AI and Cybersecurity: Issues and Challenges







Scan this to download these slides.

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

Global Webinar on Artificial Intelligence & Machine Learning, 2026

These slides and a video recording of this talk are at:
http://www.cse.wustl.edu/~jain/talks/globalai26.htm

©2026 Raj Jain



1. Our Research on AI for IoT Security
2. Lessons Learnt: Common issues with AI Security studies
3. Recent Developments in AI and Their Impact on Security
4. Security Technologies Coming Soon – Ready for Trials

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
- Security and Quantum – Current research
- AI = Pattern recognition, machine learning, deep learning, …, LLMs, GenAI, AgenticAI
- Everything we say applies to all of these variations of AI





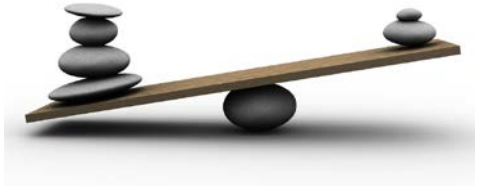
©2026 Raj Jain

Part 1
Common issues with AI Security studies

Lessons Learnt: 9 Problems with AI Studies

1. No Domain Expertise
2. Random Datasets
3. Imbalance of Security Data
4. Results Not Explainable
5. Wrong Performance Metrics
6. Too Few or Too Many Features
7. No Sensitivity Analysis
8. No Real-World Validation
9. Omitting Assumptions and Limitations







1. No Domain Expertise

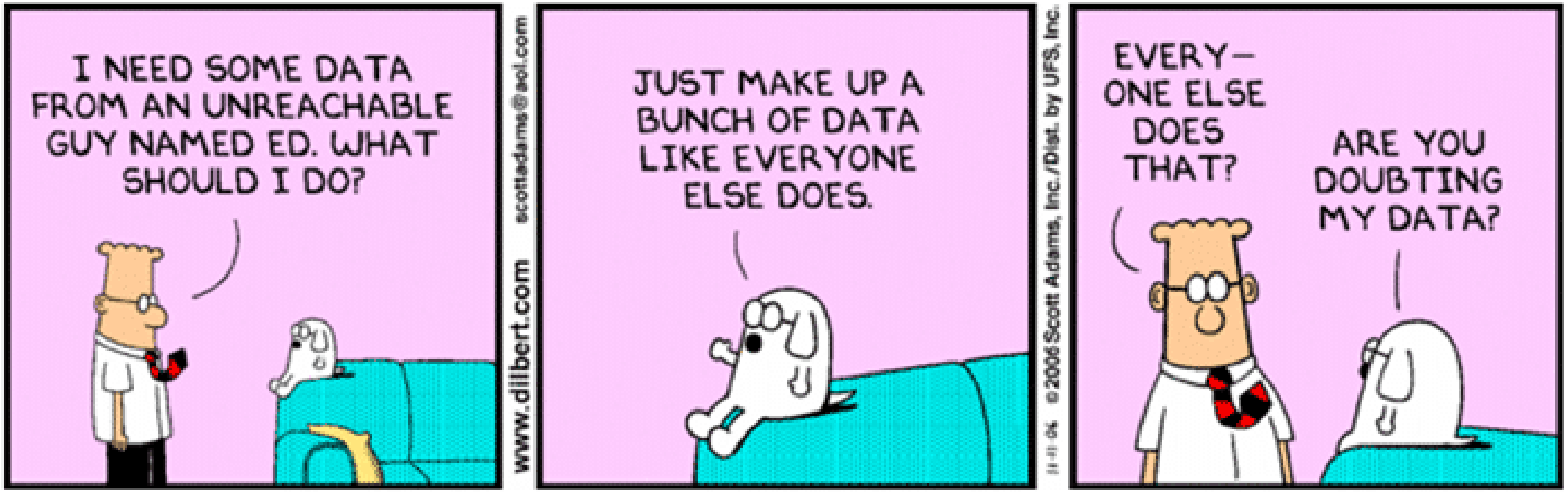
- AI algorithms are used without domain expertise
- Data cleanliness, labeling, and feature extractions require domain knowledge, e.g., What is the distance between Port 80, Port 81, and Port 8080?
- To analyze medical data with AI, you don't need to be a doctor



With AI, even a dog can be an "intelligent" doctor?

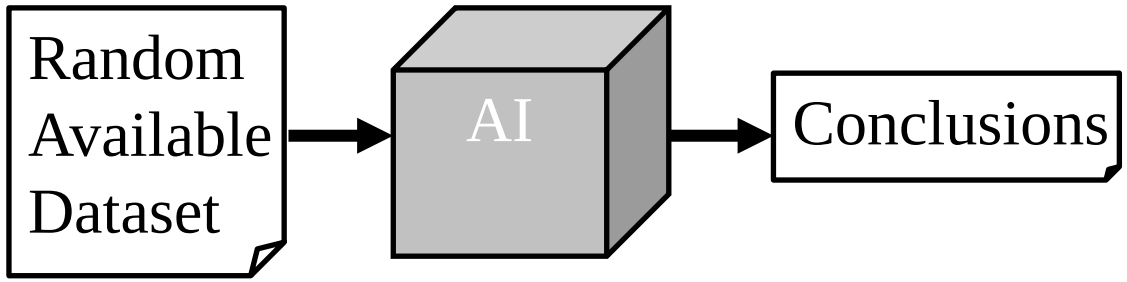
©2026 Raj Jain

2. Random Datasets



2. Random Datasets

- Real data is usually private. Not published.
- Published data is either old or too generic.
- KDD, a commonly used dataset in intrusion studies, is a simulated dataset from 1999.

