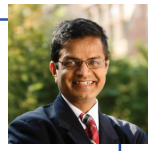
Our Research on Security of Multi-Cloud, Health Care, Industrial Control Systems



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Cyber-security Group Meeting, WUSTL, Oct 4, 2019

These slides are at:
http://www.cse.wustl.edu/~jain/talks/sec_rj.htm

1. Multi-Cloud Security
2. Health Care Security
3. Industrial Systems Security
4. Innovations in AI
5. Innovations in Blockchains

Our Research Projects

1. Multi-Cloud Management: Machine learning for Fault and performance management
2. Multi-Cloud for 5G: Network Function Virtualization Micro-edge computing, micro-service placement
3. Industrial Control Systems **Security**
4. Healthcare **Security**
5. Multi-Cloud **Security**: Scientific Collaboration
6. Blockchains for **Security**
7. Communication using UAVs

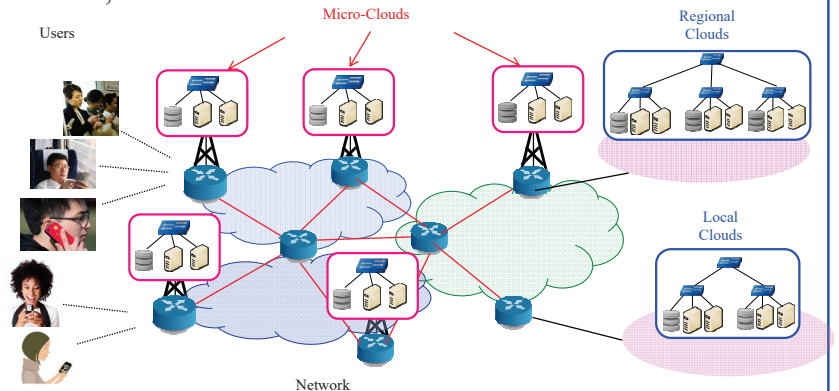
} 5 Funded Research Projects
} 3 on Security
} Approved
} Pending

Innovations:

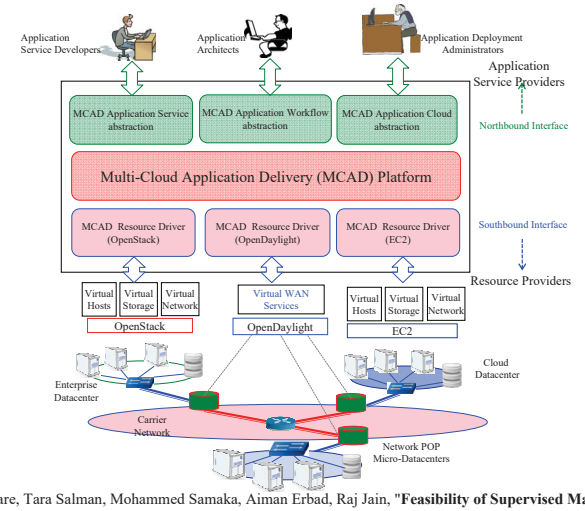
1. Machine learning and Deep Learning
2. Blockchains

1. Multi-Cloud Security

- Local and regional clouds ⇒ Fog Computing
- Internal intra-cloud threats, inter-cloud trust issues, external threats, threats on the interconnection network

