KUNAL MUKHERJEE, Ph.D.

Dallas, TX, 75052 • kunmukh@gmail.com • kunmukh.com
Google Scholar • LinkedIn

EDUCATION

Ph.D. and M.S., Computer Science Aug 2019 – May 2025
University of Texas at Dallas, Richardson, TX, USA GPA: 3.89 / 4.00
Advisors: Dr. Kangkook Jee and Dr. Murat Kantarcıoğlu
Committee Members: Dr. Bhavani Thuraisingham and Dr. Feng Chen
Dissertation: *IoT integration, Adversarial attacks, and Threat explanations in Provenance-based Intrusion Detection Systems*

B.S., Computer Engineering Aug 2016 – Jun 2019
University of Evansville, Evansville, IN, USA GPA: 3.93 / 4.00
Advisor: Dr. Dick Blandford and Dr. Donald Roberts
Minors: Computer Science and Engineering Management
Senior Thesis: *Location Dependent Cryptosystem*

RESEARCH AND PROFESSIONAL EXPERIENCE

Applied Scientist Mar 2026 – Present
Zillow Group, Inc, Dallas, TX, USA

- Design personalized ranking and recommendation objectives for real estate discovery.
- Develop user–listing representation learning models using behavioral, contextual, and graph signals.
- Build explainable recommender systems for transparent and fair personalized home recommendations.
- Apply LLMs and multimodal AI to extract decision-relevant insights from listings and market context.

Postdoctoral Associate Aug 2025 – Mar 2026
Virginia Tech, Blacksburg, VA, USA

- Dr. Murat Kantarcıoğlu's Research Group.
- Investigate LLMs adoption in system provenance with focus on adversarial resistance.
- Implement realistic adversarial attacks on GNNs across domains (blockchain, social media).
- LLM-guided forensics and governance for trustworthy agentic AI in security-critical applications.

Applied Scientist Intern May 2024 – Aug 2024
Zillow Group, Inc, Dallas, TX, USA

- Resulted in an (oral) KDD'25 workshop paper and a patent application.
- Developed a GNN-based recommendation system to suggest new regions with similar listings.
- Developed an explainability framework to increase RecSys model transparency.
- GNN-based Recommendation System (RecSys) boosted relevancy (40×) and diversity (60×).

Lead Graduate Student Researcher Aug 2019 – May 2025
The University of Texas at Dallas, Richardson, TX, USA

- Dr. Kangkook Jee's Research Group, and conducted research in System, IoT, and CPS security.

Hardware Research Intern May 2017 – Jul 2019
Ciholas, Inc., Evansville, IN, USA

- Designed a proprietary sensor-fusion model for motion tracking by fusing accelerometer, gyroscope, and magnetometer.
- Implemented a 3D orientation visualization (low-latency, accurate, and gimbal-lock-free) engine and the model in production

PROFESSIONAL ACTIVITIES

Program Committee Member:

- ACM Conference on Computer and Communications Security (CCS), 2026
- USENIX Security Symposium, 2026
- Conference on Neural Information Processing Systems (NeurIPS), 2026
- International Conference on Machine Learning (ICML), 2026
- ACM Conference on Knowledge Discovery and Data Mining (SIGKDD), 2026
- International Conference on Machine Learning (ICML), 2026
- International Conference on Learning Representations (ICLR), 2025, 2026
- Workshop on Attack Provenance, Reasoning, and Investigation for Security in Monitored Environments (PRISM), co-located with NDSS, 2026
- Workshop on AI Discovery in the Wild (AID-Wild@CAIS'26), co-located with ACM Conference on AI and Agentic Systems (ACM CAIS), 2026
- Learning on Graphs (LoG), 2025

Reviewer:

- ACM Computing Surveys (CSUR)
- ACM Transactions on Privacy and Security (TOPS)
- IEEE Transactions on Information Forensics & Security (TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Computational Social Systems (TCSS)
- IEEE Transactions on Neural Networks and Learning Systems (TNNLS)

Artifact Evaluator:

- ACM Conference on Computer and Communications Security (CCS), 2025
- USENIX Security Symposium, 2024
- Network and Distributed System Security (NDSS), 2024
- Annual Conference on Machine Learning and Systems (MLSys), 2023
- ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2023

