Reza Ebrahimi

E-mail: ebrahimim@usf.edu

Lab Website: https://star-ailab.github.io

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

EDUCATION

- **Doctor of Philosophy (Ph.D.), The University of Arizona,** **2016 - 2021**
  Major: Management Information Systems
  Minor: Computational Linguistics
- **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
- **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

RESEARCH INTERESTS

- **AI-enabled Cybersecurity Analytics:** Security and Privacy of AI, Adversarially Robust AI Agents for Cybersecurity, Automatic Cyber Threat Detection, Cross-lingual Security Analytics
- **Machine Learning and AI:** Adversarial Machine Learning, Transfer Learning and Domain Adaptation, Cross-lingual Knowledge Transfer, Reinforcement Learning, Deep Learning
- **Business Intelligence and Analytics:** Social Media Analytics, Multilingual Product Review Analysis
- **Crime Data Mining:** Online Predator Identification in Social Media, Supervised Methods for Categorizing Behavior of Offenders in Crime Incidents

TEACHING

- **Machine Learning** (ISM 6251) – Undergraduate and Master's
- **Deep Learning for Business Analytics** (ISM 7568) – Ph.D. Seminar
- **Deep Learning** (ISM 6152) – Master's

JOURNAL PUBLICATIONS

- **Ebrahimi R.**, Chai Y., Li. W., Pacheco J., Chen H. RADAR: A Framework for Developing Adversarially Robust Cyber Defense AI Agents with Deep Reinforcement Learning, **MIS Quarterly, Forthcoming.**
- **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.
- Zhang, N., **Ebrahimi, M.**, 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.
- **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* (*MISQ*),** 46(2), pp. 1209-1226.
- 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.
- **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.
- **Ebrahimi R.**, Martinez J., 2019, "Involuntary Embarrassing Exposures in Online Social Networks: A Replication Study," ***AIS Transactions on Replication Research (TRR)***, 5(1), pp. 1-20.

- **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.
- 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.

REFEREED CONFERENCE PROCEEDINGS & WORKSHOPS

- Hossain, S., **Ebrahimi, M.**, Padmanabhan, B., El Naqa, I., Kuo, P.C., Beard, A. and 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.
- 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).
- 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).
- Hu, J.L., **Ebrahimi, M.**, 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).
- **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).
- **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 (S&P) Deep Learning and Security Workshop, May 2021, San Francisco.
- **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).
- 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.
- 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)
- **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 (S&P) Deep Learning and Security Workshop, May 2020, San Francisco.
- **Ebrahimi R.**, Surdeanu M., Samtani S., Chen H., 2018, "Detecting Cyber Threats in Non-English Dark Net Markets: A Cross-Lingual Transfer Learning Approach," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, 8-10 November, pp. 85-90. (Best Paper Award Runner-up)
- **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), San Francisco, CA, 14-18 February, pp. 1-9(9).

- 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," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, pp. 110-115.
- Arnold N., **Ebrahimi R.**, Zhang N., Lazarine B., Patton M., Chen H., Samtani S., 2019, "Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, pp. 92-97.
- 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," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, 8-10 November, pp. 70-75.
- Keyvanpour M., Javideh M., **Ebrahimi R.**, 2011, "Detecting and Investigating Crime by Means of Data Mining: A General Crime Matching Framework," 2010 World Conference on Information Technology, Procedia Computer Science, Volume 3, Edited by AdemKarahoca, Sezer, pp. 872-880.

GRANT & REPORT WRITING SKILLS

- **D-ISN** (Disrupting Operations of Illicit Supply Networks), **Title:** Disrupting Illicit Trafficking by Dissecting Geometry of Darkweb and Cryptocurrency Transactions, **Source:** National Science Foundation (NSF)**, Grant Period:** 2020-2023**, Status:** Under review**, Amount:** $349,896**, Role:** Assisting Grant writer.
- **SaTC** (Secure & trustworthy Cyberspace), **Title:** Cybersecurity Big Data Research for Hacker Communities: A Topic and Language Modeling Approach, **Source:** National Science Foundation (NSF)**, Grant Period:** 2019-2022**, Grant No.:** 1936370, **Status:** Funded**, Funded Amount:** $510,624**, Role:** Assisting Grant writer.
- **SaTC-DGE** (Secure & trustworthy Cyberspace - Division of graduate Education), **Title:** Cybersecurity Big Data and Analytics Sharing Platform, **Source:** National Science Foundation (NSF)**, Reporting Year:** 2019**, Grant No.:** 1719477, **Status:** Funded**, Funded Amount:** $180,000**, Role:** Assisting Report writer.

PROFESSIONAL SERVICES (REVIEWED JOURNALS & CONFERENCES)

Workshop Chair

- IEEE ICDM Workshop on Machine Learning and Cyberecurity (MLC) 2022 and 2023

Program Committee

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

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS); 2021
- Journal of Management Information Systems (JMIS); 2019, 2020
- ACM Transactions on Management Information Systems (TMIS); 2020
- International Journal of Electronic Commerce (IJEC); 2020
- Information Systems Frontiers; 2018, 2020

AWARDS & HONORS

- ACM SIGMIS Doctoral Dissertation Award, December 2021.

- Best Paper Award in IEEE ISI, November 2021 (Paper: Automated PII Extraction from Social Media for Raising Privacy Awareness: A Deep Transfer Learning Approach).
- 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, May 2020.
- Best Paper Award Runner-up in IEEE ISI, November 2018 (Paper: Detecting Cyber Threats in Non-English Dark Net Markets: A Cross-Lingual Transfer Learning Approach).
- 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, May 2015 (Awarded based on academic excellence to 5 students each year).
- Graduate Conference and Exposition Award, December 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.

WORK 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.