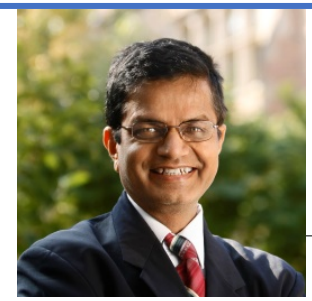
Our Research on Quantum and AI for Network Security



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

A talk in "CSE 591: Introduction to Graduate Studies in CSE"
October 13, 2023
These slides are available at:
http://www.cse.wustl.edu/~jain/talks/cs59123.htm

1. Trends in:
   - Cybersecurity
   - Quantum
   - AI
2. Our Research in these areas
3. Key distinctions of our research

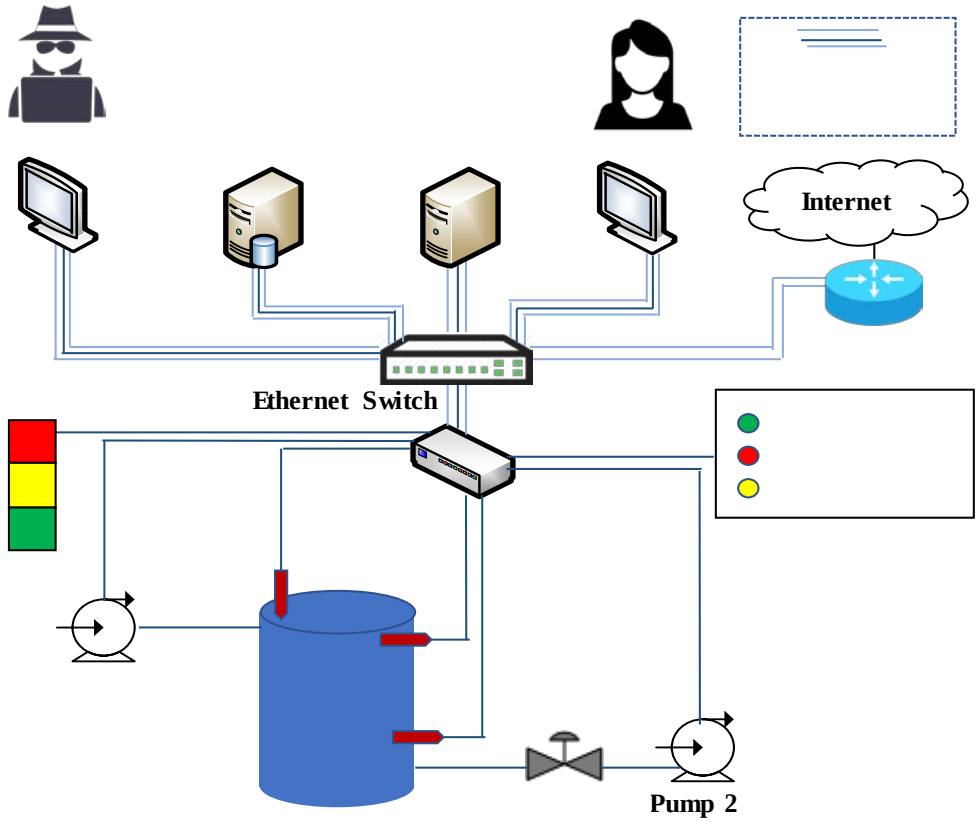
AI-Based Security of IoT: Our Research

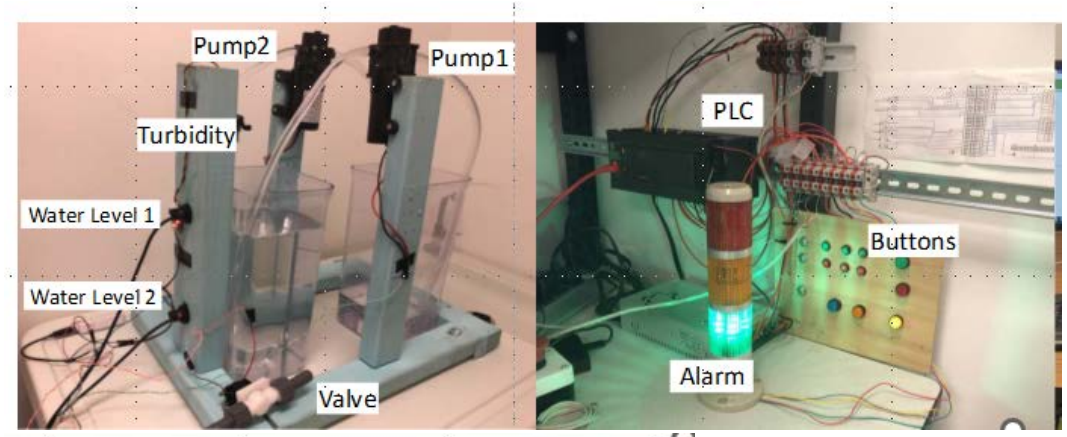
- Security research since 2009
- AI research since 2017
- Security of Industrial Internet of Things (IIoT)

