Rajvardhan Oak

University of California, Davis
1215 Dexter Avenue N, Seattle, WA 98109
+1 510-990-44086
rvoak@ucdavis.edu

PRINCIPAL INTERESTS

Cyber Security, Privacy, Adversarial Machine Learning, Fraud, Trust & Safety, Large-Scale Internet Measurement

ACADEMIC BACKGROUND

Ph.D., Computer Science Expected 2025
University of California Davis, Davis, CA

- Coursework: Computer Security, Health Informatics Security, Applied Data Analysis
- Research Focus: Fraudulent Review Detection, Privacy for At-Risk Population (advised by Zubair Shafiq)

M.S., Information Systems 2020
University of California Berkeley, Berkeley, CA

- Coursework: Privacy Engineering, Cyber Law, Public Interest Cybersecurity, Applied Machine Learning, Quantitative Research Methods, Big Data Analytics, Data Mining
- Research Focus: Malware Detection and Anomaly Detection (advised by Dawn Song)

B.E., Computer Engineering 2018
University of Pune MH, India

- Coursework: Data Structures, Algorithms, Computer Networks, Computer Architecture, Operating Systems, Databases

RESEARCH

Malware Detection with Transformers – *Advisor: Prof. Dawn Song*
Developed a BERT-based, transfer learning driven algorithm for malware detection with very few malware samples ($< 0.01\%$) and achieved high F-1 sores (> 0.92). This is an improvement of 35% over existing methods like LSTM under low-positive settings. Examined several pretraining configurations and discovered that pretraining on NLP data leads to optimal weights that results in faster convergence when fine-tuning on malware data.

Lifelong Anomaly Detection through Unlearning – *Advisor: Prof. Dawn Song*
Developed an *unlearning* framework that allows updaing an anomaly detection model without retraining. Designed a novel loss function that maximizes loss for known false positives and negatives. Examined the application of unlearning for three models: LSTM, Autoencoders and Regression showed that unlearning could reduce the false positives and negatives by as much as 75%. Benchmarked performance and demonstrated that unlearning could update the model in $< 2s$ as compared to retraining which took > 30 minutes.

Phishing Simulator – *Advisor: Prof. Steven Weber*
Developed a phishing simulation toolkit using open-source technology for non-profits to setup and analyze phishing campaigns for internal training. Researched effective

phishing strategies and leveraged deep fakes and large language models to craft efficient phishing emails. Created policies, instructional modules and quizzes for effective training.

Fault in the Stars – *Advisor: Prof. Zubair Shafiq*
Investigated the underground market of fraudulent amazon reviews by conducting qualitative studies with agents and buyers involved in fake reviews brokering. Crawled a dataset of 3000 products and audited the effectiveness of Amazon's detection mechanisms. Discovered evasion tactics employed by fraudsters to avoid detection, and three novel kinds of fraud within the fraudulent reviews ecosystem.

PUBLICATIONS

1. Poster – Towards Authorship Obfuscation with Language Models
   Rajvardhan Oak
   Proceedings of the *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2022.*
2. Poster – You are what you Pay: A Case Study in Venmo
   Rajvardhan Oak and Mrunmayee Khare
   Proceedings of the *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2022.*
3. Malware Detection on Highly Imbalanced Data through Sequence Modeling.
   Rajvardhan Oak, Min Du, David Yan, Harshvardhan Takawale, and Idan Amit.
   Proceedings of the *12th ACM Workshop on Artificial Intelligence and Security (AISec) 2019.*
4. Lifelong Anomaly Detection through Unlearning
   Min Du, Zhi Chen, Chang Liu, **Rajvardhan Oak**, and Dawn Song
   Proceedings of the *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2019.*
5. Time for a Background Check! Uncovering the Impact of Background Features on Deep Neural Networks
   Vikash Sehwag, **Rajvardhan Oak**, Mung Chiang, and Prateek Mittal
   Proceedings of the *International Conference on Machine Learning (ICML) Object Oriented Learning Workshop 2020*
6. Artificial Intelligence: Ethics in Practice
   Jessica Cussins Newman and **Rajvardhan Oak**.
   USENIX 2020 Login Magazine
7. Poster: Adversarial Examples for Hate Speech Classifiers
   Rajvardhan Oak
   Proceedings of the *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2019.*
8. Poster: Using Generative Adversarial Networks for Secure Pseudorandom Number Generations
   Rajvardhan Oak, Chaitanya Rahalkar, Dhaval Gujar
   Proceedings of the *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2019.*
9. A Literature Survey on Authentication using Behavioural Biometric Techniques.
   Rajvardhan Oak
   Proceedings of the *Springer Intelligent Computing and Information and Communication (ICIC) 2018*

10. A Novel Architecture for Continuous Authentication using Behavioural Biometrics **Rajvardhan Oak** and Mrunmayee Khare
Proceedings of the *IEEE International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), 2017.*
11. Real-Time Distributed Denial-of-Service (DDoS) Attack Detection using Decision Trees for Server Performance Maintenance
Mrunmayee Khare and **Rajvardhan Oak**
Springer Performance Management of Integrated Systems and its Applications in Software Engineering, 2020.
12. Smart Collaboration Mechanism using Blockchain Technology.
Rajvardhan Oak, Karanveer Singh Jhala and Mrunmayee Khare
Proceedings of the *5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* 2018.
13. Towards Developing a Secure and Robust Solution for E-Voting using Blockchain
Harsh Jain, **Rajvardhan Oak**, and Jay Bansal.
Proceedings of the *IEEE International Conference on Nascent Technologies in Engineering (ICNTE), 2019.*
14. Extractive Techniques for Automatic Document Summarization: A Survey.
Rajvardhan Oak
International Journal of Innovative Research in Computer and Communication Engineering Vol 4, Issue 3 (2016).
15. A Study of Digital Image Segmentation Techniques.
Rajvardhan Oak
International Journal of Engineering and Computer Science Vol. 5, Issue 12 (2016)
16. Phisherman's Net: A Tool For Understanding And Preventing Phishing Attacks
Rajvardhan Oak
Journal of Positive School Psychology Vol. 4, Issue 1 (2020)

SERVICE

Conference Program Committee & Peer Reviews

1. CVPR Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems and Online Challenges (AML-CV) - 2021
2. IEEE International Conference on Emerging trends and Innovations in ICT (ICEI) - 2022
3. Public Key Infrastructure and its Applications Conference (PKIA) - 2022
4. Mobile Human Computer Interaction (MobileHCI) - 2022
5. IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) - 2022
6. Future of Information and Communication Conference (FICC) - 2023
7. Humans and Cyber Security Workshop (HACS) - 2019

Journal & Book Peer Reviews

1. IEEE Security & Privacy (S&P) Magazine
2. Salesforce Data Architecture and Management Designer (Packt Publications)
3. Machine Learning Security Principals (Packt Publications)

Technical Symposia

1. Impetus and Concepts (INC) - 2020, 2021, 2022

2. San Francisco Hacks (SFHacks) Hackathon - 2021

AWARDS

- (ISC)^2 Global Achievement Award 2022 for Excellence in Cyber Security
- Berkeley International Office Award for Outstanding Graduate Student 2020

TALKS

- Invited Workshop on Phishing Simulation at the NSF Cyber Security Summit 2019
- Keynote on Adversarial Machine Learning at the NSF Cyber Security Summit 2019
- Invited Talk on AI Security Challenges for Developing Countries at NeurIPS 2020
- Invited Workshop on ML for Security at the NSF Cyber Security Summit 2022