IDENTIFYING INFORMATION:

NAME: Kantarcioglu, Murat

ORCID iD: https://orcid.org/0000-0001-9795-9063

POSITION TITLE: Professor and CCI Fellow

PRIMARY ORGANIZATION AND LOCATION: Virginia Tech, Blacksburg, Virginia, United States

Professional Preparation:

ORGANIZATION AND LOCATION	DEGREE (if applicable)	RECEIPT DATE	FIELD OF STUDY
Purdue University, West Lafayette, Indiana, United States	PHD	08/2005	Computer Science
Purdue University, West Lafayette, Indiana, United States	OTH	08/2005	Graduate Certificate in Statistics
Purdue University , West Lafayette, Indiana, United States	MS	06/2002	Computer Science
Middle East Technical University, Ankara, Not Applicable, N/A, Turkey	BS	06/2000	Computer Engineering
Middle East Technical University, Ankara, Not Applicable, N/A, Turkey	OTH	06/2000	Minor in Corporate Finance

Appointments and Positions

2024 - present Professor and CCI Fellow, Virginia Tech, Blacksburg, Virginia, United States

2024 - present Adjunct Professor, University of Texas at Dallas, Richardson, Virginia, United States

2021 - 2024 Ashbel Smith Professor of Computer Science, University of Texas at Dallas, Department of Computer Science, Richardson, Texas, United States

2020 - 2024 Visiting Scholar, UC Berkeley, Berkeley, California, United States

2015 - 2021 Professor of Computer Science, University of Texas at Dallas, Richardson, Texas, United States

2013 - 2026 Visiting Scholar/Associate, Harvard University, Data Privacy Lab, Cambridge, Massachusetts, United States

2012 - 2012 Visiting summer faculty, Air Force Research Lab (AFRL), Rome, New York, United States

2011 - 2015 Associate Professor of Computer Science with Tenure, University of Texas at Dallas, Richardson, Texas, United States

2011 - 2011 Visiting Summer Faculty, Air Force Research Lab (AFRL), Rome, New York, United States

2005 - 2011	Assistant Professor of Computer Science , University of Texas at Dallas, Richardson, Texas, United States
2004 - 2004	Research Intern, IBM Almaden Research Labs , San Jose, California, United States
2003 - 2003	Research Intern, NEC C&C Research Labs, Cupertino, California, United States
2002 - 2002	Research Intern, NEC C&C Research Lab, Cupertino, California, United States
2001 - 2005	Research Assistant, Purdue University, Department of Computer Sciences, West Lafayette, Indiana, United States

Products

Products Most Closely Related to the Proposed Project

1. Mukherjee K, Wiedemeier J, Wang T, Wei J, Chen F, Kim M, Kantarcioglu M, Jee K. Evading Provenance-Based ML Detectors with Adversarial System Actions.. Usenix Security; 2023; c2023. Available from: https://www.usenix.org/conference/usenixsecurity23/presentation/mukherjee
2. Alom Z, Ngo T, Kantarcioglu M, Akcora C. GOttack: Universal Adversarial Attacks on Graph Neural Networks via Graph Orbits Learning.. ICLR; 2025; c2025. Available from: https://openreview.net/forum?id=YbURbViE7l
3. Akcora C, Li Y, Gel Y, Kantarcioglu M. BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain.. IJCAI; 2020; c2020. Available from: https://doi.org/10.24963/ijcai.2020/612 DOI: 10.24963/IJCAI.2020/612
4. Azad P, Coskunuzer B, Kantarcioglu M, Akcora C. Chainlet Orbits: Topological Address Embedding for Blockchain.. ACM KDD; 2025; c2025. Available from: https://doi.org/10.1145/3690624.3709322 DOI: 10.1145/3690624.3709322
5. Shamsi K, Victor F, Kantarcioglu M, Gel Y, Akcora C. Chartalist: Labeled Graph Datasets for UTXO and Account-based Blockchains.. NeurIPS; 2022; c2022. Available from: http://papers.nips.cc/paper_files/paper/2022/hash/e245189a86310b6667ac633dbb922d50-Abstract-Datasets_and_Benchmarks.html

Other Significant Products, Whether or Not Related to the Proposed Project

1. Chang I, Sotiraki K, Chen W, Kantarcioglu M, Popa R. HOLMES: Efficient Distribution Testing for Secure Collaborative Learning.. Usenix Security; 2023; c2023. Available from: https://www.usenix.org/conference/usenixsecurity23/presentation/chang
2. Rao F, Cao J, Bertino E, Kantarcioglu M. Hybrid Private Record Linkage: Separating Differentially Private Synopses from Matching Records. ACM Trans. Priv. Secur.. 2019; 22(3):15:1-15:36. Available from: https://doi.org/10.1145/3318462 DOI: 10.1145/3318462
3. Alufaisan Y, Kantarcioglu M, Zhou Y. Robust Transparency Against Model Inversion Attacks. IEEE Trans Dependable Secure Comput. 2021 Sep-Oct;18(5):2061-2073. PubMed Central PMCID: PMC8942105.
4. Shaon F, Kantarcioglu M, Lin Z, Khan L. SGX-BigMatrix: A Practical Encrypted Data Analytic Framework With Trusted Processors.. ACM CCS; 2017; c2017. Available from: https://doi.org/10.1145/3133956.3134095 DOI: 10.1145/3133956.3134095

5. Özdayi M, Kantarcioglu M, Gel Y. Defending against Backdoors in Federated Learning with Robust Learning Rate.. AAAI; 2021; c2021. Available from: https://doi.org/10.1609/aaai.v35i10.17118 DOI: 10.1609/AAAI.V35I10.17118

Certification:

I certify that the information provided is current, accurate, and complete. This includes, but is not limited to, information related to current, pending, and other support (both foreign and domestic) as defined in 42 U.S.C. § 6605.

In accordance with Section 10632 of the CHIPS and Science Act of 2022 (42 U.S.C. § 19232), each individual identified as a senior/key person must certify that they are not a party to a malign foreign talent recruitment program.

Research Security Training Requirement for Federal Award Personnel: In accordance with Section 10634 of the CHIPS and Science Act of 2022 (42 U.S.C. § 19234), each individual identified as a senior/key person must certify that they have completed the requisite research security training that meets the requirements specified in Item 2 of Important Notice No. 149 within 12 months prior to proposal submission.

Certified by Kantarcioglu, Murat in SciENcv on 2026-06-16 18:11:21