# Reza Ebrahimi

**Website/Lab:** https://star-ailab.github.io **E-mail:** ebrahimim@usf.edu

Assistant Professor, School of Information Systems, University of South Florida


## ACADEMIC APPOINTMENTS

| Duration | Title | Institute |
|---|---|---|
| 2026-present | Visiting Assistant Professor | University of Arizona |
| 2021-2026 | Assistant Professor | University of South Florida |
| 2016-2021 | Research Associate, Artificial Intelligence (AI) Lab | University of Arizona |
| 2015-2015 | Software Engineer Intern | SAP Canada |
| 2014-2016 | Research Associate, **Cen**ter for **Pa**ttern **R**ecognition and **M**achine **I**ntelligence (CENPARMI) | Concordia University |

## EDUCATION

- **PhD, Management Information Systems (MIS), University of Arizona, 2016 – 2021**
  - **Dissertation Title:** AI-Enabled Cybersecurity Analytics: Detecting and Defending against Cyber Threats
    - Awarded the ***ACM SIGMIS Doctoral Dissertation Award*** **at ICIS 2021**
  - **Committee Members:** Dr. Hsinchun Chen (Chair), Dr. Sue Brown, Dr. Jay F. Nunamaker
  - **Minor:** Computational Linguistics, minor advisor: Dr. Sandiway Fong
- **Master of Science, Concordia University, Montreal, 2014 – 2016**
  - **Major:** Computer Science
  - **Thesis Title:** Automatic Identification of Online Predators in Chat Logs by Anomaly Detection and Deep Learning
  - **Committee Members:** Dr. Olga Ormandjieva, Dr. Ching Y. Suen
- **Bachelor of Science, Azad University at Qazvin, 2004 – 2008**
  - **Major:** Computer Science and Engineering
  - **Thesis Title:** A Framework for Intelligent Crime Matching with Neural Network

## LAB AND RESEARCH

- Founder and Director of **S**ecure **T**rustworthy **a**nd **R**eliable (STAR) AI Lab
- **Lab Website:** **https://star-ailab.github.io/team**
- **Co-Directors:**
  - Jeremiah Birrell (Mathematics Department, Texas State University)
  - Jason Pacheco (Computer Science Department, University of Arizona)
  - Rouzbeh Behnia (School of Information Systems, University of South Florida)
- **PhD Members (Co-Advised):** James Hu (University of Arizona), Yiwei Zhang (Purdue University), Arman Riasi (Virginia Tech), Atousa Arzanipour (University of South Florida), Yanjing Ren (University of South Florida)
- **Research Areas:**
  - **Secure Trustworthy and Reliable AI:** Adversarially Robust AI Agents for Cybersecurity, Privacy Preserving AI, AI-enabled Cybersecurity Analytics, Automatic Cyber Threat Detection, Cross-lingual Security Analytics
  - **Statistical Machine Learning:** Adversarial Machine Learning, Differential Privacy, Transfer Learning and Domain Adaptation, Cross-lingual Knowledge Transfer, Reinforcement Learning, Deep Learning

- **Business Intelligence and Analytics:** Social Media Analytics, Online Predator Identification in Social Media

