Last Updated: 6/8/2025

Ben Lazarine

belazar@iu.edu, 774.288.0177

Department of Operations and Decision Technologies — Kelley School of Business
Indiana University, Bloomington — 1275 E. 10th Street, Bloomington, IN 47401

EDUCATION

Ph.D., Information Systems, Indiana University, Bloomington — 2021-2026 (Expected)

- Minor: Data Science
- Advisor: Dr. Sagar Samtani
- Research Associate in Kelley's Data Science and Artificial Intelligence Lab
- Center for Applied Cybersecurity Research Student Fellow

M.S., Management Information Systems (MIS), University of Arizona — 2019-2021

- NSF CyberCorps Scholarship-for-Service (SFS) Fellow
- Advisor: Dr. Hsinchun Chen

B.S., Management Information Systems (MIS), University of Arizona — 2015-2019

- **Minor**: Computer Science
- Graduated Magna Cum Laude

RESEARCH INTERESTS

Applications: Cybersecurity, AI risk, open-source intelligence, open-source software security
Methods: Deep learning, self-supervised learning, large language models, social network analysis

DISSERTATION

Title: Mapping, Measuring, Managing, and Governing Vulnerabilities in Artificial Intelligence in Open-Source Software: Deep Learning and Large Language Model Perspectives

Abstract: Artificial Intelligence (AI) methods such as large language models (LLMs), computer vision, graph neural networks have provided unprecedented efficiencies and capabilities for modern organizations worldwide. Recently, AI developers and adopters alike have leveraged open-source (OS) practices to spur the development of millions of models and thousands of AI applications. However, OS AI introduces unique security issues, including model vulnerabilities, that existing cybersecurity procedures are not well-suited to address. This dissertation presents four essays grounded in the NIST AI Risk Management Framework (RMF). Guided by the principles of the computational design science paradigm, each essay presents a novel Information Technology (IT) artifact based on deep learning and LLMs to manage OS AI security. Essay 1 aims to detect implicit linkages between AI repositories through a self-supervised graph learning approach to map vulnerability spread in OS AI assets. Essay 2 seeks to retrieve alternatives to vulnerable OS AI assets and measure the vulnerability reduction through a multi-view learning-based information retrieval. Essay 3 profiles international OS AI development communities' security practices, constructing a novel LLM-based method to generate community-focused security management strategies. Essay 4 presents a novel LLM-based approach towards OS AI security governance through context-driven vulnerability management policies. Each essay offers potential practical utility, helping MLOSS users, adopters, developers, and security groups map, rank, remediate, and manage AI security concerns in accordance with the NIST AI RMF. Each essay also contributes to the information systems knowledge base through design principles that can inform future system designs in related cybersecurity applications.

Committee Members: Dr. Sagar Samtani (Chair), Dr. Ramesh Venkataraman (Member), Dr. Brad Wheeler (Member), Dr. Haizhen Lin (Member), Dr. Dongruo Zhou (Member)

Status: Proposal Defended; Final Defense in Spring 2026.

PUBLICATIONS

Journal Papers

1. S. Ullman, S. Samtani, H. Zhu, **B. Lazarine**, H. Chen, and J. Nunamaker "Enhancing Vulnerability Prioritization in Cloud Computing Using Multi-View Representation Learning" ***Journal of Management Information Systems (JMIS),*** 41(3), 708-743, 2024**.**

Journal Papers Under Review

1. S. Ullman, **B. Lazarine**, S. Samtani, H. Zhu, and H. Chen "Linking Vulnerabilities in Cyberinfrastructure With Their Remediations: A Contrastive Self-Supervised Learning Approach" **Invited for Third Round Review at *Information Systems Research (ISR).***

