

Cybersecurity of Healthcare: Our Research



Raj Jain

Washington University in Saint Louis
Saint Louis, MO 63130

Jain@cse.wustl.edu

WashU/AT&T Cybersecurity/Medical IoT Use Cases Meeting

WUSTL, Nov 9, 2019

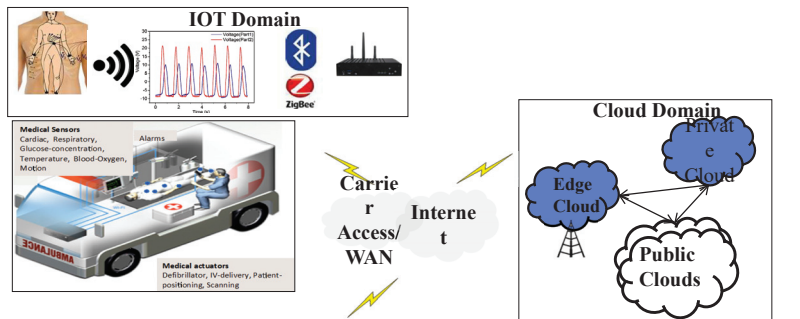
These slides are at:

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



1. Health Care Security
2. Multiple Domains: IoT, Clouds, Cellular
3. Innovations in AI
4. Innovations in Blockchains

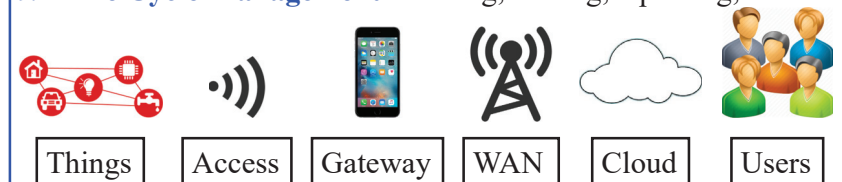
Healthcare Cybersecurity Architecture



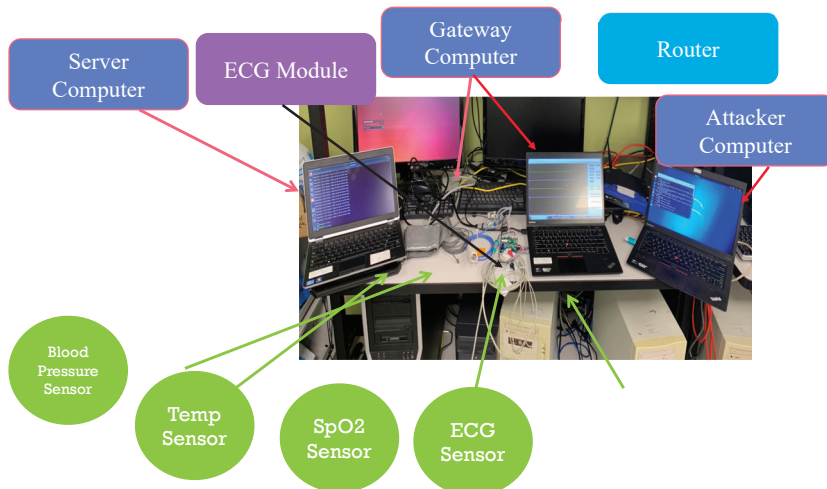
- Three interacting domains:
 1. IoT
 2. Multi-cloud storage/processing
 3. User/Action domains.

1. IoT Cybersecurity

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, ...



Hospital on Hospital on a Desk Testbed



Ref: Anar A. Hady, Ali H. Ghubaish, Tara Salman, Devrim Unal, Raj Jain, "Secure Healthcare Monitoring System using Machine Learning." Submitted.
Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/sec_hlth.htm ©2019 Raj Jain

5

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

Washington University in St. Louis

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

©2019 Raj Jain

6

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.