## JOURNALS AND SELECTED CONFERENCES

1. Lin, F., Liu, Y., Li, W., Ebrahimi, R., Chen, H., 2026, A decision support framework for privacy risk assessment on social media through automated personally identifiable information detection, *Decision Support Systems **(DSS)***, 210, p. 114752, (https://doi.org/10.1016/j.dss.2026.114752).
2. Ebrahimi, R., Chai, Y., Li, W., Pacheco, J., Chen, H., 2025, "RADAR: A Framework for Developing Adversarially Robust Cyber Defense AI Agents with Deep Reinforcement Learning," ***MIS Quarterly***, 49 (4), pp. 1385–1416, (https://doi.org/10.25300/MISQ/2024/17339).
3. Ebrahimi, R., Hu, J., Zhang, N., Nunamaker, J., Chen, H., 2025, "Defending Deep Learning-based Raw Malware Detectors Against Adversarial Attacks: A Sequence Modeling Approach," *Journal of Management Information Systems **(JMIS),*** (doi: 10.13140/RG.2.2.15331.26401).
4. Birrell, J., Ebrahimi, R., 2025, "Optimal Transport Regularized Divergences: Application to Adversarial Robustness," **SIAM** Journal on Mathematics of Data Science, 7(4), pp.1801-1827., (https://arxiv.org/pdf/2309.03791).
5. Granados A., Ebrahimi R., Pacheco J., 2025, "Risk-Sensitive Variational Actor-Critic: A Model-Based Approach," 2025, International Conference on Learning Representations (**ICLR**), (https://openreview.net/rs-VAC).
6. Ebrahimi, R., Pacheco, J., Hu J., Chen, H. ,2025, "Learning Contextualized Action Representations in Sequential Decision Making for Adversarial Malware Optimization," *IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, 22 (3), pp. 2086-2102, (https://ieeexplore.ieee.org/document/10711271).
7. Birrell J., Ebrahimi R., Behnia R., Pacheco J., 2024, "Differentially Private Stochastic Gradient Descent with Fixed-Size Minibatches: Tighter RDP Guarantees with or without Replacement," Neural Information Processing Systems (**NeurIPS**), (https://openreview.net/forum?id=TJsknGasMy&noteId=pyTbqcmR8B).
8. Zhang Y., Behnia R., Yavuz, A. A., Ebrahimi, R., Bertino, E. 2025, "Efficient Full-Stack Private Federated Deep Learning with Post-Quantum Security," *IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, (doi: 10.1109/TDSC.2025.3568704).
9. Behnia R., Riasi A., Ebrahimi R., Chow S., Padmanabhan B., Hoang T., R. 2024, "Efficient Secure Aggregation for Privacy-Preserving Federated Machine Learning," in 2024 Annual Computer Security Applications Conference (**ACSAC**), Honolulu, HI, USA, 2024, pp. 778-793, doi: 10.1109/ACSAC63791.2024.00069.
10. Ebrahimi R., Chai Y., Zhang H., Chen H., 2023, "Heterogeneous Domain Adaptation with Adversarial Neural Representation Learning: Experiments on E-Commerce and Cybersecurity," *IEEE Transactions on Pattern Analysis and Machine Intelligence (**TPAMI**)*, pp. 1862-1875.
11. Ebrahimi R., Chai Y., Samtani S., Chen H. 2022, "Cross-Lingual Security Analytics: Cyber Threat Detection in the International Dark Web with Adversarial Deep Representation Learning," ***MIS Quarterly***, 46(2), pp. 1209-1226.
12. Zhang N., Ebrahimi R., Li W., Chen H., 2022, "Counteracting Dark Web Text-Based CAPTCHA with

Generative Adversarial Learning for Proactive Cyber Threat Intelligence," *ACM Transactions on Management Information Systems (**TMIS**)*, ACM, 13(2), pp. 1-21.

13. Wen B., Hu P., Ebrahimi R., Chen, H., 2021, "Key Factors Affecting User Adoption of Open-Access Data Repositories in Intelligence and Security Informatics: An Affordance Perspective," ACM *Transactions on Management Information Systems (**TMIS**)*, 13(1), pp. 1–24.
14. Ebrahimi R., Nunamaker J., Chen, H., 2020, "Semi-Supervised Cyber Threat Identification in Dark Net Markets: A Transductive and Deep Learning Approach," *Journal of Management Information Systems (**JMIS**)*, 37(3), pp. 694-722.
15. Ebrahimi R., Martinez J., 2019, "Involuntary Embarrassing Exposures in Online Social Networks: A Replication Study," *AIS Transactions on Replication Research (**AIS TRR**)*, 5(1), pp. 1-20.
16. Ebrahimi R., Suen C.Y., Ormandjieva O., 2016, "Detecting Predatory Conversations in Social Media by Deep Convolutional Neural Networks," ***Digital Investigation**,* Elsevier, 18, pp. 33-49.
17. Keyvanpour M., Ebrahimi R., Javideh M., 2012, "Designing Efficient ANN Classifiers for Matching Burglaries from Dwelling Houses," ***Applied Artificial Intelligence**,* Taylor and Francis, 26 (8), pp. 787-807.