Journal Manuscripts in Preparation

1. **B. Lazarine**, H. Zhu, S. Samtani, R. Venkataraman, and J. Nunamaker "Identifying Linked Artificial Intelligence Repositories on GitHub: A Graph Self-Supervised Learning Approach," **Preparing for submission to the *Journal of Management Information Systems (JMIS).***
2. **B. Lazarine**, S. Ullman, H. Zhu, S. Samtani, and R. Venkataraman "Suggesting Alternatives for Insecure Machine Learning Repositories: A Multi-View Graph Transformer Approach," **Targeted at *Management Information Systems Quarterly (MISQ)*.**
3. **B. Lazarine**, B. Ampel, R. Venkataraman, and S. Samtani "Profiling and Managing Vulnerabilities Across International AI Development: A Large Language Model Approach," **Invited to *Management Information Systems Quarterly (MISQ)* AI-IA Nexus Special Issue Workshop.**
4. A. Sachdeva, **B. Lazarine**, H. Zhu, S. Samtani, and R. Venkataraman "Predicting Vulnerability Introduction in Social Coding Repositories: A Dynamic Graph Embedding Approach," **Targeted at *Management Information Systems Quarterly (MISQ)*.**
5. **B. Lazarine**, W. Rosengren, Z. Lin and S. Samtani "Identifying and Profiling Key Sellers in Cyber Carding Community: An Exact Replication Study," **Targeted at *Transactions on Replication Research (TRR)*.**

Refereed Conference Proceedings (* Indicates that I was a presenting author)

1. **B. Lazarine***, S. Pulipaka, S. Samtani, R. Venkataraman, "Collecting, Linking, and Assessing Machine Learning Open-Source Software: A Large Scale Collection and Vulnerability Assessment Pipeline," In Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, January 2025.
2. **B. Lazarine***, S. Samtani, H. Zhu, R. Venkataraman, "Suggesting Alternatives for Potentially Insecure Artificial Intelligence Repositories: An Unsupervised Graph Embedding Approach," In Hawaii International Conference on System Sciences (HICSS), Honolulu, Hawaii, January 2024.
3. A. Kathikar, A. Nair, **B. Lazarine***, A. Sachdeva, S. Samtani, "Assessing the Vulnerabilities of the Open-Source Artificial Intelligence (AI) Landscape: A Large-Scale Analysis of the Hugging Face Platform," In Proceedings of 2023 IEEE International Conference on Intelligence and Security Informatics (ISI), Charlotte, North Carolina, October 2023.
4. A. Sachdeva, **B. Lazarine**, H. Zhu, S. Samtani, "User Profiling and Vulnerability Introduction Prediction in Social Coding Repositories: A Dynamic Graph Embedding Approach: Vulnerability

Introduction Prediction in Social Coding Repositories," In Cyber Security Experimentation and Test Workshop (CSET), Virtual, California, August 2023.

5. A. Sachdeva, **B. Lazarine**, R. Dama, S. Samtani, H. Zhu, "Identifying Patterns of Vulnerability Incidence in Foundational Machine Learning Repositories on GitHub: An Unsupervised Graph Embedding Approach," In International Conference on Data Mining Workshop on Machine Learning for Cybersecurity (ICDM MLC), Orlando, Florida, November 2022.
6. **B. Lazarine**, Z. Zhang, A. Sachdeva, S. Samtani, and H. Zhu, "Exploring the Propagation of Vulnerabilities from GitHub Repositories Hosted by Major Technology Organizations," In Cyber Security Experimentation and Test Workshop (CSET), Virtual, California, August 2022.
7. C. Marx, B. Ampel, and **B. Lazarine***, "The Influence of AI-Agent Recommendations on Escalation of Commitment," In Proceedings of 2021 AIS International Conference on Information Systems (ICIS), Austin, Texas, December 2021.
8. **B. Lazarine***, S. Samtani, M. Patton, H. Zhu, S. Ullman, B. Ampel, and H. Chen, "Identifying Vulnerable GitHub Repositories and Users in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach," In Proceedings of 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Washington, D.C., November 2020.
9. S. Ullman, S. Samtani, **B. Lazarine**, H. Zhu, B. Ampel, M. Patton, and H. Chen, "Smart Vulnerability Assessment for Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach," In Proceedings of 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), Washington, D.C., November 2020.
10. N. Arnold, M. Ebrahimi, N. Zhang, **B. Lazarine**, S. Samtani, M. Patton, and H. Chen, "Dark-Net Ecosystem Cyber- Threat Intelligence (CTI) Tool," In Proceedings of 2019 IEEE Conference on Intelligence and Security Informatics (ISI). Shenzhen, China, July 2019
11. P. Du, N. Zhang, M. Ebrahimi, S. Samtani, **B. Lazarine**, N. Arnold, R. Dunn, S. Suntwal, G. Angeles, R. Schweitzer, and H. Chen, "Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs," In Proceedings of 2018 IEEE Conference on Intelligence and Security Informatics (ISI). Miami, Florida, November 2018.