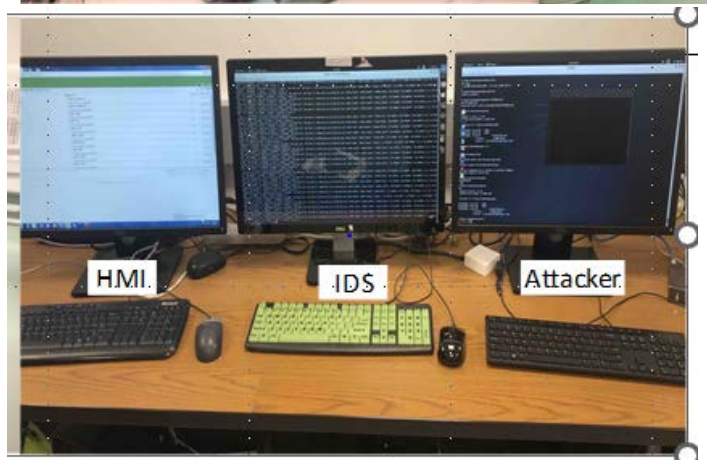
- Security of Internet of Medical Things (IoMT)

- Security using blockchains
- 24+ papers
- AI = Pattern recognition, probabilistic reasoning, machine learning, deep learning, …
- Everything we say applies to all of these variations.