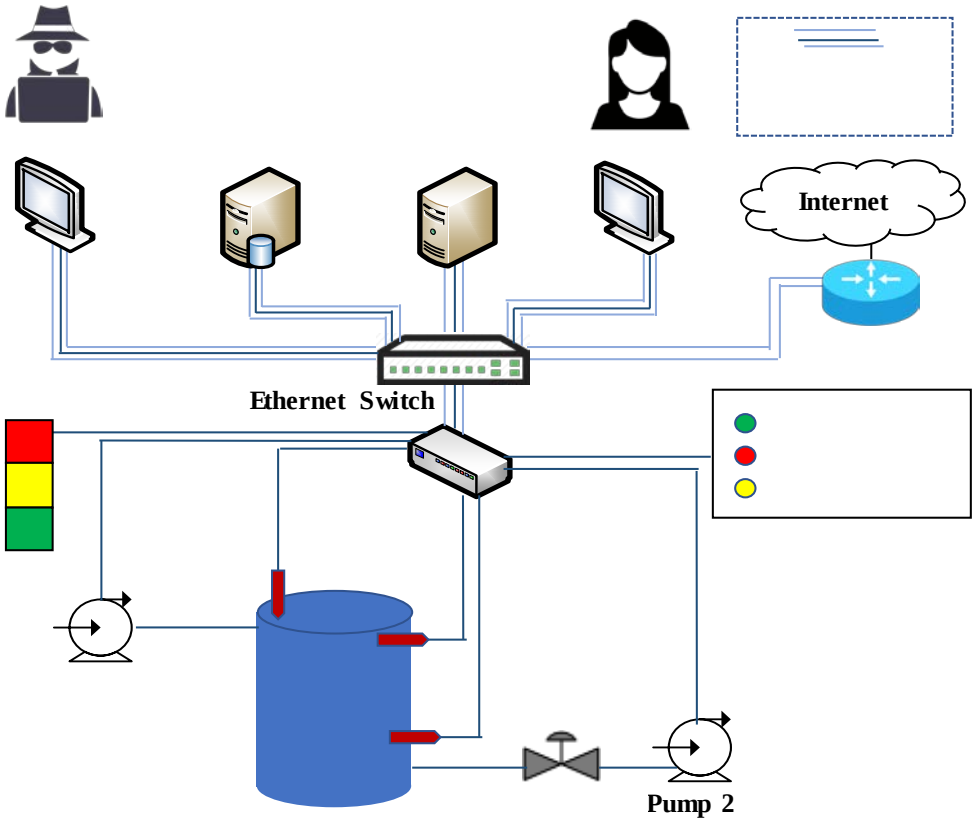


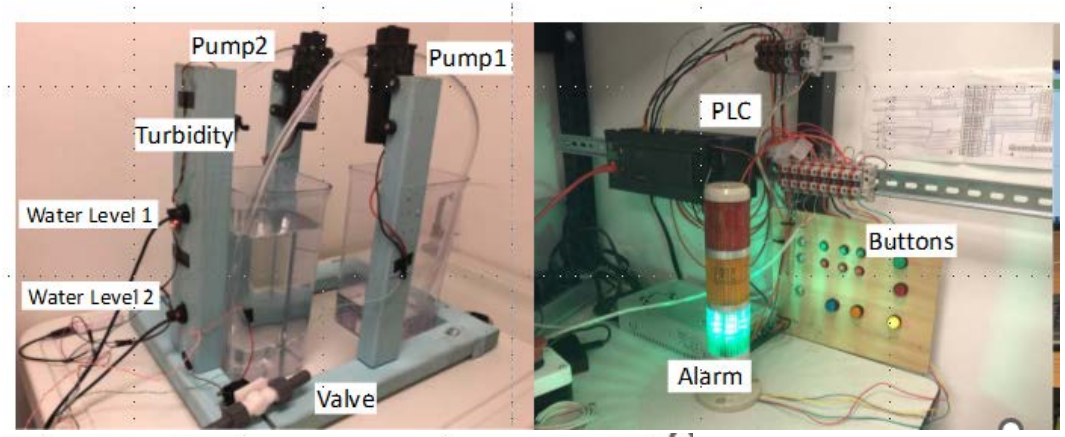
Garbage-In, Garbage-Out

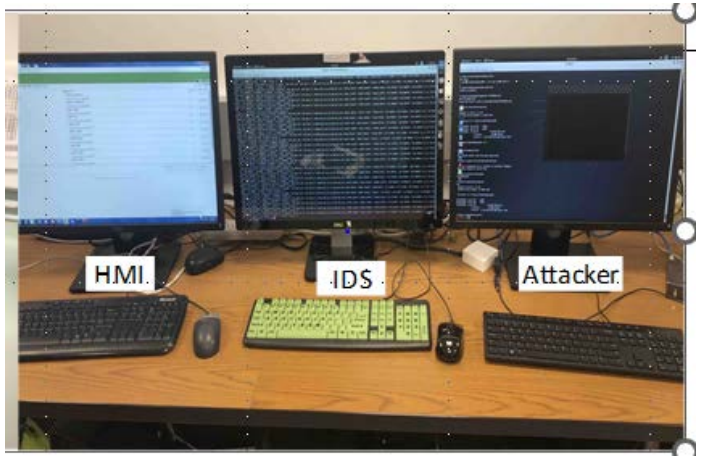
Ref: KDD Cup 1999 Data, October 28, 1999, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

