Venkata Swamy 'Kalyan' Nakka

PhD Student, SPIES Research Lab
Department of Computer Science & Engineering
Texas A&M University, College Station, TX 77843

Phone: 361-516-7796
Email: kalyan@tamu.edu
Website: kalyan-nakka.github.io

RESEARCH INTERESTS

Adversarial Machine Learning, AI/ML Security, and Deep Learning.

EDUCATION

Texas A&M University — Jan. 2024 – May 2027 *(expected)*
PhD in Computer Science
Advisor: Dr. Nitesh Saxena

Texas A&M University–Kingsville — Aug. 2021 – May 2023
MS in Computer Science
Advisor: Dr. Habib M. Ammari

Indian Institute of Technology – Dhanbad, India — Jul. 2012 – Apr. 2016
BTech in Mechanical Engineering
Advisor: Dr. L. A. Kumaraswamidhas

ACADEMIC & PROFESSIONAL EXPERIENCE

Texas A&M University
Graduate Assistant – Research — Jan. 2024 – Present

Texas A&M University–Kingsville
Graduate Research Assistant — Aug. 2022 – May 2023
Graduate Teaching Assistant — Jan. 2022 – Jul. 2022

Soroco, India
Senior Software Engineer — Sep. 2019 – Jul. 2021

Infosys, India
Senior Software Engineer — Nov. 2018 – Aug. 2019
Software Engineer — Nov. 2016 – Dec. 2018

HONORS & ACHIEVEMENTS

Distinguished Student Award — 2023
Awarded to only 1 graduate student per semester at Texas A&M University–Kingsville (University level)

Dean's Merit Scholarship for exceptional academic performance — 2022
Awarded to top 2% of Engineering graduate students at Texas A&M University–Kingsville (College level)

Computer Science Graduate Scholarship for exceptional academic performance — 2021
Awarded to top 5% of CS Graduate students at Texas A&M University–Kingsville (Department level)

Rockwell International Scholarship for exceptional academic performance 2021
Awarded to top 2% of International graduate students at Texas A&M University–Kingsville (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

PUBLICATIONS

Peer-Reviewed Conference Papers

[C3] Field demonstration of Blockchain-based security for a Solar Farm
BoHyun Ahn, **Kalyan Nakka**, Nathanial Handke, Trevor Reyna, Taesic Kim
ECCE – IEEE Energy Conversion Congress and Exposition, 2024

[C2] 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

[C1] 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

Peer-Reviewed Journal Articles

[J4] Hierarchical Deployment and Square Tessellation for Connected *k*-Coverage in Heterogeneous Planar Wireless Sensor Networks
Kalyan Nakka, Habib M. Ammari
ACM TOSN – ACM Transactions on Sensor Networks, 2025

[J3] Blockchain-assisted Resilient Control for Distributed Energy Resource Management Systems
Seerin Ahmad, **Kalyan Nakka**, BoHyun Ahn, Taesic Kim, Dongjun Han, Dongjun Won
ACCESS – IEEE Access, 2024

[J2] An Energy-Efficient Irregular Hexagonal Tessellation-based Approach for Connected *k*-Coverage in Planar Wireless Sensor Networks
Kalyan Nakka, Habib M. Ammari
ADHN – Ad Hoc Networks, 2024

[J1] *k*-CSqu: Ensuring connected *k*-coverage using Cusp Squares of Square Tessellation
Kalyan Nakka, Habib M. Ammari
JPDC – Journal of Parallel and Distributed Computing, 2023

Preprints

[P2] Is On-Device AI Broken and Exploitable? Assessing the Trust and Ethics in Small Language Models
Kalyan Nakka, Jimmy Dani, Nitesh Saxena

[P1] Breaking Indistinguishability with Transfer Learning: A First Look at SPECK32/64 Lightweight Block Ciphers
Jimmy Dani, **Kalyan Nakka**, Nitesh Saxena

RESEARCH EXPERIENCE

SPIES Research Lab, Texas A&M University Jan. 2024 – Present

- ***Security Risks and Vulnerabilities in On-Device Small Language Models*:**
  In this study, we exploited well-established trust and ethics assessments for understanding the risks and vulnerabilities in on-device Small Language Models (SLMs) deployed on smartphones. The results illustrated the significant high risks of stereotypical bias, unfairness, privacy-breaching behavior and harmful response generation of on-device SLMs. Further, we demonstrated the vulnerabilities of these on-device SLMs using vanilla prompts depicting various harmful scenarios.