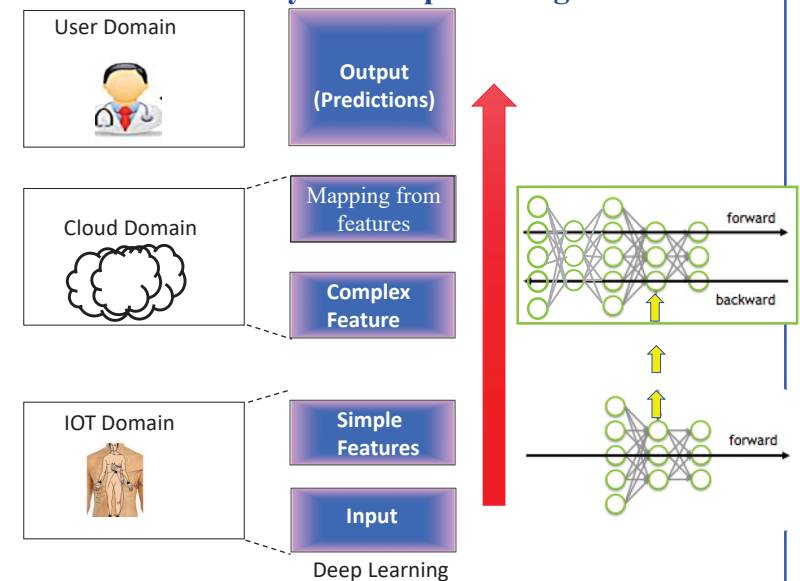
Washington University in St. Louis

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

©2019 Raj Jain

7

Multi layered deep learning model



Washington University in St. Louis

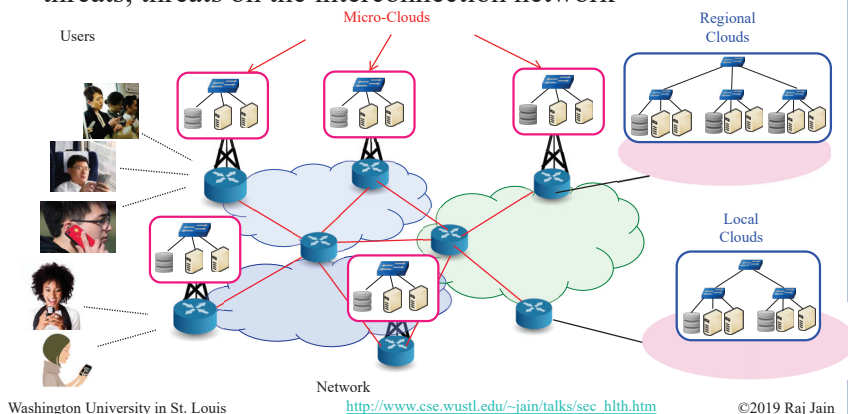
http://www.cse.wustl.edu/~jain/talks/sec_hlth.htm

©2019 Raj Jain

8

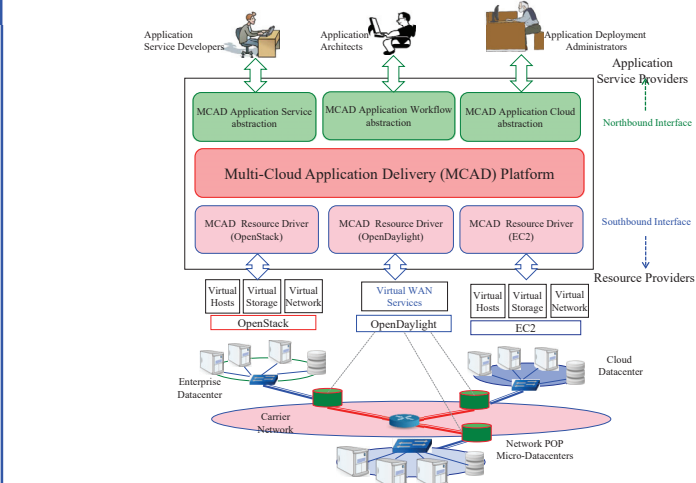
2. Multi-Cloud Cybersecurity

- 5G ⇒ Edge Clouds, Local, and regional clouds
- Internal intra-cloud threats, inter-cloud trust issues, external threats, threats on the interconnection network