## PRESENTED REFEREED CONFERENCE PROCEEDINGS & WORKSHOPS

1. Behnia R., Birrell J., Raisi A., Ebrahimi R., Dutta K., Hoang T., 2025, Trustworthy Federated Learning with Local Differential Privacy, WITS, (https://arxiv.org/abs/2510.12908) **(Best Paper Award)**.
2. Arzanipour A, Behnia R., Ebrahimi, R., Dutta, K., 2025, "RAG Security and Privacy: Formalizing the Threat Model and Attack Surface," IEEE ICDM Workshop on Machine Learning for Cybersecurity.
3. Ahmadi K., Behnia R., Ebrahimi R., Kermani M., Birrell J., Pacheco J., Yavuz A., 2025 "An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Models," IEEE Security & Privacy Workshop on Human-Machine Intelligence for Security Analytics (**Best Paper Award**).
4. Zhang Y., Behnia R., Yavuz A., Ebrahimi R. Bertino E., 2024. "Uncovering Attacks and Defenses in Secure Aggregation for Federated Deep Learning," IEEE ICDM Workshop on Machine Learning for Cybersecurity.
5. Hossain S., Ebrahimi R., Padmanabhan B., El Naqa I., Kuo P.C., Beard A. Merkel S., 2023, "Robust AI-enabled Simulation of Treatment Paths with Markov Decision Process for Breast Cancer Patients," IEEE Conference on Artificial Intelligence (CAI), pp. 105-108.
6. Etter B., Hu J., Ebrahimi R., Li W., Li X., and Chen H., 2023, "Evading Deep Learning-Based Malware Detectors via Obfuscation: A Deep Reinforcement Learning Approach," IEEE ICDM Workshop on Machine Learning for Cybersecurity (MLC), pp. 1313-1321.
7. Behnia R., Ebrahimi R. and Pacheco J., 2022. "EW-Tune: A Framework for Privately Fine-Tuning Large Language Models with Differential Privacy," IEEE ICDM Workshop on Machine Learning for Cybersecurity (MLC), pp. 560-566.
8. Hu J., Ebrahimi R., Li W., Li X. and Chen H., 2022, "Multi-view Representation Learning from Malware to Defend Against Adversarial Variants," IEEE ICDM Workshop on Multi-view

Representation Learning (MRL), pp. 1-8.

9. Ebrahimi R., Li W., Chai Y., Pacheco J., and Chen H., 2022, "An Adversarial Wargame Framework for Developing Robust Machine Learning-based Malware Detectors," IEEE ICDM Workshop on Machine Learning for Cybersecurity (MLC), pp. 567-576.
10. Ebrahimi R., Pacheco, J., Li, W., Hu, J., Chen, H., 2021, "Binary Black-Box Attacks Against Static Malware Detectors with Reinforcement Learning in Discrete Action Spaces," IEEE Symposium on Security and Privacy Workshop (S&PW) on Deep Learning and Security, pp. 85-91.
11. Liu Y., Lin F.Y., Ebrahimi R., Li W., Chen H., 2021, "Automated PII Extraction from Social Media for Raising Privacy Awareness: A Deep Transfer Learning Approach," IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1-6 **(Best Paper Award)**.
12. Ebrahimi R., Zhang, N., Hu, J., Raza M.T., Chen H, 2021, "Binary Black-box Evasion Attacks Against Deep Learning-based Static Malware Detectors with Adversarial Byte-Level Language Model," AAAI Workshop on Robust, Secure, and Efficient Machine Learning (RSEML).
13. Hu J., Ebrahimi R., Chen H., 2021, "Single-Shot Black-Box Adversarial Attacks Against Malware Detectors: A Causal Language Model Approach." IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1-6.
14. Ebrahimi R., Samtani S., Chai Y., Chen H., 2020, "Detecting Cyber Threats in Non-English Hacker Forums: An Adversarial Cross-Lingual Knowledge Transfer Approach," IEEE Symposium on Security and Privacy Workshop (S&PW) on Deep Learning and Security, pp. 20-26.
15. Ebrahimi R., Surdeanu M., Samtani S., Chen H., 2018, "Detecting Cyber Threats in Non-English Dark Net Markets: A Cross-Lingual Transfer Learning Approach," IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, 8-10 November, pp. 85-90 **(Best Paper Award Runner-up)**.
16. Ebrahimi R., Suen C.Y., Ormandjieva O., Krzyzak A., 2016, "Recognizing Predatory Chat Documents using Semi-supervised Anomaly Detection," 23rd Document Recognition Retrieval conference (DRR), pp. 1-9(9).
17. Du P., Ebrahimi R., Zhang N., Chen H., Brown R.A., Samtani, S., 2019, "Identifying High-Impact Opioid Products and Key Sellers in Dark Net Marketplaces: An Interpretable Text Analytics Approach," IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 110-115.
18. Arnold N., Ebrahimi R., Zhang N., Lazarine B., Patton M., Chen H., Samtani S., 2019, "Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool," IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 92-97.
19. Du P., Zhang N., Ebrahimi R., Samtani S., Lazarine B., Arnold N., Dunn R. et al. 2018, "Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs," IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 70-75.
20. Keyvanpour M., Javideh M., Ebrahimi R., 2011, "Detecting and Investigating Crime by Means of Data Mining: A General Crime Matching Framework," World Conference on Information Technology, Procedia Computer Science, Volume 3, Edited by AdemKarahoca, Sezer, pp. 872-880.

