

Venkata Swamy 'Kalyan' Nakka

2nd year PhD Student, SPIES Research Lab

Department of CSE, Texas A&M University, College Station, TX 77843

✉ kalyan@tamu.edu | ☎ 361-516-7796 | 🌐 kalyan-nakka.github.io | 💼 linkedin.com/in/kalyan-nakka

Research Interests

Adversarial Machine Learning and AI Security.

Education

Texas A&M University , College Station, TX, United States. <i>Doctor of Philosophy (Ph.D.) in Computer Science</i> , GPA: 4.0/4.0	Jan. 2024 – May 2027
Texas A&M University–Kingsville , Kingsville, TX, United States. <i>Master of Science (M.S.) in Computer Science</i> , GPA: 4.0/4.0 [Distinction]	Aug. 2021 – May 2023
Indian Institute of Technology (IIT) – Dhanbad , India. <i>Bachelor of Technology (B.Tech.) in Mechanical Engineering</i> , GPA: 7.73/10.0 [First Class]	Jul. 2012 – Apr. 2016

Academic & Professional Experience

Graduate Assistant – Research , <i>Texas A&M University</i> , TX, United States. <ul style="list-style-type: none">• Demonstrated risks and vulnerabilities associated with on-device <i>Small Language Models</i>, in comparison with their on-server counterparts.• Developed practically deployable on-device guardrails for securing and safeguarding <i>Small Language Models</i>, against <i>Open Knowledge Attacks</i> (a novel threat).• Developed novel Black-box Jailbreak Attack on safety aligned <i>Large Language Models</i>, that exploits Bitstream Camouflage vulnerability.	Jan. 2024 – Present
Graduate Research Assistant , <i>Texas A&M University–Kingsville</i> , TX, United States. <ul style="list-style-type: none">• Developed <i>Blockchain</i>-based security and control platforms for Distributed Energy Resources and Smart Inverters.• Developed <i>Quantum-secure IEEE 2030.5 Network</i> for Distributed Energy Resources.• Developed protocols for achieving fault-tolerant and energy-efficient coverage in <i>Wireless Sensor Networks</i>, leveraging Square and Irregular Hexagonal Tessellations.	Aug. 2022 – May 2023
Graduate Teaching Assistant , <i>Texas A&M University–Kingsville</i> , TX, United States. <ul style="list-style-type: none">• Managed academic activities for <i>Massive Parallel Computing</i> and <i>Foundations of Computer Science</i> courses, including assignments and exams grading, supporting 90+ graduate students.• Evaluated group projects for <i>Foundations of Computer Science</i> course, delivering constructive feedback on algorithmic design, course project deliverables and practical implementations to enhance student learning outcomes.	Jan. 2022 – Jul. 2022
Senior Software Engineer , <i>Soroco Limited</i> , Bangalore, India. <ul style="list-style-type: none">• Coordinated 5+ teams of engineers on projects for development of Python-based Automation Systems and their components, achieving over 90+% project success rate.• Improved efficiency by 20% for Automation System of Fortune 200 insurance company, that currently saves 960 full-time equivalents (FTE) per month and \$325,000 of annual operational cost.• Engineered Automation Systems for Fortune 500 pharmaceutical company, where one saves 10,000+ FTEs of repetitive work and another one saves 5,000+ FTEs of manual repetitive activities and \$120,000 of operational cost.• Enhanced Automation Systems for utilizing AWS services like RDS and Secrets, for achieving 100% data storage and management to cloud.	Sep. 2019 – Jul. 2021
Senior Software Engineer , <i>Infosys Limited</i> , Bangalore, India. <ul style="list-style-type: none">• Mentored 2 teams of engineers on projects for Windows computer software, accessed by 6,000+ client employees for business case processing and achieved over 95% of project expectations.• Integrated legacy Windows-based computer software with Web-based REST API using C#, saving over 70% time of document generation.• Facilitated the transition of over 90+% databases by leveraging strategic design and planning principles.	Nov. 2018 – Aug. 2019
Software Engineer , <i>Infosys Limited</i> , Bangalore, India. <ul style="list-style-type: none">• Developed various Windows computer software, accessed by 6,000+ employees for over 85+% of business case processing.• Programmed various features as additions to legacy computer software, saving 2 FTEs per business case and \$20,000 of operational cost.	Nov. 2016 – Oct. 2018

Honors & Achievements

Distinguished Student Award (2023) – Awarded to top graduate student (only 1) across the university
Dean's Merit Scholarship (2022) – Recognized among top 2% of engineering graduate students for academic excellence
Computer Science Graduate Scholarship (2021) – Merit based scholarship for top 5% of CS graduate students
Rockwell International Scholarship (2021) – Awarded to academically top 2% of international graduate students
Insta Award (2018) – Corporate recognition for outstanding project delivery and performance excellence at Infosys
IIT MCM Scholarship (2013-2016) – Merit-based scholarship for top 20% of undergraduate students across the university
All India Rank 10760 in IIT-JEE (2012) – Nationwide top 2 % in entrance exam for IISc & IITs
All India Rank 8076 in AIEEE (2012) – Nationwide top 1% in entrance exam for NITs