©2026 Raj Jain

Industrial Control Systems Security Using AI



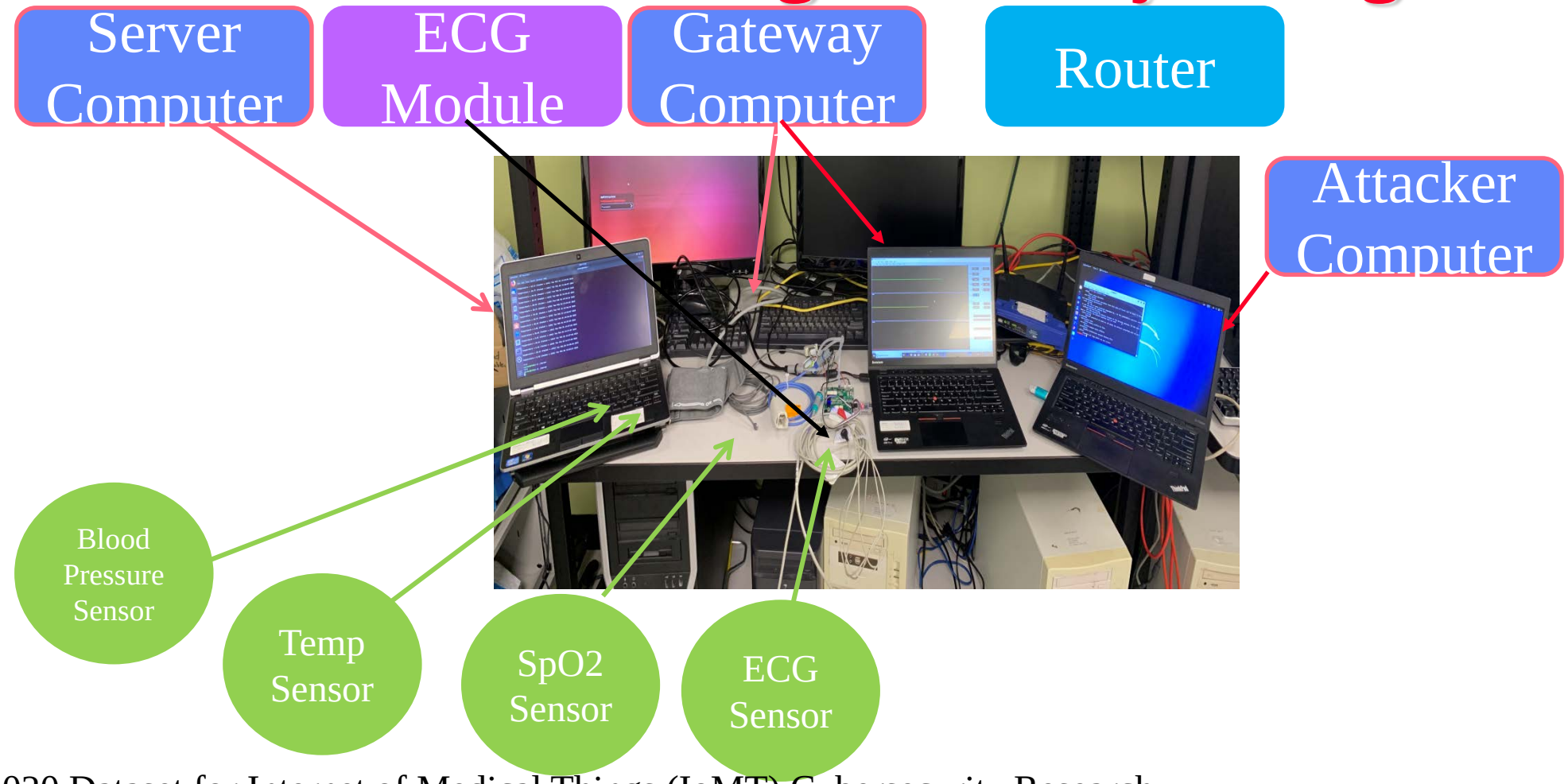




WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research,
http://www.cse.wustl.edu/~jain/iiot2/index.html

©2026 Raj Jain

Internet of Medical Things Security Using AI

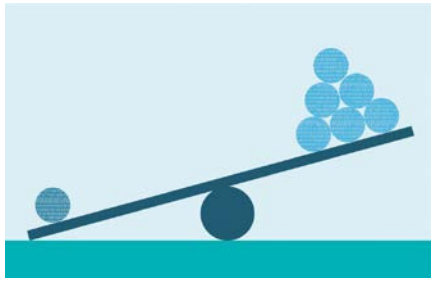


WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research, http://www.cse.wustl.edu/~jain/ehms/index.html

©2026 Raj Jain

3. 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





1% attack

Extreme Data imbalance is a critical issue in security

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

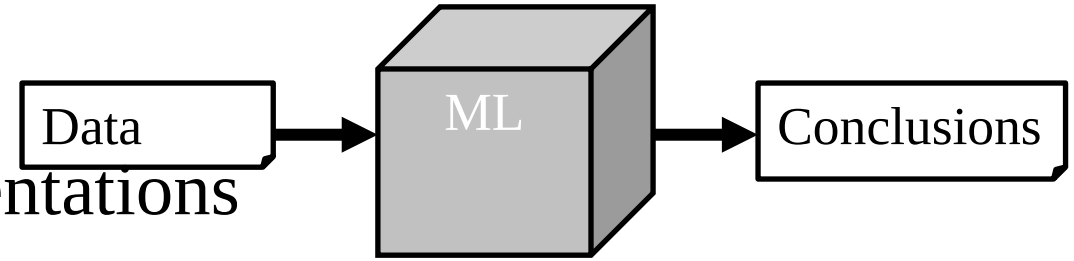
4. Results Not Explainable

- 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 AI model implementations
- Need Trustable AI = Explainable AI



$\Rightarrow$ 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.

©2026 Raj Jain

5. Wrong Metrics

- In Image analysis:
  Cost of predicting "0" when it is "1" = Cost of predicting "1" when it is "0."
  ⇒ Cost of errors is symmetric ⇒ Almost all metrics are symmetric.
- In Cyber Security:
  - Cost of missing an attack = 10^6 × Cost of false attack prediction
  - Newsweek (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 AI Technique ⇒ 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