External Reviewer:

- USENIX Security Symposium, 2024, 2025
- ACM Conference on Computer and Communications Security (CCS), 2024
- Information Security Conference (ISC), 2023

TEACHING EXPERIENCE

Teaching Assistant

- Information Security: Spring-23, Spring-25
- Undergraduate Operating System Concepts: Fall-24
- System Security and Malicious Code Analysis: Spring-21, Spring-22
- Cybersecurity Attacks and Defenses Laboratory: Fall-21
- Graduate Operating System Concepts: Fall-19, Spring-20, Summer-20
- Object-Oriented Analysis and Design: Summer-20
- Organization of Programming Languages: Spring-20

STUDENT RESEARCH ADVISING

** Co-Author of peer-reviewed publications*

- Jonathan Yu*, B.S. CS, University of Texas at Dallas → American Airlines
- James Wei*, B.S. CS, University of Texas at Dallas → Sandia National Labs
- Alex Armstrong, B.S. CS, University of Texas at Dallas → Google
- Nick D. Baker, B.S. CS, University of Texas at Dallas → AWS
- Guangze Zu, B.S. CS, University of Texas at Dallas → Meta
- Rahul Muthyam, B.S. CS, University of Texas at Dallas → Amplitude
- Ahad Jawaid, B.S. CS, University of Texas at Dallas → Amazon (internship)

INVITED TALKS

Conference Talks

A1 International Conference on Machine Learning (ICML) '26 – *BOCLOAK: Optimal Transport-Guided Adversarial Attacks on Graph Neural Network-Based Bot Detection*

A2 ACM Conference on AI and Agentic Systems (ACM CAIS) '26 – *MoltGraph: A Longitudinal Temporal Graph Dataset of Moltbook for Coordinated-Agent Detection*

A3 KDD '25 (MLoG-GenAI Workshop) – *Z-REx: Human-Interpretable GNN Explanations for Real Estate Recommendations*

A4 International Conference on Applied Cryptography and Network Security (ACNS) '25 – *ProvDP: Differential Privacy for Provenance Dataset*

A5 International Conference on Applied Cryptography and Network Security (ACNS) '24 – *ProvIoT: Countering Attacks with Edge-Cloud Collaborative IoT Security*

A6 USENIX Security Symposium '23 – *Evading Provenance-Based ML Detectors with Adversarial System Actions*

Research Symposium

B1 Applied Machine Learning Conference '26 – Invited to present my talk on: *Human-Interpretable ML Explanations in High-Stakes Graph ML.*

B2 Commonwealth Cyber Initiative Symposium '26 – Invited to present paper in AI for Cyber/Cyber for AI track: *LLM-driven Provenance Forensics for Threat Investigation and Detection*

B3 Commonwealth Cyber Initiative Symposium '26 – Invited to present paper in AI for Cyber/Cyber for AI track: *Explaining Provenance-Based GNN Detectors with Interpretable Graph Structural Features*

B4 Virginia Tech '25 – Invited talk CS 5914: *LLM-driven Provenance Forensics for Threat Investigation and Detection*

B5 **University of Texas at Dallas '25** – Week of AI Research Showcase: *Intrusion Detection System Using AI Agents*

B6 **Zillow Group '24** – Research Showcase: *Enhancing Similar Regional Recommendations Using Graph Neural Networks and Providing User-Centric Explanation*

B7 **Virginia Tech '24** – Research Highlight: *Resilient and Explainable Graph Neural Networks: From Provenance to Personalization*

B8 **MIT '18** – IEEE URTC Lightning Talk: *Location Dependent Cryptography*

PATENTS

C1 **Explainable Graph Neural Network** (US #19/048,398) — Filed: Feb 07, 2025.

C2 **Subgraph Differential Privacy** — To be filed: May 2026.

C3 **Provenance Domain Lossless Graph-to-Tree Conversion** — To be filed: May 2026.

PUBLICATIONS

Conferences/workshops are primary venues in computer science.

Manuscripts (preprints/submissions)

D1 **Kunal Mukherjee** and Murat Kantarcioglu. "*ProvSEEK: LLM-driven Provenance Forensics for Threat Investigation and Detection*," submitted to Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS), 2026.