Industrial Control Systems Security Using AI

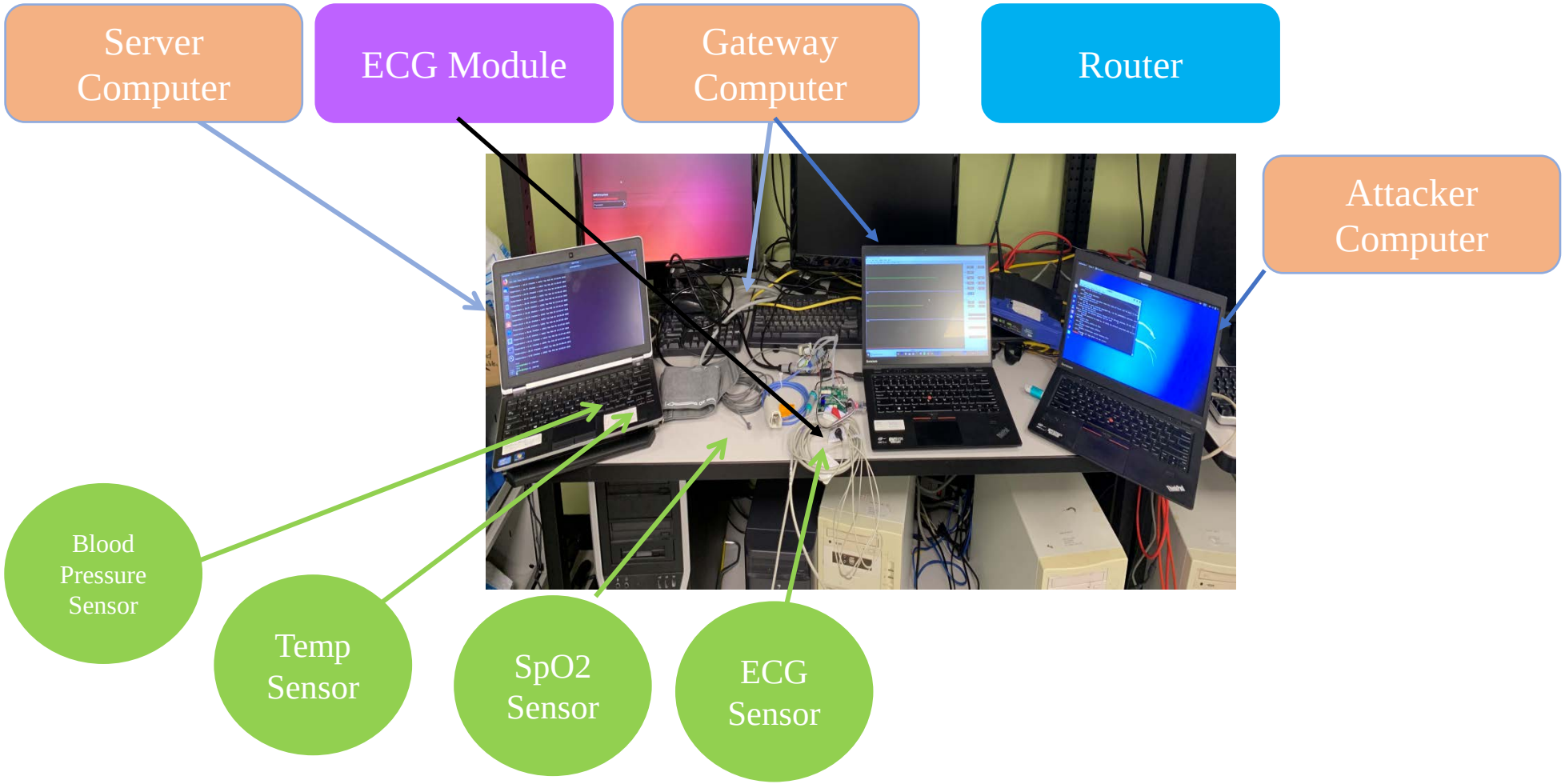






WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research, http://www.cse.wustl.edu/~jain/iiot2/index.html

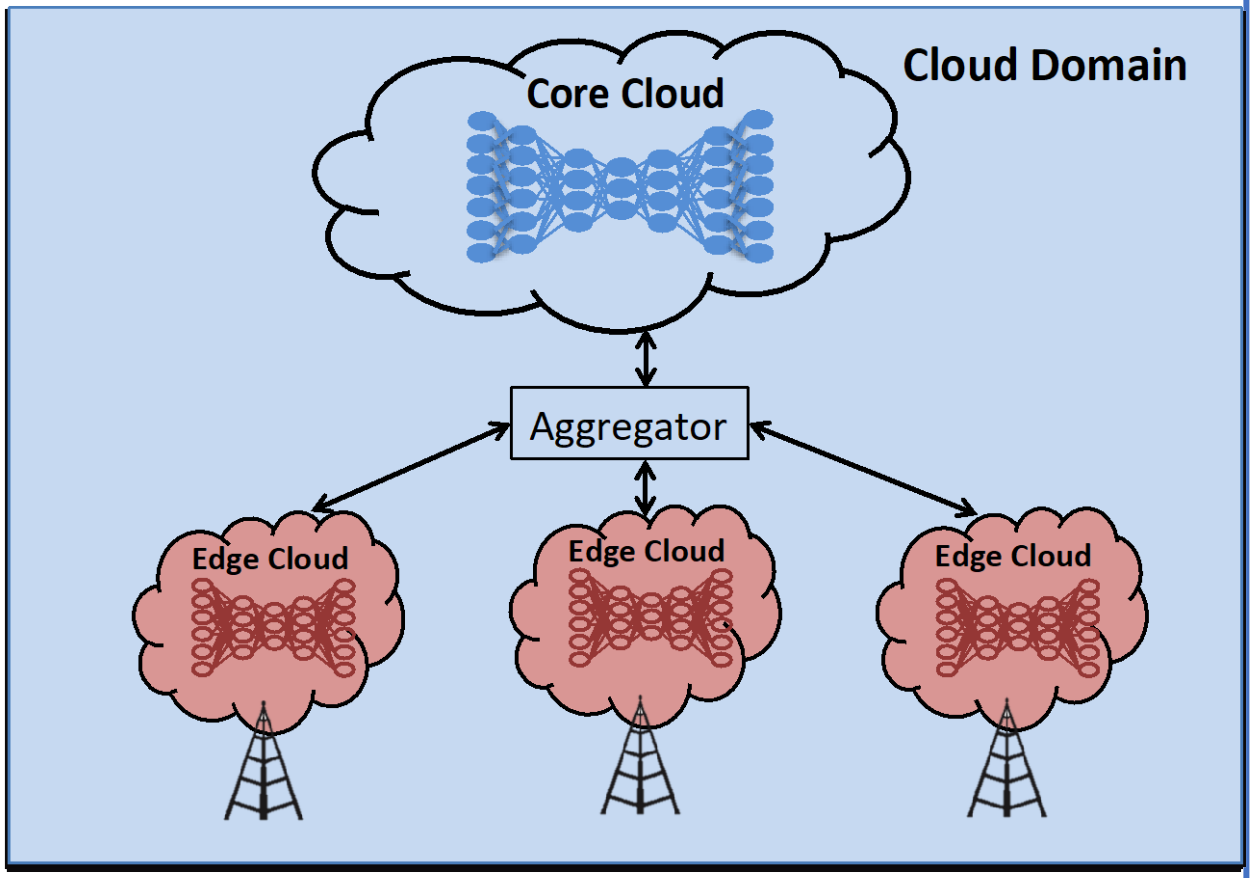
Internet of Medical Things Security Using AI



WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research, http://www.cse.wustl.edu/~jain/ehms/index.html

Edge AI: Hierarchical Deep Learning

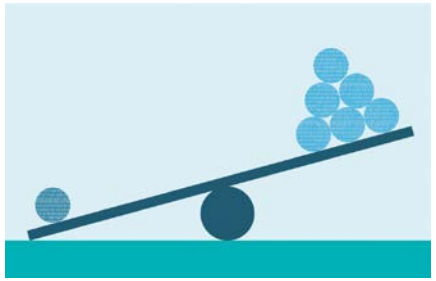
- No need to send data to the core cloud
- Edge clouds send a preliminary model to the core
- Also known as "Federated Learning"



Ref: L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, R. Jain, "**Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach**," Applied Soft Computing (2022), 5 January 2022, http://www.cse.wustl.edu/~jain/papers/muse.htm

Imbalance of Security Data

- AI started with image analysis but needs to be extended for security
- Security data is very different from image data
  - Most security datasets are not representative of the real world.
  - In most papers, 10-15% of the packets are attack packets
- In the real world, 1 in several billion packets is an attack packet. Mis-classify the attack packet ⇒ 99.9999% accuracy
- **Extreme Data imbalance** is a critical issue in security



1% attack

Ref: 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

Wrong Metrics

- In Image analysis:
  Cost of predicting "0" when it is "1" = Cost of predicting "1" when it is "0."
  $\Rightarrow$ Cost of errors is symmetric $\Rightarrow$. Almost all metrics are symmetric.
- In Cyber Security:
  - Cost of missing an attack = $10^6 \times$ Cost of false attack prediction
  - Washington Post (5/30/22): 5 missiles hit Iraqi base hosting US troops
  - Would you live at the base protected with 90% accuracy?
- Need new metric to find the best algorithm $\Rightarrow$ Use **Safety Score**

Ref: Tara Salman, Ali Ghubaish, Devrim Unal, Raj Jain, "**Safety Score as an Evaluation Metric for Machine Learning Models of Security Applications**," IEEE Networking Letters, Vol. 2, Issue 4, December 2020, pp. 207-211, http://www.cse.wustl.edu/~jain/papers/safety.htm

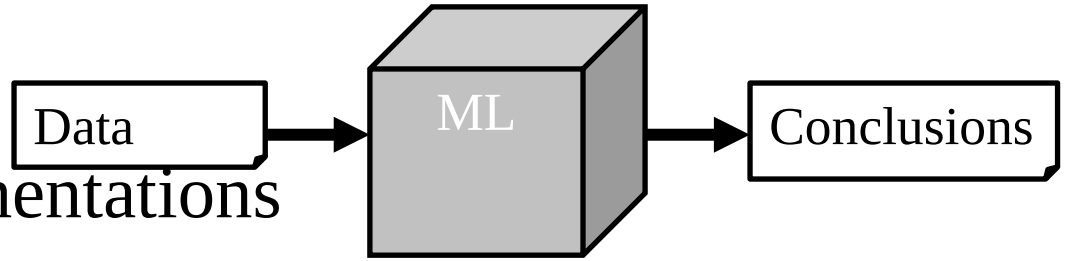
Results Not Explainable

- Would you trust AI to diagnose your disease?
- No, because you have no idea why the results are what they are