©2026 Raj Jain

Jain's List of Issues Challenges with AI

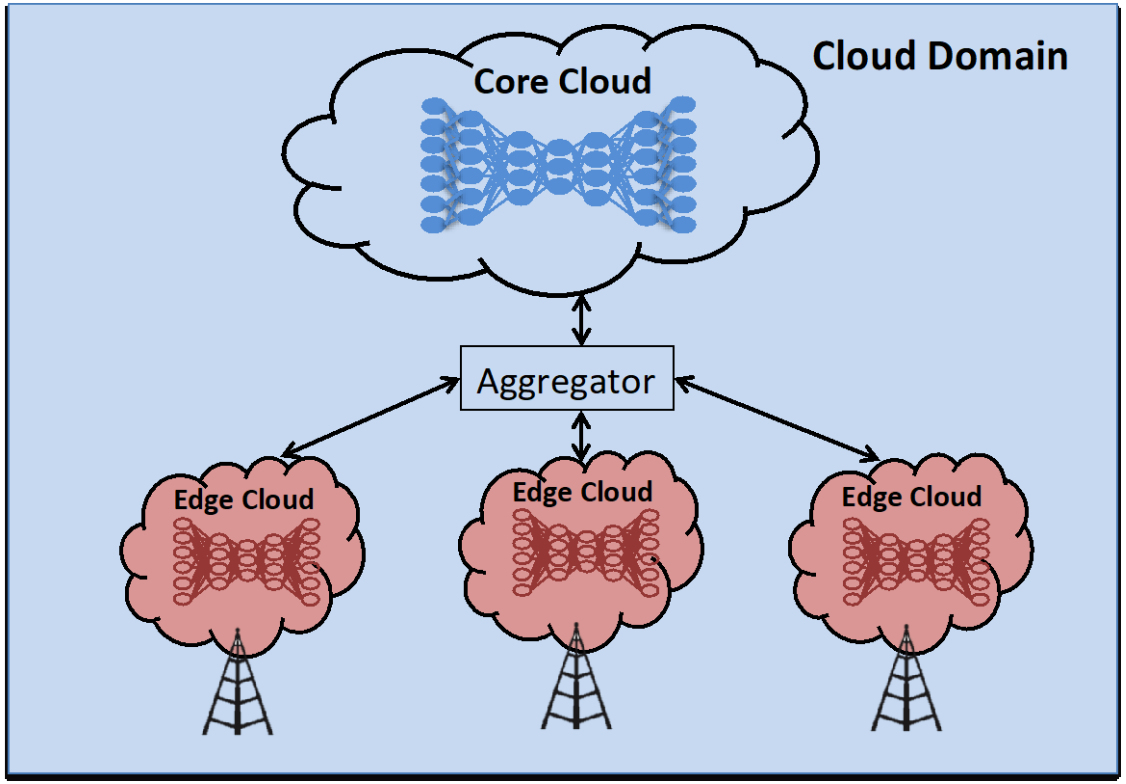
1. No Domain Expertise
2. Random Datasets
3. Imbalance of Security Data
4. Results Not Explainable
5. Wrong Performance Metrics
6. Too Few or Too Many Features
7. No Sensitivity Analysis
8. No Real-World Validation
9. Omitting Assumptions and Limitations

Issues ⇒ Challenges ⇒ Opportunities for Research.

©2026 Raj Jain

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**"
- Provides energy-efficient **privacy-preserving** threat detection without centralizing raw data



Federated Learning is privacy-preserving and avoids large transfers

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

©2026 Raj Jain

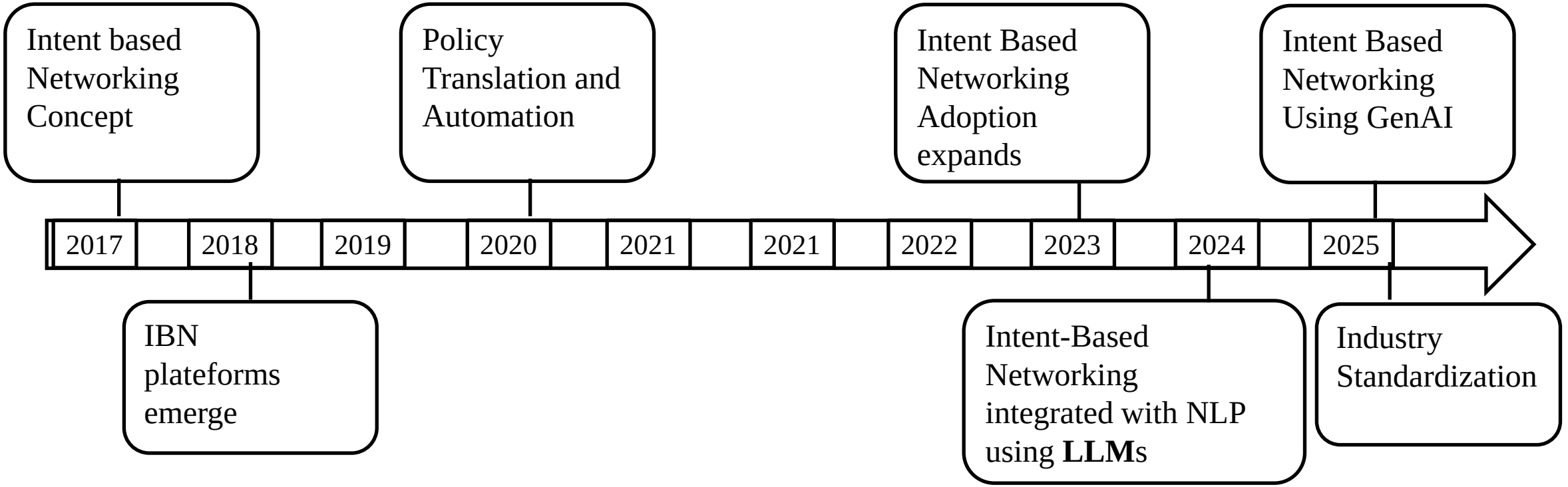
Part 2
Recent Developments in AI and their Impact on Security

Seven Generations of AI

2025	**7. Agentic AI**	Plan, Decide, Act Autonomously
2025	**6. Generative AI (GenAI)**	Generate New Concepts
2024	5. Real-Time Multi-Modal Agents (**RTMMA**)	Integrated Voice, Video, and Data
2018	4. Generative Pre-Trained Transfer (**GPT**)	Reduce Training Time ⇒ **LLM**
2017	3. Transformers	Transformers ⇒ Language
2006	2. Deep Learning (**DL**)	Unsupervised Learning
1980	1. Machine Learning (**ML**)	Supervised Learning

For security, you can use Transformers. GenAI, and Agentic AI are coming.

Intent-Based Networking (IBN)



Intent-Based Networking allows network operations using natural language.

