Mohammadreza (Reza) Ebrahimi

E-mail: ebrahimim@usf.edu

Personal Website: https://mohammadrezaebrahimi.github.io
USF School of Information Systems and Management, 12011 Sago Drive, Tampa, FL 33620

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:** 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

SELECTED JOURNAL PUBLICATIONS

- **M. Ebrahimi**, Y. Chai, S. Samtani, H. Chen, "Cross-Lingual Security Analytics: Cyber Threat Detection in the International Dark Web with Adversarial Deep Representation Learning," Forthcoming, ***MIS Quarterly* (*MISQ*).**
- B. Wen, P. Hu, **M. Ebrahimi**, H. Chen, "Key Factors Affecting User Adoption of Open-Access Data Repositories in Intelligence and Security Informatics: An Affordance Perspective," Forthcoming, ***ACM Transactions on Management Inforamtio Systems (TMIS).***
- **M. Ebrahimi**, J. F. Nunamaker Jr., H. Chen, 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.
- **M. Ebrahimi**, J.D. Martinez, 2019. "Involuntary Embarrassing Exposures in Online Social Networks: A Replication Study," ***AIS Transactions on Replication Research (TRR)***, Volume 5(1), p. 7.
- **M. Ebrahimi**, C. Y. Suen, O. Ormandjieva, 2016. "Detecting Predatory Conversations in Social Media by Deep Convolutional Neural Networks," *Journal of Digital Investigation*, Elsevier, Volume 18, pp. 33-49.
- M. Keyvanpour, **M. Ebrahimi**, M. Javideh, 2012. "Designing Efficient ANN Classifiers for Matching Burglaries from Dwelling Houses," **Applied Artificial Intelligence**, Taylor and Francis, Volume 26 (8), pp. 787-807.

REFEREED CONFERENCE PROCEEDINGS & WORKSHOPS (*: presenting author)

- ***M. Ebrahimi**, J. Pacheco, W. Li, J. Hu, H. Chen, 2021. "Binary Black-Box Attacks Against Static Malware Detectors with Reinforcement Learning in Discrete Action Spaces, **IEEE Symposium on**

Security and Privacy (IEEE S&P), accepted to Deep Learning and Security Workshop, May 2021, San Francisco.

- ***M. Ebrahimi**, N. Zhang, J. Hu, M.T Raza, H. Chen, 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).
- ***M. Ebrahimi**, S. Samtani, Y. Chai, H. Chen, 2020. "Detecting Cyber Threats in Non-English Hacker Forums: An Adversarial Cross-Lingual Knowledge Transfer Approach," **IEEE Symposium on Security and Privacy (IEEE S&P)**, Deep Learning and Security Workshop, May 2020, San Francisco.
- ***M. Ebrahimi,** M. Surdeanu, S. Samtani, H. Chen, 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, 2018, pp. 85-90, (Best Paper Award Runner-up).
- ***M. Ebrahimi,** C. Y. Suen, O. Ormandjieva, A. Krzyzak, 2016. "Recognizing Predatory Chat Documents using Semi-supervised Anomaly Detection," 23rd Document Recognition Retrieval Conference (DRR16), San Francisco, CA, 14-18 February, pp. 1-9(9).
- P. Du, **M. Ebrahimi**, N. Zhang, H. Chen, R. A. Brown and S. Samtani, 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, China, pp. 110-115.
- N. Arnold, **M. Ebrahimi**, N. Zhang, B. Lazarine, M. Patton, H. Chen, S. Samtani, 2019. "Dark-Net Ecosystem Cyber-Threat Intelligence (CTI) Tool," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, pp. 92-97.
- P. Du, N. Zhang, ***M. Ebrahimi**, S. Samtani, B. Lazarine, N. Arnold, R. Dunn 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.
- M. Keyvanpour, M. Javideh, **M. Ebrahimi**, 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.

CURRENT TEACHING

- **Data Mining** (ISM 6136) – Master's
- **Deep Learning for Business Analytics** (ISM 7561) – Ph.D.

PROFESSIONAL SERVICES (REVIEWED JOURNALS & CONFERENCES)

Referee

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

Program Committee

- IEEE ICDM workshop on Deep Learning for Cyber Threat Intelligence Workshop (DL-CTI); 2020
- Informs Data Sciene Workshop; 2021

AWARDS & HONORS

- Department Candidate for Doctoral Consortium, International Conference on Information Systems (ICIS), 2020.
- IEEE S&P Student Travel and Registration Award for Deep Learning and Security Workshop, May 2020.
- IEEE ISI 2018 Best Paper Award Runner-up, November 9, 2018 (First author of the paper titled: 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, Concordia University, December 2015.
- Team Ranked 1st in RoboCup Iran Open International Competitions 2007- Middle Size Robots.
- Ranked with the highest GPA among university students in fall 2007 and spring 2008 with GPA 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.