## BOOK CHAPTERS

1. Keyvanpour, M., Ebrahimi, R., Nayebi, N.G., Ormandjieva, O. And Suen, C.Y., 2016, "Automated Identification of Child Abuse in Chat Rooms by Using Data Mining," In Data Mining Trends and Applications in Criminal Science and Investigations, pp. 245-274, IGI Global Scientific Publishing.

## PATENTS

1. Ebrahimi R., Behnia R., Pacheco J., Padmanabhan B., 2023, "System and Method of Fine-Tuning Large Language Models Using Differential Privacy." Pending
2. Behnia R., Ebrahimi R., Padmanabhan B., Hoang T., 2024, "Systems and Methods for Secure Aggregation for Privacy-Preserving Federated Learning." Pending

## GRANT EXPERIENCE

1. **Title:** CyberAI Innovation: A Hands-on CyberAI Learning Platform for Malware Defense, **Funding Source:** NSF, **Requested Amount:** $500,000, **Role:** Co-PI, **Duration:** 2026-2029, **Status:** Under Review.
2. **Title:** Mechatronics Integrated into STEM Teaching: AI Meets Mechatronics Workshop, **Funding Source:** NSF (DUE), **Funding Amount:** $25,000, **Role:** Senior Personnel, **Duration:** 2026
3. **Title:** AI for Business Intelligence (AI4BI) in Taiwan Semiconductor Manufacturing Company (TSMC), **Funding Source:** TSMC, **Funding Amount:** $30,000. **Role:** Co-PI, **Duration:** 2024-2025.
    a. Co-mentored Two PhD students partially funded by the grant at University of Arizona and University of South Florida
4. **Title:** Fine-Tuning Large Language Models with Differential Privacy. **Funding Source:** USF Interdisciplinary Research Grant, **Funding Amount:** $20,000, **Role:** Co-PI, **Duration:** 2023-2024.
5. **Title:** Mechatronics Integrated into STEM Teaching for Transformative Inclusive Communities (MISTTIC), **Funding Source:** NSF, **Funding Amount:** $3,000,000, **Role:** Senior Personnel, **Duration:** 2024-2030.
6. **Title:** Cybersecurity Big Data and Analytics Sharing Platform, **Source:** NSF **(**SaTC-DGE), **Year:** 2019**, Grant No.:** 1719477**, Funded Amount:** $180,000**, Role:** Lead annual report writer.

## TEACHING EXPERIENCE

**Course Development**

1. Proposed and Developed ISM-7568, Deep Learning for Business Analytics for PhD students
2. Co-Developed ISM-6251: Data Science Programming and ISM-6251: Machine Learning

| Course | Semester | Level | Modality | Student Participation | TE Score |
|---|---|---|---|---|---|
| MIS331: Database Systems (UArizona) | Fall 2026 | Undergrad | In person | - | - |
| MIS331: Database Systems (UArizona) | Fall 2026 | Undergrad | In person | - | - |
| ISM-7568: Deep Learning for Business Analytics (USF) | Spring2026 | PhD | In person | 3/3 | 5.0/5.0 |
| ISM – 6251: Machine Learning (USF) | Spring2025 | Undergrad & Master's | In person | 17/18 | 4.88/5.0 |

| | | | | | |
|---|---|---|---|---|---|
| ISM- 7568: Deep Learning for Business Analytics (USF) | Spring2024 | PhD | In person | 6/6 | 5.0/5.0 |
| ISM – 6251: Machine Learning (USF) | Fall2024 | Master's | In person | 21/23 | 4.67/5.0 |
| ISM – 6251: Machine Learning (USF) | Fall2024 | Master's | In person | 34/36 | 4.79/5.0 |
| ISM- 7568: Deep Learning for Business Analytics (USF) | Spring2024 | PhD | In person | 6/6 | 5.0/5.0 |
| ISM-6136: Data Minning | Fall2023 | Master's | In person | 19/23 | 4.68/5.0 |
| ISM-6251: Data Science Programming (USF) | Fall2023 | Master's | In person | 44/45 | 4.53/5.0 |
| ISM-6136: Data Mining (USF) | Spring2023 | Master's | In person | 11/12 | 4.91/5.0 |
| ISM-6136: Data Mining (USF) | Fall2022 | Master's | In person | 40/46 | 4.83/5.0 |
| ISM-6136: Data Mining (USF) | Fall2022 | Master's | In person | 39/46 | 4.68/5.0 |
| ISM-7930: Deep Learning for Business Analytics (USF) | Spring2022 | Master's | Hybrid | 7/8 | 4.86/5.0 |
| ISM-6136: Data Mining (USF) | Spring22 | Master's | Hybrid | 28/30 | 4.86/5.0 |
| ISM-6136: Data Mining (USF) | Fall2021 | Master's | Hybrid | 40/44 | 4.72/5.0 |
| MIS-562: Cyber Threat Intelligence (UArizona) | Summer2020 | Master's | Online | 18/25 | 4.55/5.0 |
| MIS-562: Cyber Threat Intelligence (UArizona) | Summer2019 | Master's | Online | 21/21 | 4.23/5.0 |