Ref: S. Kapoor, et al., "GenAI-powered Intent-Based Autonomous Networks: Standardisation Landscape and Emerging Industry Trends," Authorea 2025, https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.175756256.63633045

©2026 Raj Jain

GenAI-Driven Phishing and Attacks

- Phishing has increased by 40X in the last three years.
- GenAI and LLM powered website generators and **deepfake audio/video** tools
  - Hyper-realistic phishing scheme and social engineering campaigns
  - Real-time impersonations of executives on phone calls or video meetings
  - Wire frauds impersonating finance chiefs
- Commodity phishing-as-a-service (PhaaS) platforms. Cost ~$50.
- Polymorphic phishing kits automatically mutate message content, bypassing signature-based spam and security filters ⇒ Zero-day social engineering

GenAI has increased phishing by 40X

Ref: Michael Siegel, S. Zeijlemaker, V. Baxi, and S. Raajah, "Rethinking the Cybersecurity Arms Race: When 80% of Ransomware Attacks are AI-Driven ," MIT Sloan School working Paper Series CAMS25.1114, 31 pp., April 10, 2025, https://cams.mit.edu/wp-content/uploads/Safe-CAMS-MIT-Article-Final-4-7-2025-Working-Paper.pdf

©2026 Raj Jain

Generative AI for Phishing Defense

- AI and machine learning tools for phishing detection, anomaly spotting
  - Analyze subtle linguistic cues, behavioral patterns
- Attacks and defenses continuously leapfrog each other
- Need to invest in AI-powered anti-phishing tools and staff training to avoid phishing attacks using email, messaging, and collaboration platforms.
- Need **AI cybersecurity governance** to ensure no critical data leakage by unrestricted use of AI by employees: Samsung semiconductor source code leak, pasting API keys and passwords into ChatGPT, Confidential meeting transcripts uploaded to public clouds.

Invest in GenAI tools for defense.

Cisco AI Canvas

- **GenAI** dashboard for:
  - **NetOps**: Network Operations, automation and orchestration
  - **SecOps**: Integrate IT operations and security teams
  - **DevOps**: Collaborative software development by developers and operations
  - Real-time analytics and collaborative troubleshooting
- Uses Deep Learning and LLMs
- Works across on-prem, cloud, multi-cloud, and hybrid deployments
- **AgenticOps**: Autonomous agents that reason, act, and learn across domains

Ref: Cisco, "Announcing Cisco AI Canvas. Revolutionizing IT with AgenticOps." June 10, 2025, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m06/announcing-cisco-ai-canvas-revolutionizing-it-with-agenticops.html

©2026 Raj Jain

Agentic AI

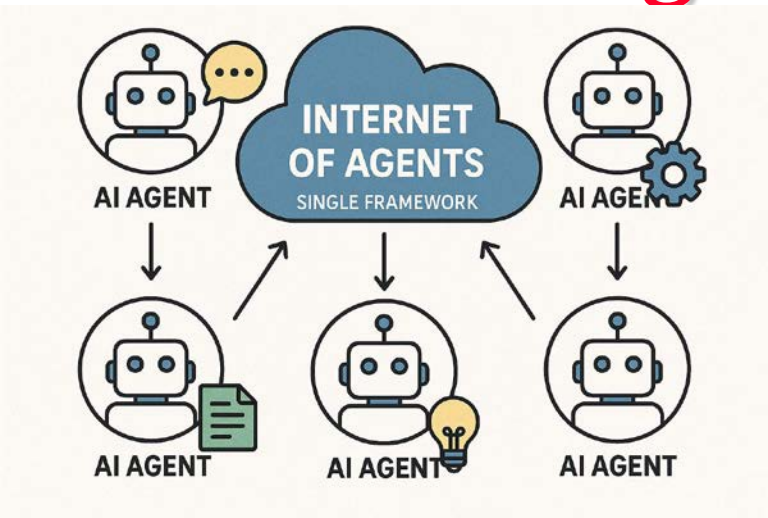
- **Agents**:
  - Independently or semi-autonomously performing tasks on behalf of a client, e.g., Insurance Agent, Real Estate Agent, Copilot, Gemini, …
- **Agentic**: Adjective
  - Capable of achieving outcomes independently
- **Agentic AI**: Programs that can make decisions, take actions, solve problems, reason, etc., on their own. This is beyond simple chatbots that respond to your queries.
  Example: Resolve a customer service issue or issue a refund without any human oversight.

Be ready to invest in AgenticOps tools.

Ref: Merriam-Webster Dictionary

©2026 Raj Jain

Internet of AI Agents



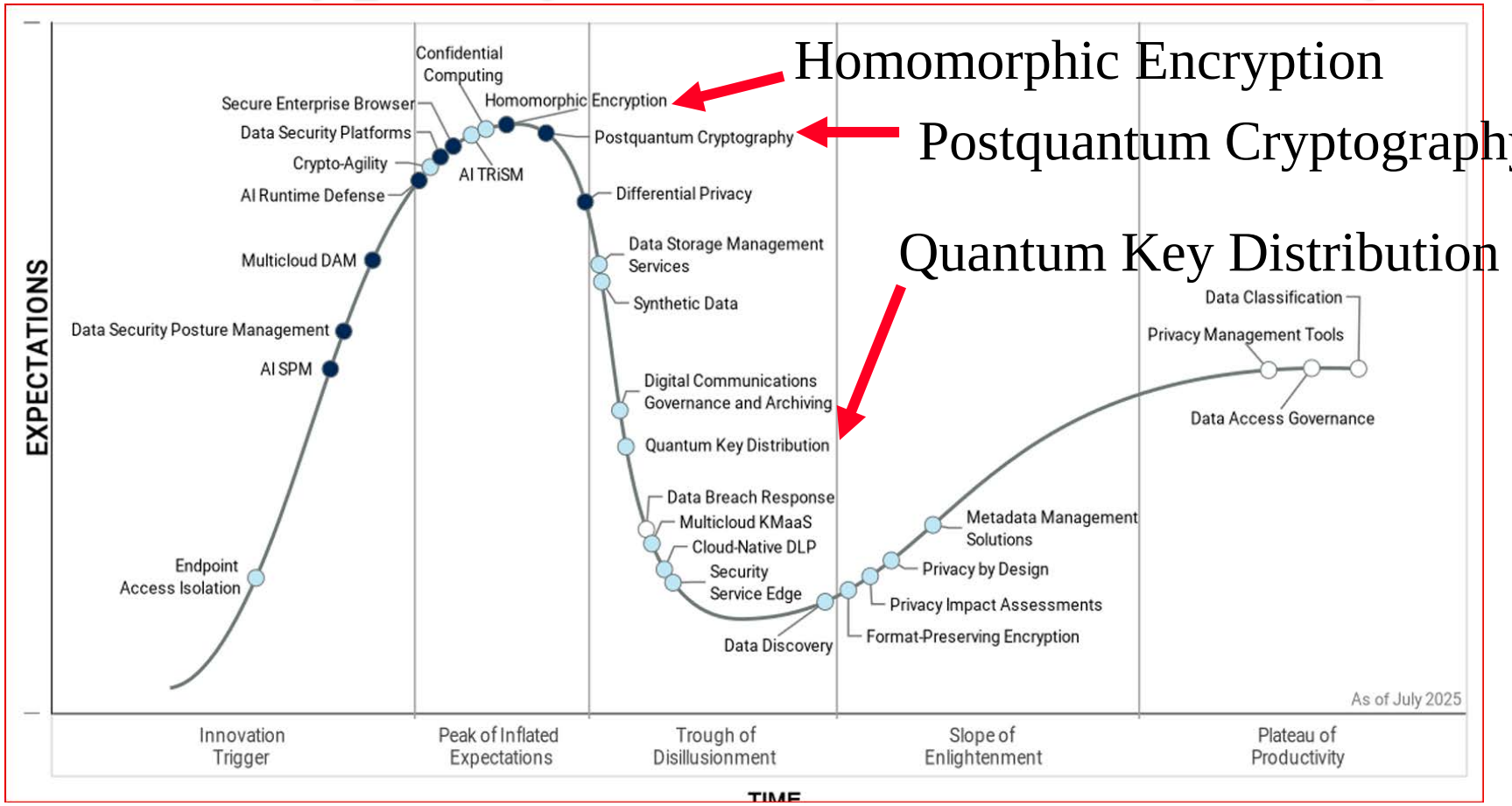
- A distributed Network of autonomous or semi-autonomous software entities powered by AI, e.g., travel agents need to communicate with airline, hotel, car rental agents.
- Special protocols are being developed for interconnection of AI agents
- AGNTCY effort in Linux Foundation.