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

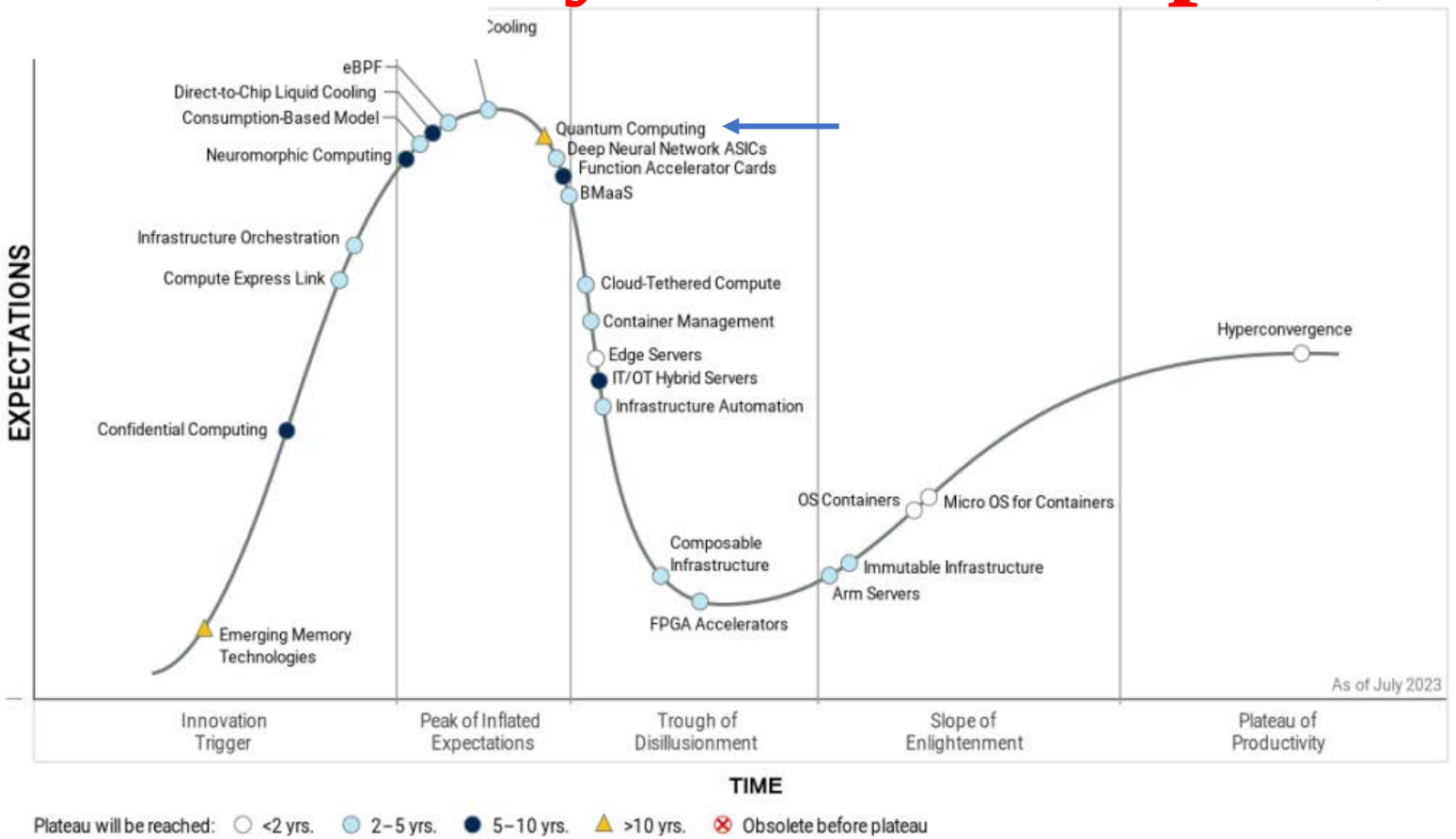
- AI is a black box
- Can't discover bugs in ML model implementations
- Need Trustable AI = Explainable AI

  ⇒ Models to explain the AI predictions so that humans can understand



Ref: Maede Zolanvari, Zebo Yang, Khaled Khan, Raj Jain, and Nader Meskin, "TRUST XAI: A Novel Model for Explainable AI with An Example Using IIoT Security," IEEE IoT Journal, preliminary acceptance, September 2021.

Gartner's Hype Cycle for Compute, 2023



Research & Startup → Sell Startup → Technology Profit → Manufacturing Profit →

Ref: T. Harvey, J. Donham, "Hype Cycle for Compute, 2023," Gartner G00790907, July 10, 2023, 87 pp.

How Quantum Threatens Cybersecurity?

1. Easy to factorize large numbers

- Easy to find the private key given the public key
- Anyone with your private key can sign your contracts ⇒ ID theft
- They can empty your wallet by giving away your cryptocurrencies

2. Easy to invert one-way hash functions

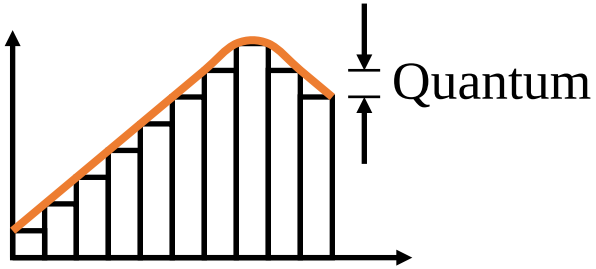
Proof-of-Work uses a puzzle to find the number that hashes below a threshold ⇒ Trivial to win Proof-of-Work puzzles

3. Easily find hash collisions: Two numbers with the same hash

- Hash is used in Merkle tree ⇒ Can change a transaction with no change in hash
- Hash of a block is used as a pointer by the next block
  ⇒ Can change a block such that the hash does not change.