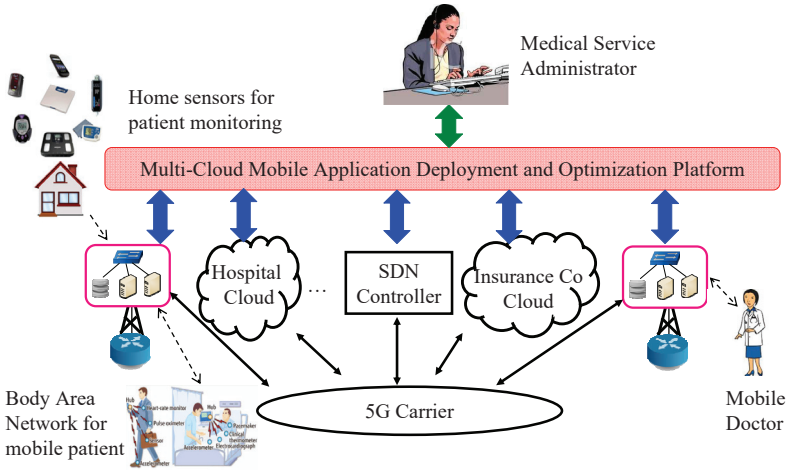


OpenADN Multi-Cloud Management



Ref: Deval Bhamare, Tara Salman, Mohammed Samaka, Aiman Erbad, Raj Jain, "**Feasibility of Supervised Machine Learning for Cloud Security**," 3rd International Conference on Information Science and Security (ICISS2016), December 19th - 22nd, 2016, Pattaya, Thailand, http://www.cse.wustl.edu/~jain/papers/iciss16.htm

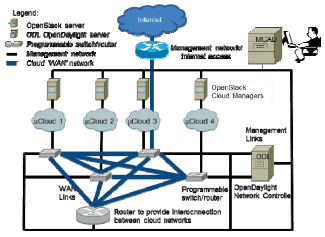
Mobile Healthcare Use Case

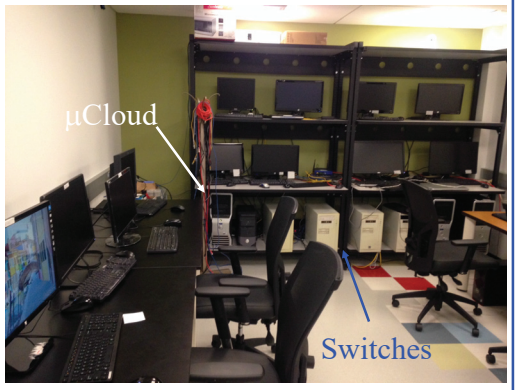


Ref: Tara Salman, Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "**Machine Learning for Anomaly Detection and Categorization in Multi-cloud Environments**," The 4th IEEE International Conference on Cyber Security and Cloud Computing, June 26-28, 2017, http://www.cse.wustl.edu/~jain/papers/cscloud.htm

Our Multi-Cloud Testbed

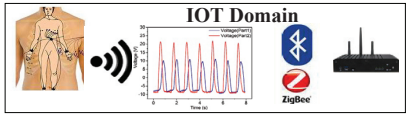
- Four OpenStack micro-clouds connected via programmable switches

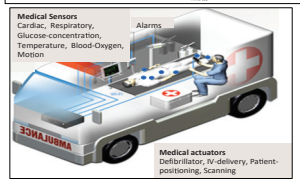


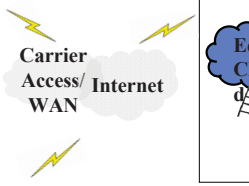


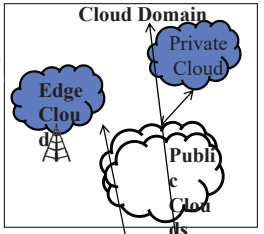
Ref: Tara Salman, Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "**Machine Learning for Anomaly Detection and Categorization in Multi-cloud Environments**," The 4th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2017), New York, June 26-28, 2017, http://www.cse.wustl.edu/~jain/papers/cscloud.htm

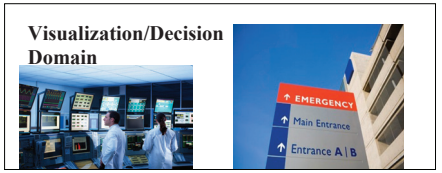
2. Healthcare Security











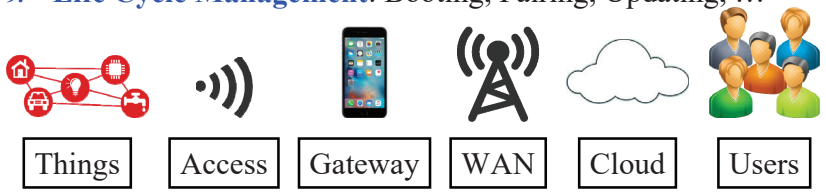
- Security in bluetooth, Zigbee, 4G/5G, IoT Cloud, and back

