Venkata Swamy 'Kalyan' Nakka

Contact Information

Phone: +1 361-516-7796
E-mail: kalyan@tamu.edu
Webpage: https://kalyan-nakka.github.io/
LinkedIn Google Scholar

Research Interests

Deep Learning; Adversarial Machine Learning; AI/ML Security.

Education

Texas A&M University
Doctor of Philosophy (PhD) in Computer Science — 01/2024 – 05/2027

Texas A&M University – Kingsville
Master of Science (MS) in Computer Science — 08/2021 – 05/2023

Indian Institute of Technology – Dhanbad
Bachelor of Technology (BTech) in Mechanical Engineering — 07/2012 – 04/2016

Academic & Professional Experience

Texas A&M University
Graduate Assistant – Research — 01/2024 – Present

Texas A&M University–Kingsville
Graduate Research Assistant — 08/2022 – 05/2023
Graduate Teaching Assistant — 01/2022 – 07/2022

Soroco, India
Senior Software Engineer — 09/2019 – 07/2021

Infosys, India
Senior Software Engineer — 11/2018 – 08/2019
Software Engineer — 11/2016 – 10/2018

Research Projects

SPIES Research Lab, TAMU — 01/2024 – Present
Security of Emerging Artificial Intelligence Systems

CPPES Lab, TAMUK — 08/2022 – 05/2023
Blockchain-based Cybersecurity for Photovoltaic Systems

CPPES Lab, TAMUK — 08/2022 – 05/2023
Resilient Cyber-Physical Security for Next-Generation Distributed Energy Resources at Grid Edge

WiSeMAN Research Lab, TAMUK — 08/2022 – 05/2023
Development of Fault-tolerant and Energy-efficient WirelessSensor Networks

Technical Expertise

Programming Languages: Python, Kotlin, Java, SQL, Go
Platforms/Tools: Linux, Windows, Visual Studio Code, Android Studio, PyCharm
Machine Learning: TensorFlow, Jupyter, PyTorch

Teaching Experience

Guest Lectures
Quantum Threat to Current Cyber-Security, TAMUK — Spring 2023

Teaching Assistant

Massive Parallel Computing, TAMUK — Summer 2022
Foundations of Computer Science, TAMUK — Spring 2022

Invited Talks

TAMUK Graduate Science and Engineering Research Colloquium Series — 2023
SunSpec Alliance 2022 Annual Meeting — 2022

Honors & Achievements

Distinguished Student Award — 2023
Awarded to only 1 graduate student per semester at TAMUK (University level)

Dean's Merit Scholarship for exceptional academic performance — 2022
Awarded to top 2% of Engineering graduate students at TAMUK (College level)

Computer Science Graduate Scholarship for exceptional academic performance — 2021
Awarded to top 5% of CS Graduate students at TAMUK (Department level)

Rockwell International Scholarship for exceptional academic performance — 2021
Awarded to top 2% of International graduate students at TAMUK (Department level)

Insta Award — 2018
Infosys, India

IIT MCM Scholarship for exceptional academic performance — 2013 – 2016
Awarded to top 20% of Undergraduate students at IIT Dhanbad (University level)

All India Rank 10760 (98.2 %ile) — 2012
Indian Institute of Technology Joint Entrance Examination (IIT-JEE)
Entrance exam for IISc & IITs

All India Rank 8076 (99.2 %ile) — 2012
All India Engineering Entrance Examination (AIEEE)
Entrance exam for NITs

Fellowships

TAMU Graduate Research Assistantship (US $12,000 p.a.)	2024 – 2024
Graduate Research Assistant Scholarship (US $6,000 p.a.)	2022 – 2023
Dean's Merit Scholarship (US $1,000 p.a.)	2022 – 2023
TAMUK In-State Scholarship (US $8,500 p.a.)	2021 – 2023
HEERF III Student Scholarship (US $1,600 p.a.)	2021 – 2022
Computer Science Graduate Scholarship (US $1,000 p.a.)	2021 – 2022
Rockwell International Scholarship (US $1,000 p.a.)	2021 – 2022
IIT MCM Scholarship (IND ₹72,000 p.a.)	2013 – 2016

Publications

Preprints

[1] Is On-Device AI Broken and Exploitable? Assessing the Trust and Ethics in Small Language Models
Kalyan Nakka, Jimmy Dani, Nitesh Saxena

[2] Breaking Indistinguishability with Transfer Learning: A First Look at SPECK32/64 Lightweight Block Ciphers
Jimmy Dani, **Kalyan Nakka**, Nitesh Saxena

Articles in Peer-Reviewed Conference Proceedings

[1] Field demonstration of Blockchain-based security for a Solar Farm
BoHyun Ahn, **Kalyan Nakka**, Taesic Kim
ECCE – IEEE Energy Conversion Congress and Exposition, 2024

[2] Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks
Kalyan Nakka, Seerin Ahmad, Logan Atkinson, Taesic Kim, Habib M. Ammari
ISGT – IEEE PES Innovative Smart Grid Technologies, 2024

[3] Square Tessellation for Stochastic Connected *k*-Coverage in Planar Wireless Sensor Networks
Kalyan Nakka, Habib M. Ammari
ISCC – IEEE Symposium on Computers and Communications, 2023

Articles in Peer-Reviewed Journals

[1] Enhancing Photovoltaic System Security using Blockchain and Security Module
BoHyun Ahn, **Kalyan Nakka**, Taesic Kim, Jinchun Choi, Seerin Ahmad, Alan Mantooth
IEEE OJPEL – IEEE Open Journal of Power Electronics (submitted)

[2] Blockchain-assisted Resilient Control for Distributed Energy Resource Management Systems
Seerin Ahmad, **Kalyan Nakka**, BoHyun Ahn, Taesic Kim, Dongjun Han, Dongjun Won
IEEE TIE – IEEE Transactions on Industrial Electronics (submitted)

[3] An Energy-Efficient Irregular Hexagonal Tessellation-based Approach for Connected *k*-Coverage in Planar Wireless Sensor Networks
Kalyan Nakka, Habib M. Ammari
AdHoc – Elsevier's Ad Hoc Networks, 2024

[4] *k*-CSqu: Ensuring connected *k*-coverage using Cusp Squares of Square Tessellation
Kalyan Nakka, Habib M. Ammari
JPDC – Elsevier's Journal of Parallel and Distributed Computing, 2023

Service

Reviewer

ACM Transactions on Privacy and Security (TOPS)	2024
IEEE Energy Conversion Conference and Exposition (ECCE)	2024

Sub-Reviewer

Annual Computer Security Applications Conference (ACSAC)	2024
IEEE International Conference on Distributed Computing Systems (ICDCS)	2024

Student Mentoring

Ausmit Mondal, Undergraduate Student, Texas A&M University	2024

References

Dr. Nitesh Saxena, Texas A&M University	Email: nsaxena@tamu.edu
Dr. Taesic Kim, University of Missouri	Email: tkx96@missouri.edu
Dr. Habib M. Ammari, Texas A&M International University	Email: habib.ammari@tamiu.edu