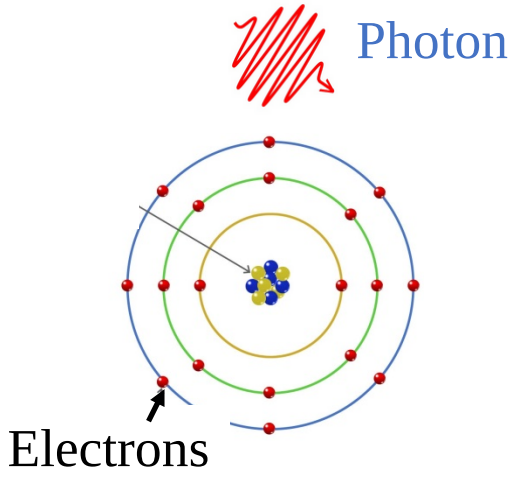
What is a Quantum?

- Quantization: Analog to digital conversion
  - **Quantum** = Smallest discrete unit



Wave Theory: Light is a continuous wave. It has a frequency, phase, amplitude

- **Quantum Mechanics**: Light behaves like discrete packets of energy that can be absorbed and released
- **Photon** = One quantum of light energy
- Photons can move an electron from one energy level to the next higher level
- Photons are released when an electron moves from one level to a lower energy level



How to Protect Security?

A. **Quantum-Resistant Blockchains**
   1. **Post-Quantum Cryptography**: Does not use factoring. NIST recommends:
      - ✓ CRYSTALS-KYBER for public-key encryption and key-establishment
      - ✓ CRYSTALS-DILITHIUM, FALCON, and SPHINCS+ for Digital signature
   2. **Secret-Key Cryptography**: With sufficiently large keys
   3. **Larger Hashes**: SHA-512

B. **Quantum Native Cryptography**: Hybrid of classical computing and quantum computing. Most quantum circuits require classical communication lines after measurement.

Ref: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

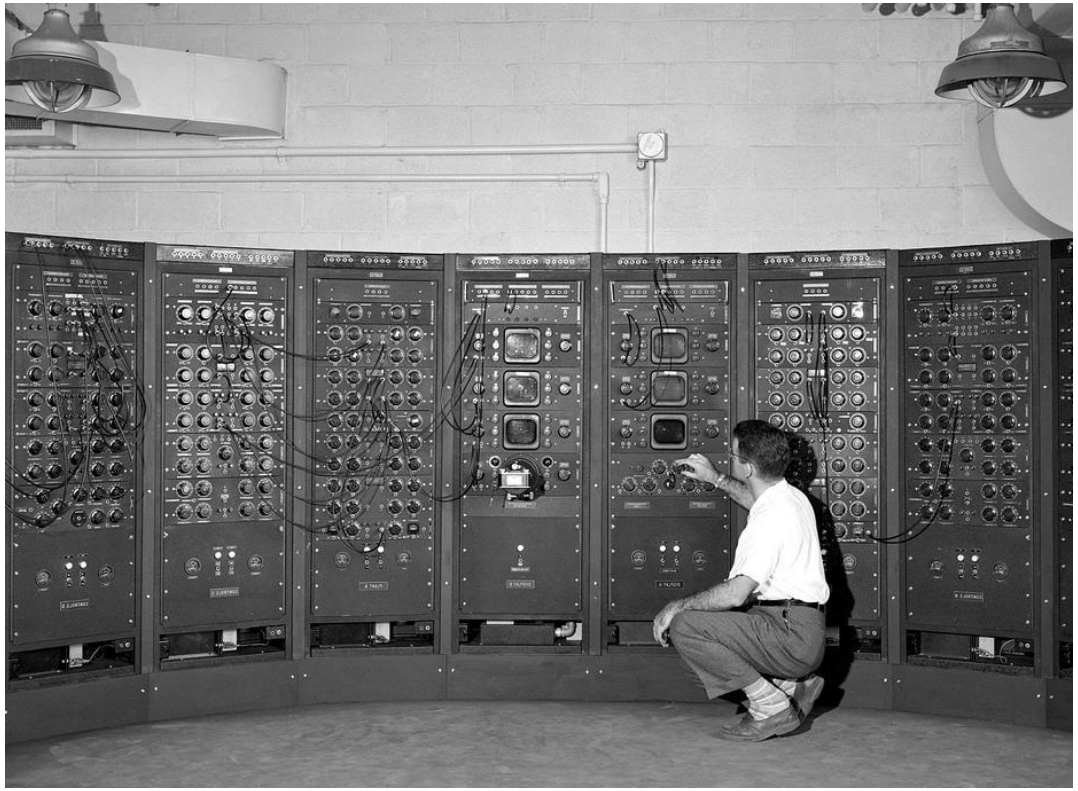
Challenges for Quantum

- **Decoherence**: Qubits lose their state over time.
  In nanoseconds to seconds, depending upon the temperature.
  - Need near zero-kelvin (10 milli Kelvin) temperature ⇒ Large cooling equipment.
  - Need extra qubits for quantum error correction to overcome decoherence
- Errors in quantum computers accumulate fast and require a thousand times more qubits to take care of errors
- Most of the research is theoretical.
  Practical experiments are limited to a tiny number of qubits.