Security ≠ AES-128

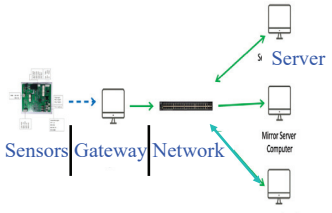
- Use of AES-128 does not guarantee security.
- Insecurity:
  - How strong is the key?
  - Where the key is stored?
  - Bugs in system code
  - Backdoors

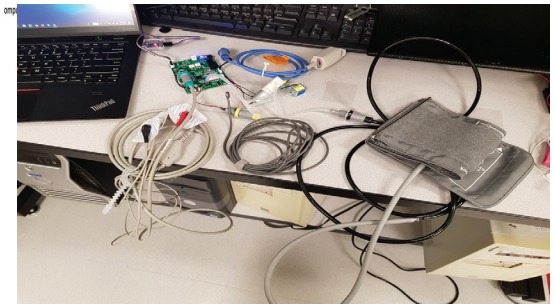
Attack Surface

1. **IoT Devices**
2. **IoT wireless access technology**: DECT, WiFi, Z-wave, …
3. **IoT Gateway**: Smart Phone
4. **Home LAN**: WiFi, Ethernet, Powerline, …
5. **IP Network**: DNS, Routers, …
6. **Higher-layer Protocols**
7. **Cloud**
8. **Management Platform**: Web interface
9. **Life Cycle Management**: Booting, Pairing, Updating, …



Health Systems Security Testbed

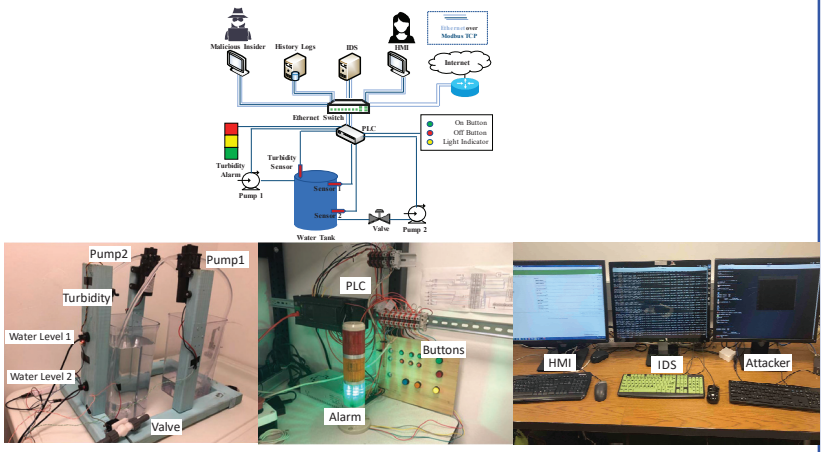




3. Industrial Control Systems Security

- Pre-Ethernet era networks and protocols: Modbus
- Extremely critical infrastructure
- Nation state level attacks
- Any weakness in the lifetime management, installation, or upgrades, may lead to attacks

ICS Testbed



Ref: Marcio Andrey Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, and Mohammed Samaka, "**SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach**," Future Internet 2018, 10(8), 76, http://www.cse.wustl.edu/~jain/papers/ics_ml.htm

Problems with Current AI

- 1. Very large globally distributed systems
  - Cannot use one central place to collect all data, analyze in a timely manner
- 2. Security data is highly imbalanced
  - Attacks are rare. 1 in a billion packets.
  - Almost any model will give 99.999% accuracy by declaring that all traffic is normal all the time.
- 3. AI is a black box.
  - Every paper simply states the results obtained
  - Using data from anywhere using software from anywhere.
  - No idea why the results are what they are.