Ref: S. Almekinders, "Cisco donates AGNTCY to Linux Foundation: what does that mean for Internet of Agents?" Jul 30, 2025, https://www.techzine.eu/blogs/infrastructure/133408/cisco-donates-agntcy-to-linux-foundation-internet-of-agents-on-its-way/

©2026 Raj Jain

Part 3
Security Technologies Coming Soon – Ready for Trials

Gartner's Hype Cycle for Data Security Techs 2025



Homomorphic Encryption, Postquantum Cryptography, and QKD are here.

Ref: A. Bales, "Hype Cycle for Data Security Technologies, 2025," Gartner ID G00828131, 10 July 2025, 114 pp. (Available by subscription).

Quantum Computing

- Current Security Methods are largely based on RSA, which is based on the difficulty of factorization of large numbers
- As the computers become faster, we keep increasing the key size: RSA-1024, RSA-2048, …
- **Quantum Threat**: Peter Shor showed in 1994 that quantum computers can factorize numbers exponentially faster than legacy computers.

Adopt quantum-safe security.

©2026 Raj Jain

Post-Quantum Cryptography

- The National Institute of Standards and Technology (NIST) has finalized:
  - **FIPS 203: ML-KEM**: Based on CRYSTALS-Kyber (lattice-based) replaces RSA and ECC for secure key distribution.
  - **FIPS 204: ML-DSA**: Based on CRYSTALS-Dilithium and FALCON (also lattice-based) for digital signatures.
  - **FIPS 205: SLH-DSA**: Based pm SPHINCS+ for hash-based signatures. For long-term integrity in archival and regulatory environments
- Hardware vendors have incorporated quantum-resistant algorithms:
  - Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs)

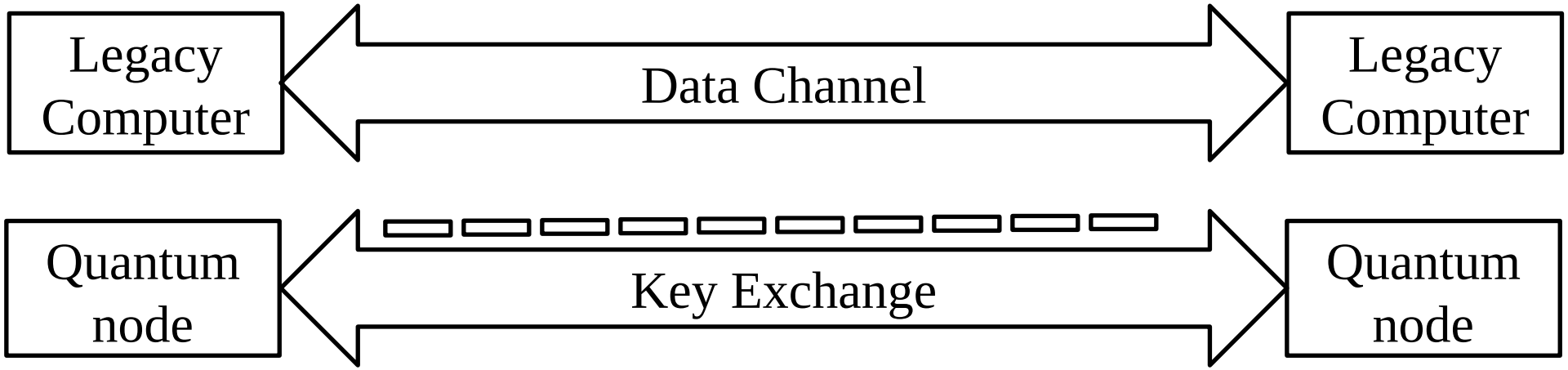
PQC will help you protect from "Harvest Now Decrypt Later" Attacks.