Ref: M. Dyaknov, "The case against Quantum Computing," IEEE Spectrum, Nov 15, 2018, https://spectrum.ieee.org/the-case-against-quantum-computing#toggle-gdpr
D. Monroe, "Quantum Computers and the Universe," Communications of the ACM, December 2022, p10-11, https://dl.acm.org/doi/pdf/10.1145/3565977

Quantum Hardware

IBM's Quantum System One (2019) 20-qubit in a 9 ft cube



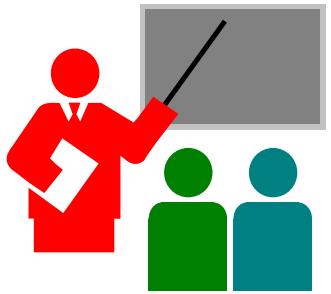
ENIAC (1943) 20 accumulators (10 decimal digits each)

Ref: https://www.datacenterdynamics.com/en/news/ces-ibm-announces-q-system-one-quantum-computer-9ft-cube/

Key Distinction of Our Research

- Goal: Impact to the real-world
  DECbit congestion indication in almost all networking architectures since its invention
- Funded by industry partners:
  Intel, Cisco, Broadcom, Boeing, …
- Impact real-world by participating in standards organizations and industry forums:
  ATM Forum, IEEE Standards, American National Standards Institute (ANSI), Internet Engineering Task Force (IETF), WiMAX Forum
- Work on long term as well as short term research

Summary



1. AI → Explainable AI → Federated AI
2. IoT Intelligent IoT Secure and Intelligent IoT
   - Industrial systems
   - Medical systems
3. Shor's factorization algorithm allows the factorization of integers in less time on quantum computers than in classical computing
4. Quantum-Safe Crypto is in standardization
5. Research for Impact

References: Class Recordings

- Recordings of all of my classes and talks are available on YouTube and on my website:

1. CSE 473: Introduction to Computer Networks, http://www.cse.wustl.edu/~jain/cse473-23/index.html
2. CSE 570: Recent Advances in Networking http://www.cse.wustl.edu/~jain/cse570-21/index.html
3. CSE 574S: Wireless Networks, http://www.cse.wustl.edu/~jain/cse574-20/index.html
4. CSE 567: Computer Systems Analysis http://www.cse.wustl.edu/~jain/cse567-17/index.html
5. CSE 571S: Network Security, http://www.cse.wustl.edu/~jain/cse571-17/index.html

Our Courses on YouTube

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

CSE 570: Recent Advances in Networking (Spring 2013)
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Our Papers

- Tara Salman, Ali Ghubaish, Roberto Di Pietro, Mohammed Baza, Raj Jain and Kim-Kwang Raymond Choo **CrowdFAB: Intelligent Crowd-Forecasting using Blockchains and its use in Security**, Transactions on Dependable and Secure Computing, October 2023.
- Zebo Yang, Maede Zolanvari, Raj Jain, "**A Survey of Important Issues in Quantum Computing and Communications**," IEEE Communications Surveys and Tutorials, March 2023, http://www.cse.wustl.edu/~jain/papers/qsurvey.htm
- Zebo Yang, Tara Salman, Raj Jain, and Roberto Di Pietro, "Decentralization using Quantum Blockchain: A Theoretical Analysis," IEEE Transactions on Quantum Engineering, September 2022, 16 pp., http://www.cse.wustl.edu/~jain/papers/qbif.htm
- Tara Renduchintala, Haneen Alfauri, Zebo Yang, Roberto Di Pietro, and Raj Jain, "A Survey of Blockchain Applications in the FinTech Sector," Journal of Open Innovation: Technology Market, and Complexity 2022, Vol. 8, Issue 4, 185, http://www.cse.wustl.edu/~jain/papers/fintech.htm

Our Papers (Cont)

- 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, http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm
- 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, 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