Machine Learning is what only machines can do, but human cannot do and cannot explain

Innovations in AI

1. Hierarchical AI Modeling

Small AI models in each edge cloud

Models are reused in the central cloud

2. AI Techniques and metrics for imbalanced data

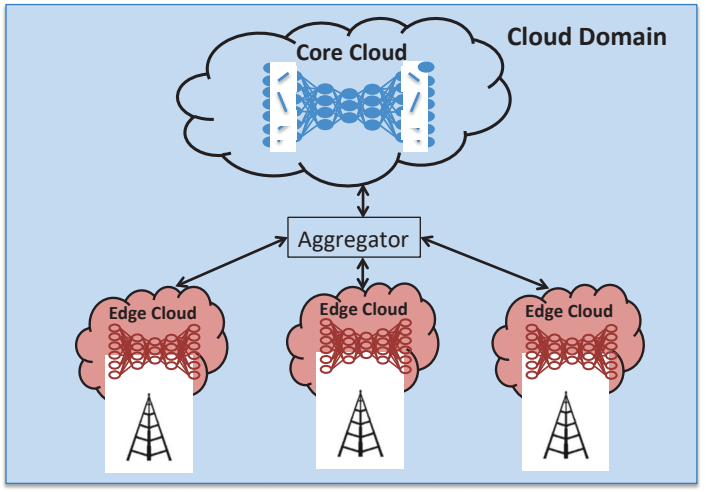
Accuracy etc are not appropriate

3. Explainable AI models

Ref: M. Zolanvari, M. A. Teixeira, R. Jain, "Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp., http://www.cse.wustl.edu/~jain/papers/imb_isi.htm

M. Zolanvari, M. A. Teixeira, R. Jain, "An Explainable Machine Learning Based Security Framework: A Special Case on Industrial IoT," Submitted February 2019.

Innovations in Multi-Cloud Hierarchical AI Model with Layer Reuse



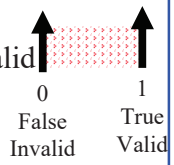
Limitations of Blockchains

Limitation 1: Only facts are recorded

- Alice signed a contract with Bob to pay 10 coins for 1 kg of xx.

Limitation 2: Binary Validity

- All transactions recorded on the blocks that are committed are valid
- Those not on the committed blocks and old are invalid
- So the recording is binary: only 0 or 1.



Limitation 3: Deterministic Events only

- Can not record that I am only 90% sure that Alice gave 20 coins to Bob.

Ref: Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "**Security Services Using Blockchains: A State of the Art Survey**" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm

Innovations in Blockchain

1. Probabilistic Blockchains (Patent Pending)

- Allows probabilistic statements:
  - I am 50% sure that this is a spam
- Uses statistics/AI to create a knowledge summary
- Good for decisions based on large number of opinions

2. Reputation Management System

Ref: Tara Salman, Raj Jain, and Lav Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

- Tara Salman, Raj Jain, Lav Gupta, "**A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains**," 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019,

Summary

- Developing real solutions for real-world problems using real systems
- Working with industry partners: Intel, Cisco, Broadcom, Boeing, …
- World-wide collaborations: Purdue, IUPUI, Qatar U, HBKU

Papers on Security

- Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "**Security Services Using Blockchains:A State of the Art Survey**" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
- Marcio Andrey Teixeira, Tara Salman, Maede Zolanvari, Raj Jain, Nader Meskin, and Mohammed Samaka, "**SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach**," Future Internet 2018, 10(8), 76, http://www.cse.wustl.edu/~jain/papers/ics_ml.htm
- Maede Zolanvari, Marcio A. Teixeira, Raj Jain, "**Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning**," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami FL, Nov. 9 - 11, 2018, 6 pp., http://www.cse.wustl.edu/~jain/papers/imb_isi.htm
- Tara Salman, Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "**Machine Learning for Anomaly Detection and Categorization in Multi-cloud Environments**," The 4th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2017), New York, June 26-28, 2017, http://www.cse.wustl.edu/~jain/papers/cscloud.htm

Papers on Security (Cont)

- Deval Bhamare, Tara Salman, Mohammed Samaka, Aiman Erbad, Raj Jain, "**Feasibility of Supervised Machine Learning for Cloud Security**," 3rd International Conference on Information Science and Security (ICISS2016), December 19th - 22nd, 2016, Pattaya, Thailand, http://www.cse.wustl.edu/~jain/papers/iciss16.htm
- Jianli Pan, Raj Jain, Subharthi Paul, Mic Bowman, Shanzhi Chen, "**Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet**," Proceedings of IEEE International Conference on Communications (ICC) 2009, Dresden, Germany, June 14-18, 2009, http://www.cse.wustl.edu/~jain/papers/emilsa.htm
- Deval Bhamare, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan, Nader Meskin, "**Cybersecurity for Industrial Control Systems: A Survey**," Submitted December 2018.
- Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "**Security of Advanced Industrial Wireless and Sensor Networks: An Overview**," Submitted July 2017.