D2 **Kunal Mukherjee**. "*Red-Teaming Claude Opus and ChatGPT-based Security Advisors for Trusted Execution Environments*," submitted to AI Discovery in the Wild (AID-Wild@CAIS'26) Workshop at ACM Conference on AI and Agentic Systems (ACM CAIS), 2026.

D3 **Kunal Mukherjee**, Joshua Wiedemeier, Tianhao Wang, Muhyun Kim, Feng Chen, Murat Kantarcioglu, and Kangkook Jee. "*Explaining Provenance-Based GNN Detectors with Graph Structural Features*," submitted to the 23rd Annual International Conference on Privacy, Security, and Trust (PST), 2026.

D4 Tianhao Wang, Simon Klancher, **Kunal Mukherjee**, Josh Wiedemeier, Feng Chen, Murat Kantarcioglu, and Kangkook Jee. "*ProvCreator: Synthesizing Graph Data with Text Attributes*," submitted to arXiv, 2025.

Peer-reviewed Conference Publications

E1 **Kunal Mukherjee**, Zulfikar Alom, Tran Gia Bao Ngo, Cuneyt Gurcan Akcora, and Murat Kantarcioglu. "*BOCLOAK: Optimal Transport-Guided Adversarial Attacks on Graph Neural Network-Based Bot Detection*," International Conference on Machine Learning (ICML), July 2026.

E2 **Kunal Mukherjee**, Cuneyt Gurcan Akcora, and Murat Kantarcioglu. "*MoltGraph: A Longitudinal Temporal Graph Dataset of Moltbook for Coordinated-Agent Detection*," ACM Conference on AI and Agentic Systems (ACM CAIS), May 2026.

E3 **Kunal Mukherjee**, Jonathan Yu, Partha De, and Dinil Mon Divakaran. "*ProvDP: Differential Privacy for Provenance Dataset*," International Conference on Applied Cryptography and Network Security (ACNS), Jun 2025.

E4 **Kunal Mukherjee**, Joshua Wiedemeier, Qi Wang, Junpei Kamimura, John Junghwan Rhee, James Wei, Zhichun Li, Xiao Yu, Lu-An Tang, Jiaping Gui, and Kangkook Jee. "*ProvIoT: Countering Stealthy Attacks with Edge-Cloud Collaborative IoT Security*," International Conference on Applied Cryptography and Network Security (ACNS), Mar 2024.

E5 **Kunal Mukherjee**, Joshua Wiedemeier, Tianhao Wang, James Wei, Feng Chen, Muhyun

Kim, Murat Kantarcioglu, and Kangkook Jee. "*Evading Provenance-Based ML Detectors with Adversarial System Actions*," Proceedings of the USENIX Security Symposium, Aug 2023.

Peer-reviewed Workshop and Journal Publications

F1 **Kunal Mukherjee**, Zachary Harrison, and Saeid Balaneshin. "*Z-REx: Human-Interpretable GNN Explanations for Real Estate Recommendations*," (**oral**) ACM SIGKDD Conference on Knowledge Discovery and Data Mining Workshop on Machine Learning on Graphs in the Era of Generative AI (MLoG-GenAI@KDD), Aug 2025.

F2 **Kunal Mukherjee**. "*Location-Dependent Cryptosystem: Geographically Bounded Decryption via UWB Timing-Encoded Key Reconstruction*," International Journal of Computer Applications, 2026.

HONORS

Awards

- 3rd Place, University of Texas at Dallas HackReason Hackaton, Jan 2021
- Semi-Finalist, Big Idea Competition, Sept 2020
- 3rd Place, Emerging Technology Hackathon, Oct 2019
- 1st Place, Best Senior Undergraduate Project Poster (University of Evansville), May 2019.
- 2nd Place, Outstanding Senior Undergraduate Project (University of Evansville), May 2019.
- University of Evansville Cultural Engagement and International Services Outstanding International Achievement, Apr 2019.
- University of Evansville Leadership Academy Gold Service Medal, Apr 2018.
- Evansville High School Athletic Council Academic All City Team, Feb 2014.