Ref: Post-Quantum Cryptography Coalition, https://pqcc.org

©2026 Raj Jain

Quantum Key Distribution (QKD)

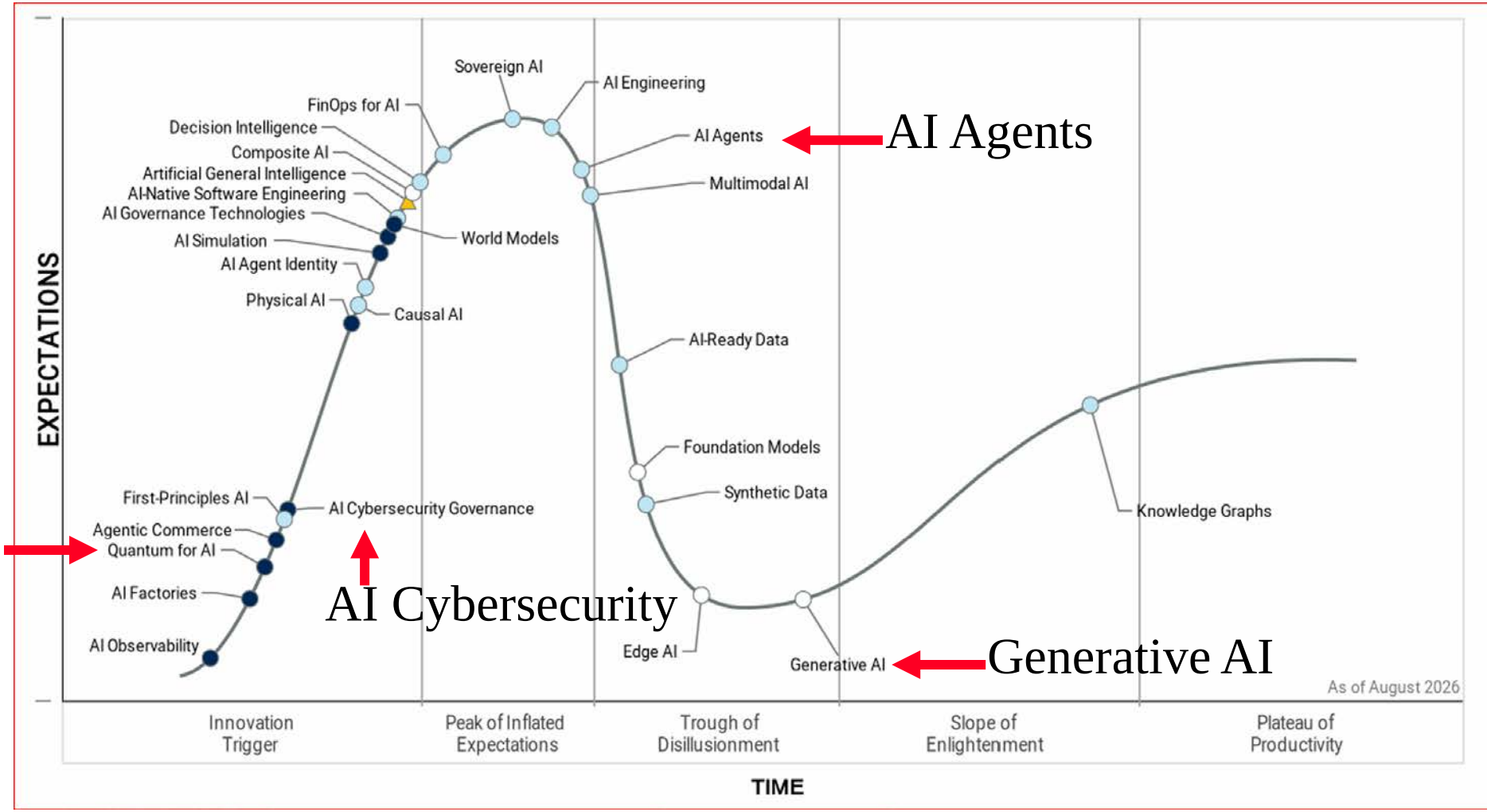
- Quantum computers are not yet suitable for very high-speed data transfer
- One important property of quantum bits (qubits) is that if you read it, it is destroyed ⇒ If anyone on the way reads a qubit, the receiver will know
- Quantum Link is a secure way to transfer encryption keys.
- While data goes on the traditional networks



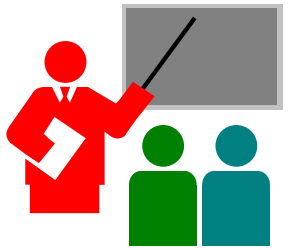
QKD is being used now for highly secure cryptographic key exchange

©2026 Raj Jain

Gartner's Hype Cycle for AI 2026



Ref: H. Khandabattu, B. Tamersoy, S. Barot, "Hype Cycle for Artificial Intelligence, 2026," Gartner Report ID G00846822, 28 August 2026, 109 pp. (Available by subscription).



Summary

1. **Common Issues**: No domain expertise, Random datasets, Imbalance, No explainability (use TrustXAI), Wrong Metrics (use Safety Score), …
2. **Use Now**: Intent-based networking, GenAI, AI Agents, Postquantum Computing, Quantum Key Distribution
3. **Ready for Trial**: Agentic AI, Internet of AI agents
4. Issues: AI Cybersecurity, Quantum for AI,

Our Publications on Quantum

- M. Mahmud, R. Jain, Z. Yang, C. Tian, R. Kompella, R. Nezabati, E. Kaur, A. Erbad, M. Abdallah, "Quantum Error Correction Survey, IEEE Access, Accepted September 2026, 43 pp., http://www.cse.wustl.edu/~jain/papers/qec_access.htm
- Zebo Yang, Ali Ghubaish, Raj Jain, Ala Al-Fuquha, Aiman Erbad, Ramana Compella, Hassan Shapourian, Reza Nejabati, "Layer-Wise Security Framework and Analysis for the Quantum Internet," IEEE Selected Areas in Communications, Vol. 43, Issue 8, pp. 2825-2840, Aug. 2025, http://www.cse.wustl.edu/~jain/papers/quint.htm
- Zebo Yang, Ali Ghubaish, Raj Jain, Ramana Kompella, and Hassan Shapourian, "Multi-Tree Quantum Routing in Realistic Topologies," IEEE Communications Magazine, Vol. 62, No. 10, October 2024, pp. 78-85, http://www.cse.wustl.edu/~jain/papers/multitree.htm
- Zebo Yang, Ali Ghubaish, Raj Jain, and H. Shapourian, "Asynchronous Entanglement Routing for the Quantum Internet," AVS Quantum Sci. 6, 013801, Jan 2024, http://www.cse.wustl.edu/~jain/papers/qrout.htm
- Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto DiPietro, and Aiman Erbad, "A Survey and Comparison of Post-quantum and Quantum Blockchains," IEEE Communications Surveys & Tutorials, 2nd Quarter 2024, Vol. 26, Issue 2, http://www.cse.wustl.edu/~jain/papers/qbpqb.htm