Refereed Workshop Papers (No Proceedings)

1. A. Sachdeva, **B. Lazarine**, S. Samtani, and H. Zhu, "User Profiling and Vulnerability Introduction Prediction in Social Coding Repositories: A Dynamic Graph Embedding Approach," In 2022 INFORMS Workshop on Data Science, Indianapolis, Indiana, October 2022.
2. **B. Lazarine***, A. Sachdeva, S. Samtani, and H. Zhu, "Identifying Linked Repositories on GitHub: A Self-Supervised Graph Embedding Approach," In 2022 INFORMS Workshop on Data Science, Indianapolis, Indiana, October 2022.

INVITED TALKS AND EXTERNAL PRESENTATIONS

1. 2025 Hawaii International Conference on System Sciences (HICSS). **Presentation Title:** "Analyzing Vulnerabilities in Machine Learning Open-Source Software: An Introduction and Tutorial" January 6, 2025.
2. Spring 2024 Institute for Digital Enterprise (IDE) Digital Unleashed: Bridging Research and Practice on AI, Cybersecurity, and Digital Transformation. **Presentation Title:** "Identifying Linked Artificial Intelligence Repositories on GitHub: A Graph Self Supervised Learning Approach" April 19, 2024.
3. Fall 2023 Institute for Business Analytics (IBA) Conference on Generative AI and Cybersecurity: Navigating the New Era of Threats and Safeguards. **Presentation Title:** "Assessing the

Vulnerabilities of the Open-Source AI Landscape: A Large-Scale Analysis of the Hugging Face Platform" November 10, 2023.

4. NSF Cybersecurity Summit Vulnerability Management Workshop. **Presentation Title:** "Detecting and Linking Vulnerabilities in Scientific Cyberinfrastructure to MITRE ATT&CK" October 19, 2021.
5. NSF Cybersecurity Summit. **Presentation Title:** "Identifying Vulnerable GitHub Repositories in Scientific Cyberinfrastructure: An Artificial Intelligence Approach" October 13, 2021.

RESEARCH GRANTS

Grant Experience

- **Year**: 2025. **Grant Title:** "CICI: TCR: Enhancing the Resilience of Open Source Artificial Intelligence Software: Vulnerability Detection and Deep Learning-based Linkage and Remediation" **Funding source:** National Science Foundation. **Funding Amount:** $1,200,000. **Status:** Under Review. **Role**: Lead Grant Writer.
- **Year**: 2023. **Grant Title:** "CICI: UCSS: Enhancing the Usability of Vulnerability Assessment Results for Open-Source Software Technologies in Scientific Cyberinfrastructure: A Deep Learning Perspective" **Funding source:** National Science Foundation. **Funding Amount:** $600,000. **Status:** Accepted. **Role**: Assisting Grant Writer.
- **Year**: 2021. **Grant Title:** "CICI: Proactively Detecting, Categorizing, and Mitigating Configuration and Social Coding-based Vulnerabilities in Scientific Cyberinfrastructure: An AI-enabled Scientific Infrastructure Vulnerability Discovery (SIVD) Approach" **Funding source**: National Science Foundation. **Funding Amount**: $500,000. **Status:** Declined. **Role**: Assisting Grant Writer.

TEACHING EXPERIENCE

Semester	Course	Location	Teaching Score
Fall 2024	**K353**: Business Analytics and Modeling	Indiana University	6.2/7
Fall 2023	**K353**: Business Analytics and Modeling	Indiana University	6.3/7

PROFESSIONAL SERVICE

Ad-hoc Reviewer (3 Journals):

- IEEE Transactions on Engineering Management (TEM), 2024.
- Digital Threats: Research and Practice (DTRAP), 2022.
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2020.

Ad-hoc Reviewer (7 Conferences):

- AAAI Workshop on Artificial Intelligence for Cyber Security (AICS), 2025.
- ACM KDD Workshop on AI-enabled Cybersecurity Analytics (AI4Cyber), 2024.
- Hawaii International Conference on System Sciences (HICSS), 2023.
- Conference on Applied Machine Learning for Information Security (CAMLIS), 2023.
- The Americas Conference on Information Systems (AMCIS), 2023.
- INFORMS Workshop on Data Science (WDS), 2022.
- Conference on Information Systems and Technology (CIST), 2022.