Scholarships

- University of Texas at Dallas Graduate Research Scholarship, Aug 2019-May 2025.
- University of Michigan CSE Workshop Travel Scholarship, Oct 2018.
- University of Evansville International Student Scholarship, Aug 2016-May 2019.
- University of Evansville Excellence in Mathematics Scholarship, Apr 2016.
- IVY Tech Valedictorian, May 2016.
- Anna & Benjamin Bosse, May 2016.
- William N. Lindsey, Sr., May 2016.

MEMBERSHIP

- Phi Kappa Phi (since Sep 2020).
- IEEE Eta Kappa Nu (since Apr 2018).
- ACM (since May 2017).
- IEEE (since May 2017).
- Sigma Phi Epsilon (since Sep 2016).

MEDIA COVERAGE

Interpretable Real Estate Recommendations,
Data Skeptic Podcast, Sep 2025. [Youtube Episode].

Senior Computer Engineering Students Present at MIT Conference,
University of Evansville Press, Oct 2018. [Article].

Top of the class of 2016,
Courier & Press Evansville, Jun 2016. [Article].

Optimist OPTICS, Optimist Club of Evansville – Downtown, Apr 2016. [Article].

HACKATHONS

UTD Emerging Technology Hackathon Oct 2019
3rd Place (DJI Tello Drones) [DEVPOST LINK].
AI.FRED: multilingual age-restricted chatroom with a vision-transformer gatekeeper.

UTD Inst. for Innovation and Entrepreneurship Big Idea Competition Sep 2020
Semi-finalist [PREZI PPT].
EnFoodie: Match making between supply deficient food network and donors.

UTD Artificial Intelligence Society (AIS) HackReason Jan 2021
3rd Place ($250) [DEVPOST LINK].
RESTD: Commonsense reasoning engine for threat detection and patch recommendation using s(CASP) developed by Dr. Gopal Gupta's Lab.

SELECTED PROJECTS

RAG Pipeline: LLM-Powered Threat Intelligence Extraction and Correlation

- Designed a RAG pipeline using LLM-based agents to analyze threat reports, extract indicators of compromise (IOCs), and generate accurate SQL queries to probe system databases.
- Used chain-of-thought (CoT) and reasoning-action (reAct) prompting to improve contextual precision and contextual relevance by 34%.
- During forensic investigation, it achieves 22% higher precision and 29% higher recall than SOTA.
- Framework increases its token usage by only 1.42x and time required by 1.63x when the database size increases 50x making it optimal for large-scale deployment.
- Repository: [ProvSEEK]

Adversarial ML: Attacks on Graph Neural Networks in the Wild

- Designed and implemented realistic adversarial attacks on state-of-the-art bot detectors across social media domains (e.g., Twitter/X and Reddit).
- Built an optimal transport (OT) guided adversarial attack on node classification to achieve up to 80.13% higher attack success rates while using 99.80% less GPU memory under realistic real-world constraints.
- Repository: [BoCloak]

Adversarial ML: Adversarial System Action Generation for Intrusion Detectors

- Automated, data-driven framework generating realizable evasive attacks that bypass path- and graph-based Intrusion Detection Systems.
- Evaluated on two realistic APTs and 15k fileless malware; new attacks were detected 56% less often.
- Investigated three real-world advanced persistent threat (APT) scenarios by designing labs and experimenting to gain insights to develop detailed case studies.
- Repository: [ProvNinja]

Differential Privacy: Data Sharing for System Data with DP Guarantees

- Framework for inter-organization data sharing with ϵ subtree-DP privacy and minimal utility loss (0.03% $\downarrow$ F1).
- Deployed with real-world provenance data; validated privacy and downstream performance.
- Legal and Regulatory awareness proven by securing IRB approval to share system data between different labs.
- Repository: [ProvDP]

IoT Security: Privacy-Preserving Federated Intrusion Detection

- Novel host-based and edge-cloud collaborative IDS for IoT devices (97–99% accuracy across malware/APTs).
- Secure infrastructure for executing real malware/APT scenarios; IRB approval for cross-lab data sharing.
- Repository: [ProvIoT]

Explainable ML: GNN-based Intrusion Detector Explanations

- Introduced robust graph structural features and discriminative subgraphs; achieved 99% explanation fidelity.
- Case studies on three real-world malware datasets; contributed to DGL (heterogeneous graph support).
- DGL Merge Requests: [#5315, #5550, #5739]