Our Publications on Quantum (Cont)

- 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/qbif.htm
- Zebo Yang, "Scaling Quantum Systems: Quantum Networks, Distributed Quantum Computing, and Security," Ph.D. Thesis, Washington University, May 2025, http://www.cse.wustl.edu/~jain/theses/zebophd.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, M. Noorizadeh, M. Shakerpour, N. Meskin, K. Khan, R. Jain, "A Machine Learning Based Framework For Real-time Detection and Mitigation of Sensor False Data Injection Cyber-Physical Attacks in Industrial Control Systems," IEEE Access, Aug 2023, http://www.cse.wustl.edu/~jain/papers/rt_iot.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 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

©2026 Raj Jain

Our Publications on ICS Security (Cont)

- 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
- 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

©2026 Raj Jain

Our Publications on Healthcare Security

- Ali Ghubaish, Zebo Yang, Raj Jain, "HDRL-IDS: A Hybrid Deep Reinforcement Learning Intrusion Detection System for Enhancing the Security of Medical Applications in 5G Networks," 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), Best Paper Award, May 2024, http://www.cse.wustl.edu/~jain/papers/hdrl.htm
- 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

©2026 Raj Jain

Our Publications on Blockchains

- Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto DiPietro, and Aiman Erbad, "A Survey and Comparison of Post-quantum and Quantum Blockchains," IEEE Communications Surveys & Tutorials, 2nd Quarter 2024, Vol. 26, Issue 2, http://www.cse.wustl.edu/~jain/papers/qbpqb.htm
- Tara Salman, Ali Ghubaish, and Roberto Di Pietro, Mohammed Baza, Hani Alshahrani, Raj Jain, and Kim-Kwant Raymond Choo, "CrowdFAB: A Framework for Crowdsourced Forecasting Applications using Blockchains and its use for Security," IEEE Transactions on Dependable and Secure Computing, 2023, http://www.cse.wustl.edu/~jain/papers/crowdfab.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/fintech.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/qbif.htm

©2026 Raj Jain

Our Publications on Blockchains (Cont)

- Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto DiPietro, and Aiman Erbad, "A Survey and Comparison of Post-quantum and Quantum Blockchains," IEEE Communications Surveys & Tutorials, 2nd Quarter 2024, Vol. 26, Issue 2, http://www.cse.wustl.edu/~jain/papers/qbpqb.htm
- Tara Salman, Ali Ghubaish, and Roberto Di Pietro, Mohammed Baza, Hani Alshahrani, Raj Jain, and Kim-Kwant Raymond Choo, "CrowdFAB: A Framework for Crowdsourced Forecasting Applications using Blockchains and its use for Security," IEEE Transactions on Dependable and Secure Computing, 2023, http://www.cse.wustl.edu/~jain/papers/crowdfab.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/fintech.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

©2026 Raj Jain

Our Publications on Blockchains (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, 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

©2026 Raj Jain

Acronyms

- ADDAI Anomaly Detection using Distributed AI
- AgenticAI Agentic Artificial Intelligence
- AgenticOp Agentic Operation
- AI Artificial Intelligence
- AIChain Artificial Intelligence for Blockchain
- AIIoT AI Internet of Tthings
- APT Advanced Persistent Threats
- CCA Confidential Computing Architecture
- CEO Chief Executive Officer
- CISA Cybersecurity Infrastructure Security Agency
- CNC Computer Networking and Communications
- CRYSTALS Cryptographic Suite for ALgebraic Lattices
- DDoS Distributed Denial of Service
- DevOp Development and Operations

©2026 Raj Jain

Acronyms (Cont)

- DID Decentralized identity
- DSA Digital Security Algorithm
- ECC Elliptic Curve Cryptography
- EO Executive Order
- FALCON Fast-Fourier Lattice-based Compact Signatures over NTRU
- FHEW Fast-Fourier Lattice-based Homomorphic Encryption over the Weintrob ring
- FIPS Federal Information Processing Standard
- FP7 Framework Program 7
- GDPR General Data Protection Regulation
- GPU Graphical Processing Unit
- HDRL Hybrid Deep Reinforcement Learning
- HE Homomorphic Encryption

©2026 Raj Jain

Acronyms (Cont)

HSM	Hardware Security Module
HVAC	Heating, Ventilation, and Air Conditioning
HYPER-VINES	HYbrid Learning Fault anHYbrid Learning Fault and Performance Issues ERadicator for VIrtual NEtwork Services
IBN	Intent-Based Networking
ICISS	Information Science and Security
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IEEE	Institution of Electrical and Electronics Engineers
IET	Institution of Engineering and Technology
IFAC	International Federation of Automatic Control
IIoT	Industrial Internet of Things

Acronyms (Cont)

- IoMT Internet of Medical Things
- IoT Internet of Things
- ISI Intelligence and Security Informatics
- IT Information Technology
- KDD Knowledge Discovery and Data Mining
- KEM Key Encapsulation Mechanism
- LLM Large Language Models
- ML Machine Learning
- NetOp Network Operations
- NIST National Institute of Standards and Technology
- NLP Natural language processing
- NTRU Nth-Degree Truncated Polynomial Ring Units
- OMB Office of Management and Budgets

©2026 Raj Jain

Acronyms (Cont)

PhaaS	Phishing-as-a-service
RSA	Rivest, Shamir, and Adleman
SCADA	Supervisory Control and Data Acquisition
SecOp	Security and Operations
SEV	SEV-SNP, NVIDIA Confidential GPUs,
SLH	Stateless Hash Based
SPHINCS	Stateless Practical Hash-based INternet Compact Hash-based Encryption Scheme Signature
TIP	Testing in production
TPM	Trusted Platform Modules
TPU	Tensor processing units
TrustXAI	Trustworthy Explainable AI
UMSL	University of Missouri, Saint Louis
XAI	Explainable AI
ZKP	Zero-Knowledge Proof

©2026 Raj Jain

Scan This to Download These Slides



Thank you!

Raj Jain

Rajjain.com or
http://www.cse.wustl.edu/~jain

http://www.cse.wustl.edu/~jain/talks/globalai26.htm

©2026 Raj Jain