Other Service to the Field (IS):

- Program Committee Member, ACM KDD Workshop on AI-enabled Cybersecurity Analytics (AI4Cyber). 2024. Washington, DC.
- Volunteer, Conference on Applied Machine Learning for Information Security (CAMLIS), 2022. Arlington, Virginia.

- Volunteer, INFORMS Workshop on Data Science (WDS), 2022. Indianapolis, Indiana.
- Webmaster, Conference on Applied Machine Learning for Information Security (CAMLIS), 2022. Arlington, Virginia.
- Program Committee Member, ACM KDD Workshop on AI-enabled Cybersecurity Analytics and Deployable Defense (AI4Cyber/MLHat). 2022. Washington, DC.
- Volunteer, International Conference on Information Systems (ICIS), 2021. Austin, Texas.
- Volunteer, INFORMS Workshop on Data Science (WDS), 2021. Virtual.
- Webmaster, KDD Workshop on AI-enabled Cybersecurity Analytics, 2021. Singapore (Virtual).

HONORS & AWARDS

- Operations and Decision Technologies ICIS Doctoral Consortium Nominee (2025)
- Panschar Undergraduate Teaching Award Finalist (2025)
- Alan R. Dennis Doctoral Fellow (2024)
- Robert James Waller Doctoral Fellow (2024)
- Center for Applied Cybersecurity Research Fellow (2024-2025)
- Institute for Digital Enterprise (IDE) Digital Unleashed Best Presentation Award (2024)
- AMCIS Outstanding Reviewer (2023)
- CyberCorps: NSF Scholarship-for-Service Fellow (2019-2021)
- Eller Business School Circle of Excellence Inductee (2019)

PROFESSIONAL AFFILIATIONS AND SOCIETIES

1. Association for Information Systems (AIS), Member
2. The Institute for Operations Research and the Management Sciences (INFORMS), Member
3. Association for Computing Machinery (ACM), Member
4. Institute of Electrical and Electronics Engineers (IEEE), Member

RELEVANT TECHNOLOGY SKILLS

1. **Databases:** MySQL, PL/SQL
2. **Programming Languages:** Python, Java
3. **Web Development:** HTML, JavaScript, WordPress
4. **Visualization tools:** Tableau, Gephi
5. **Data mining tools:** RapidMiner, WEKA, scikit-learn

WORK EXPERIENCE

Indiana University — **Bloomington, Indiana**
Graduate Research Assistant — August 2021 – Present

Artificial Intelligence Laboratory — **Tucson, Arizona**
NSF Research Experience for Undergraduates Student — February 2017 – May 2019

USAA — **San Antonio, Texas**
Software Developer and Integrator — Summer 2018

PROFESSIONAL REFERENCES

1. **Sagar Samtani, Ph.D. (Dissertation Committee Chair)**
   Associate Professor and Arthur M. Weimer Faculty Fellow

Executive Founding Director, Data Science and Artificial Intelligence Lab
Founding Editor-in-Chief, *ACM Transactions on AI Security and Privacy*
Kelley School of Business
Indiana University, Bloomington
Email: ssamtani@iu.edu
Phone: 812.855.8925

2. **Ramesh Venkataraman, Ph.D. (Dissertation Committee Member)**
   John R. Gibbs Professor of Information Systems
   Acting Co-Director, Data Science and Artificial Intelligence Lab
   Dean, Hutton Honors College
   Kelley School of Business
   Indiana University, Bloomington
   Email: venkat@iu.edu
   Phone: 812.855.2641
3. **Brad Wheeler, Ph.D. (Dissertation Committee Member)**
   Sungkyunkwan Professor of Information Systems
   IU James H. Rudy Professor
   Acting Co-Director, Data Science and Artificial Intelligence Lab
   Advisor to the Dean for Technology and Innovation
   Kelley School of Business
   Indiana University, Bloomington
   Email: brad@iu.edu
   Phone: 812.855.3478
4. **Hsinchun Chen, Ph.D.**
   Regents' Professor of Management Information Systems
   Thomas R. Brown Chair of Management and Technology
   Director, Artificial Intelligence Lab
   Director, AZSecure Cybersecurity Program
   Eller College of Management
   University of Arizona
   Email: hsinchun@arizona.edu
   Phone: 520.621.2748