## PROFESSIONAL SERVICES

**Editorial Roles:**

1. Associate Editor, International Conference on Information Systems (ICIS), Computational Design and Evaluation Track, 2026

**Workshop Chair:**

2. IEEE Security and Privacy (S&P) Workshop on Human-Machine Intelligence for Security Analytics (HMI-SA), 2025
3. IEEE ICDM Workshop on Machine Learning and Cybersecurity (MLC) 2022, 2023, 2024, 2025

**Program Committee:**

1. IEEE Security and Privacy (S&P) Workshop on Deep Learning and Security 2022, 2023, 2024
2. IEEE ICDM workshop on Deep Learning for Cyber Threat Intelligence (DL-CTI); 2020
3. Informs Data Science Workshop; 2021

**Journal Ad-hoc Reviewer (8 journals):**

1. PNAS, 2. MIS Quarterly, 3. Journal of Management Information Systems (JMIS), 4. IEEE Transactions on Dependable and Secure Computing (TDSC), 5. IEEE Transactions on Information Forensics and Security (TIFS), 6. ACM Transactions on Management Information Systems (TMIS), 7. International Journal of Electronic Commerce (IJEC), 8. Information Systems Frontiers

**PhD Student Co-Mentoring (8 students):**

1. James Hu (University of Arizona, 2019 - Present), 2. Yizhi (Louis) Liu (University of Maryland, 2023-2026), 3. Chi-Heng Yang (University of Arizona, 2023 - 2026), 4. Yiwei Zhang (Purdue University, 2024 - Present), 5. Arman Riasi (Virgina Tech, 2024 - Present), 6. Alysson De Oliveira (University of South Florida, 2023-Present), 7. Atousa Arzanipour (University of South Florida, 2025, Present), 8. Yanjing Ren (University of South Florida, 2026-Present)

## AWARDS & HONORS

- Rapid7-USF Cyber Threat Intelligence Lab Representative of Muma College of Business, 2026, $10,000
- Dean's Research Fund, 2026, $2,500
- Best Paper Award in WITS, 2025
- Best Paper Award in IEEE S&PW, 2024
- Invited Panelist in AMCIS, 2024
- IEEE Senior Member, 2024
- ACM SIGMIS Best Doctoral Dissertation Award at ICIS, 2021
- Best Reviewer Award in INFORMS Workshop on Data Science, 2021
- Best Paper Award in IEEE ISI, November 2021
- Best Reviewer Award, Informs Data Science Workshop, 2021
- LaSalle Teaching Excellence Award, 2021
- Selected for Doctoral Consortium of International Conference on Information Systems (ICIS), 2020
- Paul S. and Shirley Goodman Award, 2020

- IEEE S&P Student Travel and Registration Award for Deep Learning and Security Workshop, 2020
- Best Paper Award Runner-up in IEEE ISI, 2018
- Concordia University 25th Anniversary Fellowship – Engineering and Computer Science Department, January 2015 (Awarded based on academic excellence to a few students each year)
- Power Corporation of Canada Graduate Fellowship, 2015 (Awarded based on academic excellence to 5 students each year)
- Graduate Conference and Exposition Award, 2015
- Ranked 1st in RoboCup Iran Open International Competitions 2007, Middle Size Robots
- Ranked 1st university student in Fall 2007 and Spring 2008 with GPAs of 18.43/20.00 and 19.50/20.00, respectively

## INDUSTRY EXPERIENCE

**SAP Canada (Internship)** **2015**

- **Role:** Data & Software Engineer (Users behavior analysis for order management systems)
- **Address:** 999 Boulevard de Maisonneuve West Montreal, Quebec H3A 3L4 Canada.