9

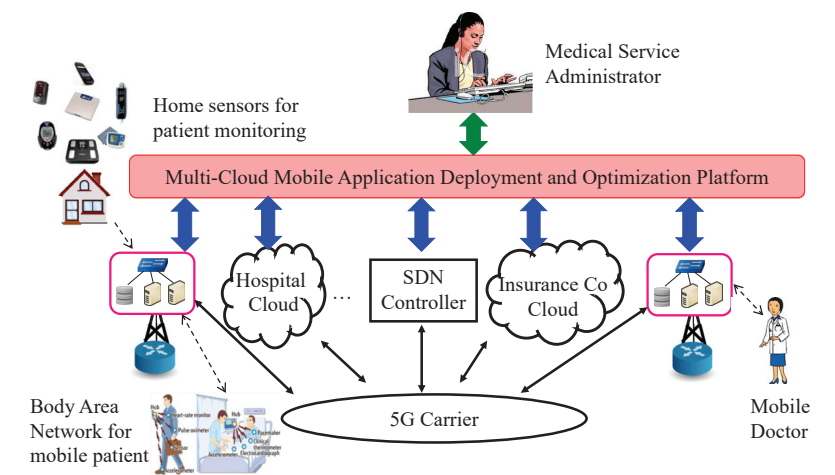
OpenADN Multi-Cloud Management



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>
Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/sec_hlth.htm ©2019 Raj Jain

10

Mobile Healthcare Use Case

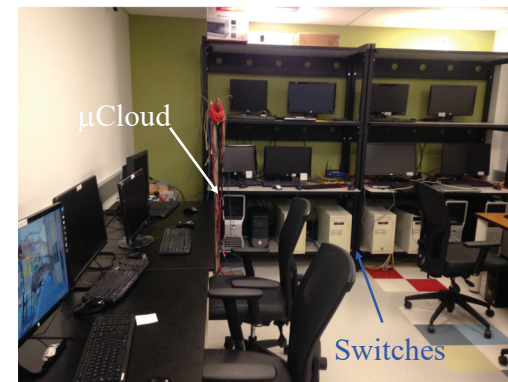
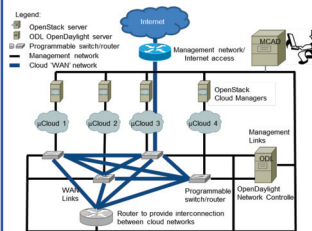


Ref: Tara Salman, Deval Bhamare, Aiman Erbad, Raj Jain, Mohammed Samaka, "Machine Learning for Anomaly Detection and Categorization in Multi-cloud Environments," The 4th IEEE International Conference on Cyber Security and Cloud Computing, June 26-28, 2017, <http://www.cse.wustl.edu/~jain/papers/cscloud.htm>
Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/sec_hlth.htm ©2019 Raj Jain

11

Our Multi-Cloud Testbed

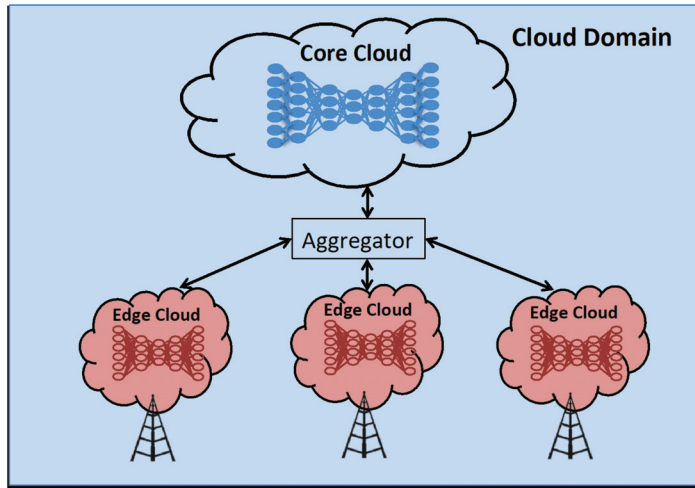
- Four OpenStack micro-clouds connected via programmable switches



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>
Washington University in St. Louis http://www.cse.wustl.edu/~jain/talks/sec_hlth.htm ©2019 Raj Jain

12

Innovations in Multi-Cloud Hierarchical AI Model with Layer Reuse



Summary



- ❑ Developing real solutions for real-world problems using real systems
- ❑ Five Funded projects on Security: Security of Medical Systems, Industrial Systems, Scientific Collaborations
- ❑ Also extending blockchains for security

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/csccloud.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 (AICChain 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/abc_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/abc_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/abc_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/abc_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/abc_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), Bangalore, India, Sep 10, 2016, http://www.cse.wustl.edu/~jain/talks/abc_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_hlth.htm