CPPES Lab, Texas A&M University–Kingsville Aug. 2022 – May 2023

- ***Blockchain-based Cybersecurity for Photovoltaic Systems:***
  We designed a Blockchain-based Cybersecurity platform for securing Photovoltaic systems against control-command and firmware-update attacks from adversaries, and developed a testbed for demonstrating defense against various real-time attack scenarios.
- ***Post Quantum Cryptography (PQC) grade Distributed Energy Resources Networks:***
  Our study designed a Post Quantum Cryptography (PQC) grade IEEE 2030.5 network architecture for Distributed Energy Resources (DERs), and developed a testbed for understanding the performance of various PQC cipher suites. Also, we demonstrated real-time monitoring and control of DERs using our proposed PQC-grade IEEE 2030.5 network.
- ***Blockchain-assisted Resilient Control for Distributed Energy Resouce Management Systems:***
  In this study, we designed a Blockchain-based resilient control mechanism for DER Management Systems (DERMS), such that monitoring and control of DERs will be not affected by failure of DERMS. We developed a testbed for demonstrating the effectiveness of our proposed resilient control mechanism for real-time voltage and frequency control recovery scenarios.

WiSeMAN Research Lab, Texas A&M University–Kingsville Aug. 2022 – May 2023

- ***Development of fault-tolerant and energy-efficient 2D Wireless Sensor Networks using Square Tessellation:***
  We designed a Square Tessellation-based connected *k*-coverage theory and developed centralized protocols *k*-CSqu (deterministic), St-*k*-CSqu (stochastic) and Het-*k*-CSqu (heterogeneous) for 2D Wireless Sensor Networks, that ensures fault-tolerant coverage and energy-efficient network operation.
- ***Development of fault-tolerant and energy-efficient 2D Wireless Sensor Networks using Irregular Hexagonal Tessellation:***
  In this study, we designed an Irregular Hexagonal Tessellation-based connected *k*-coverage theory and developed centralized protocols *k*-InDi (deterministic) and St-*k*-InDi (stochastic) for 2D Wireless Sensor Networks, that ensures fault-tolerant coverage and energy-efficient network operation.

- ***Development of fault-tolerant and energy-efficient 3D Wireless Sensor Networks using Cubic Honeycomb:***
  This work designs a Cubic Honeycomb-based connected *k*-coverage theory and develops centralized protocol 3D-*k*-CuHon for 3D Wireless Sensor Networks, that ensures fault-tolerant coverage and energy-efficient network operation.

TEACHING EXPERIENCE

Guest Lecture, Texas A&M University–Kingsville
- CSEN 5303: Industrial Control Systems Security — Spring 2023

Teaching Assistant, Texas A&M University–Kingsville
- CSEN 5303: Massive Parallel Computing — Summer 2022
- CSEN 5303: Foundations of Computer Science — Spring 2022

INVITED TALKS

Can Geometry Solve Complex Computer Science Problems? — Feb. 2023
Graduate Science and Engineering Research Colloquium Series
Texas A&M University–Kingsville, TX

Potential Quantum Computing Attacks on Distributed Energy Resources and Post-Quantum Cryptography grade IEEE 2030.5 — Dec. 2022
SunSpec Alliance Annual Meeting (Virtual)
Las Vegas, NV

FELLOWSHIPS

Graduate Research Assistantship (US $12,000 p.a.) — 2024–2025
Texas A&M University

Graduate Research Assistant Scholarship (US $6,000 p.a.) — 2022–2023
Texas A&M University–Kingsville

Dean's Merit Scholarship (US $1,000 p.a.) — 2022–2023
Texas A&M University–Kingsville

Graduate Assistant Scholarship (US $8,500 p.a.) — 2021–2023
Texas A&M University–Kingsville

HEERF III Student Scholarship (US $1,600 p.a.) — 2021–2022
Texas A&M University–Kingsville

Computer Science Graduate Scholarship (US $1,000 p.a.) — 2021–2022
Texas A&M University–Kingsville

Rockwell International Scholarship (US $1,000 p.a.) — 2021–2022
Texas A&M University–Kingsville

MCM Scholarship (IND ₹72,000 p.a.) — 2013–2016
Indian Institute of Technology – Dhanbad

SERVICES

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
ACM Conference on Computer and Communications Security (CCS)	2025

Student Mentoring

Ausmit Mondal, Undergraduate Student, Texas A&M University	2024–2025

REFERENCES

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