Papers on Blockchains

- Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "**Security Services Using Blockchains:A State of the Art Survey**" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
- Tara Salman, Raj Jain, Lav Gupta, "**A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains**," IEEE 1st International Workshop on Advances in Artificial Intelligence for Blockchain (AIChain 2019), held in conjunction with the 2019 IEEE International Conference on Blockchain, Atlanta, July 14, 2019,
- Tara Salman, Raj Jain, and Lav Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

Talks on Security

- Raj Jain, "**Extending Blockchains for Risk Management and Their Applications to Network Security**," Open Networking Summit 2019, San Jose, CA, April 4, 2019, http://www.cse.wustl.edu/~jain/talks/pbc_ons.htm
- Raj Jain, "**Internet of Things and Smart Cities Security: Challenges and Issues**," Keynote at 1st Annual Research Workshop on Advances & Innovations in Cyber Security, Memphis, TN, June 10, 2016, http://www.cse.wustl.edu/~jain/talks/iots_tns.htm
- Raj Jain, "**Internet of Things Security: Challenges and Issues**," Keynote at 9th Central Area Networking and Security Workshop (CANSec), University of Central Missouri, Warrensburg, MO, April 16, 2016, http://www.cse.wustl.edu/~jain/talks/iots_ucm.htm
- Raj Jain, "**Internet of Things Security**," Keynote at STLCybercon 2015, University of Missouri, St. Louis, November 20, 2015, http://www.cse.wustl.edu/~jain/talks/iots_um.htm

Talks on Blockchains

- Raj Jain, "**Extending Blockchains for Risk Management and Their Applications to Network Security**," Open Networking Summit 2019, San Jose, CA, April 4, 2019, http://www.cse.wustl.edu/~jain/talks/pbc_ons.htm
- Raj Jain, "**Extending Blockchains Beyond Smart Contracts**," Keynote at Blockchain Connect Conference, San Francisco, January 11, 2019, http://www.cse.wustl.edu/~jain/talks/pbc_svi.htm
- Raj Jain, "**Extending Blockchains for Risk Management and Decision Making**," Invited talk at Innovation and Breakthrough Forum 2018, Hong Kong, Nov. 9, 2018,
- Raj Jain, "**Blockchains: Networking Applications**," An invited talk at the 38th IEEE Sarnoff Symposium, Newark, NJ, Sep 19, 2017, http://www.cse.wustl.edu/~jain/talks/blc_srnf.htm
- Raj Jain, "**Blockchains: The Distributed Trust Technology**," Keynote at The 2017 International Conference on Computer, Information and Telecommunication Systems (CITS 2017), Dalian, China, July 21, 2017, http://www.cse.wustl.edu/~jain/talks/cits17.htm
- Raj Jain, "**Blockchains: The Revolutionary Trust Protocol**," BEL Keynote at 22nd Annual International Conference on Advanced Computing and Communications (ADCOM 2016), Bangaluru, India, Sep 10, 2016, http://www.cse.wustl.edu/~jain/talks/blc_ad16.htm

Acronyms

- 3GPP Third Generation Partnership Project
- AI Artificial Intelligence
- ANSI American National Standards Institute
- AT&T American Telephone and Telegraph
- BSS Business Support Services
- CA California
- CGNAT Carrier Grade Network Address Translator
- CSE Computer Science and Engineering
- DECbit Digital Equipment Corporation Bit
- IEEE Institution of Electrical and Electronic Engineering
- IoT Internet of Things
- ML Machine Learning
- MO Missouri
- MS Master of Science
- NFV Network Function Virtualization
- NTT Nippon Telephone and Telegraph

Acronyms (Cont)

- OpenADN Open Application Delivery Networking
- OSS Operations Support Services
- SON Self-Organizing Networks
- TV Television
- UK United Kingdom
- US United States
- VC Venture Capital
- WAN Wide Area Network
- WiMAX Worldwide Interoperability for Microwave Access
- WUSTL Washington University in St. Louis

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/talks/sec_rj.htm