to nodes in adjacent layers.

References for Machine Learning and IA Applications

1. S. Durga, R. Nag and E. Daniel, "Survey on Machine Learning and Deep Learning Algorithms used in Internet of Things (IoT) Healthcare," Proc. 3rd Int'l Conf. on Computing Methodologies and Communication (ICCMC), 2019, pp. 1018-1022.
2. U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu and M. Stanley, "A brief survey of machine learning methods and their sensor and IoT applications," Proc. 8th Int'l Conf. on Information, Intelligence, Systems & Applications (IISA), 2017, pp. 1-8.
3. A. Arpteg, B. Brinne, L. Crnkovic-Friis and J. Bosch, "Software Engineering Challenges of Deep Learning," Proc. 44th Euromicro Conf. on Software Engineering and Advanced Applications (SEAA), 2018, pp. 50-59.

References for Machine Learning and IA Applications

4. P. Podder, S. Bharati, M. R. H. Mondal, P. K. Paul, and U. Kose, "Artificial Neural Network for Cybersecurity: A Comprehensive Review," Jour. Information Assurance and Security, 2021, oo. 10-26.
5. S. S. Yau, A. B. Buduru and V. Nagaraja, "Protecting Critical Gloud Infrastructures with Predictive Capability", Proc. IEEE 8th Int'l Conf. on Cloud Computing, New York, NY, June 2015, pp. 1119-1124
6. S. Guha, S. S. Yau and A. B. Buduru, "Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection", Proc. IEEE Int'l Conf. on Dependable, Autonomic and Secure Computing (DASC), Auckland, New Zealand, August 2016, pp. 414-419