Our Publications on AI

- L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," Applied Soft Computing (2022), 5 January 2022, http://www.cse.wustl.edu/~jain/papers/muse.htm
- Maede Zolanvari, Ali Ghubaish, and Raj Jain, "ADDAI: Anomaly Detection using Distributed AI," in Proceedings of IEEE ICNSC (International Conference on Networking, Sensing and Control), October 2021., http://www.cse.wustl.edu/~jain/papers/addai.htm
- M Zolanvari, Z Yang, K Khan, R Jain, N Meskin, "TRUST XAI: Model-Agnostic Explanations for AI With a Case Study on IIoT Security," IEEE Internet of Things Journal, 2021, http://www.cse.wustl.edu/~jain/papers/trustxai.htm
- Tara Salman, Ali Ghubaish, Devrim Unal, Raj Jain, "Safety Score as an Evaluation Metric for Machine Learning Models of Security Applications," IEEE Networking Letters, Vol. 2, Issue 4, December 2020, pp. 207-211, http://www.cse.wustl.edu/~jain/papers/safety.htm
- Lav Gupta, Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, "Fault And Performance Management In Multi-Cloud Virtual Network Services Using AI: A Tutorial And A Case Study," Computer Networks, Pre-Proof published on 14 Oct 2019, http://www.cse.wustl.edu/~jain/papers/fp_comst.htm

Our Publications on AI (Cont)

- Lav Gupta, Tara Salman, Ria Das, Aiman Erbad, Raj Jain, Mohammed Samaka, "HYPER-VINES: A HYbrid Learning Fault and Performance Issues ERadicator for VIrtual NEtwork Services over Multi-cloud," International Workshop on Computing, Networking and Communications (CNC19) at the International Conference on Computing, Networking and Communications (ICNC 2019), Honolulu, Hawaii, Feb. 18-21, 2019, 7 pp., http://www.cse.wustl.edu/~jain/papers/hypervin.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

Our Publications on AI (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

Our Publications on ICS Security

- M Elnour, N Meskin, K Khan, R Jain, "Application of data-driven attack detection framework for secure operation in smart buildings," Sustainable Cities and Society 69, 102816, 2021, http://www.cse.wustl.edu/~jain/papers/secbldg.htm
- M Elnour, N Meskin, K Khan, R Jain, "HVAC System Attack Detection Dataset," Data in Brief, 107166, 2021, http://www.cse.wustl.edu/~jain/papers/hvac.htm
- MA Teixeira, M Zolanvari, KM Khan, R Jain, N Meskin, "Flow-based intrusion detection algorithm for supervisory control and data acquisition systems: A real-time approach," IET Cyber-Physical Systems: Theory & Applications, 2021, http://www.cse.wustl.edu/~jain/papers/ids_ijis.htm
- M. Elnour, N. Meskin, K. Khan, R. Jain, "A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems," IEEE Access, Vol. 8, 19 February 2020, pp. 36639 - 36651, http://www.cse.wustl.edu/~jain/papers/dif.htm
- Mariam Elnour, Nader Meskin, Khaled Khan, Raj Jain, "A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems," IEEE Access, Vol. 8, 19 February 2020, pp. 36639 - 36651, http://www.cse.wustl.edu/~jain/papers/dif.htm

Our Publications on ICS Security

- *Mariam Elnour, Nader Meskin, Khaled M. Khan, Raj Jain, Syed Zaidi, Hammadur Siddiqui, "Full-Scale Seawater Reverse Osmosis Desalination Plant Simulator," 21st IFAC World Congress in Berlin, Germany, July 12-17, 2020, 8 pp., http://www.cse.wustl.edu/~jain/papers/swrodp.htm*
- *D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, "Cybersecurity for Industrial Control Systems: A Survey," Computers and Security, Elsevier, Volume 89, February 2020, Article 101677, http://www.cse.wustl.edu/~jain/papers/ics_survey.htm*
- M. Zolanvari, M. Teixeira, L. Gupta, K. Khan, R. Jain, "Machine Learning Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, Vol. 6, Issue 4, Aug 2019, http://www.cse.wustl.edu/~jain/papers/vulnerab.htm
- M. Zolanvari, M. 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
- 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

Our Publications on Healthcare Security

- Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Khalid Al-Ali, Raj Jain, "Recent Advances in the Internet of Medical Things (IoMT) Systems Security," IEEE Internet of Things Journal, Vol. 8, Issue 11, June 1, 2021, http://www.cse.wustl.edu/~jain/papers/iomt_iot.htm
- Anar A. Hady, Ali Ghubaish, T. Salman, Devrim Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," IEEE Access, June 2020, http://www.cse.wustl.edu/~jain/papers/hms.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
Rajjain.com

http://www.cse.wustl.edu/~jain/talks/cs59123.htm