Publications

Peer-Reviewed Conference/Workshop Papers

- **[IJCNLP-AACL 2025]** Kalyan Nakka, Jimmy Dani, Ausmit Mondal, and Nitesh Saxena. “*LiteLMGuard: Seamless and Lightweight On-Device Guardrails for Small Language Models against Quantization Vulnerabilities*”, In Findings of the Association for Computational Linguistics: IJCNLP-AACL.
- **[STWiMob 2025]** Kalyan Nakka and Habib M. Ammari. “*Stochastic Connected k-Coverage in Planar Wireless Sensor Networks Using Optimal Hexagonal Tessellation*”, In IEEE International Workshop on Selected Topics in Wireless and Mobile computing (STWiMob).
- **[PST 2025]** Jimmy Dani, Kalyan Nakka, and Nitesh Saxena. “*A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of Lightweight Block Ciphers*”, In Annual International Conference on Privacy, Security & Trust (PST).
- **[ECCE 2024]** BoHyun Ahn, Kalyan Nakka, Nathaniel Handke, Trevor Reyna, and Taesic Kim. “*Field demonstration of Blockchain-based security for a Solar Farm*”, In IEEE Energy Conversion Conference and Expo (ECCE).
- **[ISGT 2024]** Kalyan Nakka, Seerin Ahmad, Logan Atkinson, Taesic Kim, and Habib M. Ammari. “*Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks*”, In IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT).
- **[ISCC 2023]** Kalyan Nakka and Habib M. Ammari. “*Square Tessellation for Stochastic Connected k-Coverage in Planar Wireless Sensor Networks*”, In IEEE Symposium on Computers and Communications (ISCC).

Peer-Reviewed Journal Articles

- **[ACM TOSN]** Kalyan Nakka and Habib M. Ammari. “*Hierarchical Deployment and Square Tessellation for Connected k-Coverage in Heterogeneous Planar Wireless Sensor Networks*”, In ACM Transactions on Sensor Networks (TOSN), 21(2), 2025.
- **[IEEE ACCESS]** Seerin Ahmad, Kalyan Nakka, BoHyun Ahn, Taesic Kim, Dongjun Han, and Dongjun Won. “*Blockchain-assisted Resilient Control for Distributed Energy Resource Management Systems*”, In IEEE Access, 2024.
- **[ADHN]** Kalyan Nakka and Habib M. Ammari. “*An Energy-Efficient Irregular Hexagonal Tessellation-based Approach for Connected k-Coverage in Planar Wireless Sensor Networks*”, In Ad Hoc Networks (ADHN), 154, 2024.
- **[JPDC]** Kalyan Nakka and Habib M. Ammari. “*k-CSqu: Ensuring connected k-coverage using Cusp Squares of Square Tessellation*”, In Journal of Parallel and Distributed Computing (JPDC), 182, 2023.

Preprints

- **[arXiv]** Kalyan Nakka and Nitesh Saxena. “*BitBypass: A New Direction in Jailbreaking Aligned Large Language Models with Bitstream Camouflage*”.
- **[arXiv]** Kalyan Nakka, Jimmy Dani, and Nitesh Saxena. “*Is On-Device AI Broken and Exploitable? Assessing the Trust and Ethics in Small Language Models*”.

Dissertation

- **[M.S. Dissertation]** Kalyan Nakka. “*Achieving Connected k-Coverage in Wireless Sensor Networks Using Computational Geometry-Based Approaches*”, Texas A&M University-Kingsville, 2023.

Research Experience

SPIES Research Lab, Texas A&M University

Jan. 2024 – Present

- **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.

- **Safeguarding On-Device Small Language Models:** In this work, we developed a practical on-device deployable lightweight deep learning (DL)-based guardrails for safeguarding Small Language Models (SLMs) against quantization-induced risks and vulnerabilities, by characterizing a novel threat model called *Open Knowledge Attack*. The results illustrated that our prompt guard secures on-device SLMs effectively and efficiently in terms of safety and latency assessments. Further, we practically demonstrated the mitigation of these vulnerabilities using our guardrails.
- **Jailbreaking Aligned Large Language Models:** In this study, we demonstrated the effectiveness of novel vulnerability, called Bitstream Camouflage, in jailbreaking aligned Large Language Models (LLMs). The results illustrate the high effectiveness of this vulnerability in jailbreaking aligned LLMs in terms of adversarial performance, generating phishing content, and bypassing guard models.

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 Resource 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 not be 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

Graduate Teaching Assistant, Texas A&M University–Kingsville

- CSEN 5303: Massive Parallel Computing
- CSEN 5303: Foundations of Computer Science

Summer 2022

Spring 2022

Invited Talks/Presentations

- [GCRI 2025] “Safeguarding Both Mobile AI and User: Seamless and Lightweight On-Device Guardrails for Small Language Models against Quantization Vulnerabilities”, Texas A&M Global Cyber Research Institute Annual Summit (GCRI), College Station, TX, September 2025
- [TICI 2025] “Trust and Ethics Gap in On-Device Quantized Language Models: Risks and Vulnerabilities”, Texas A&M Initiative for Connected Intelligence (TICI), College Station, TX, March 2025
- [GCRI 2024] “Broken and Exploitable On-Device AI: A Comparative Trust and Ethics Assessment of Small Language Models”, Texas A&M Global Cyber Research Institute Annual Summit (GCRI), College Station, TX, September 2024
- [GSERQ 2023] “Can Geometry Solve Complex Computer Science Problems?”, Texas A&M Graduate Science and Engineering Research Colloquium (GSERQ) Series, Kingsville, TX, USA, February 2023
- [SunSpec 2022] “Potential Quantum Computing Attacks on Distributed Energy Resources and Post-Quantum Cryptography grade IEEE 2030.5”, SunSpec Alliance Annual Meeting (Virtual), Las Vegas, NV, December 2022

Fellowships

Graduate Research Assistantship, Texas A&M University (US \$12,000 p.a.)

2024–2025

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

2022–2023

Dean's Merit Scholarship , Texas A&M University–Kingsville (US \$1,000 p.a.)	2022–2023
Graduate Assistant Scholarship , Texas A&M University–Kingsville (US \$8,500 p.a.)	2021–2023
HEERF III Student Scholarship , Texas A&M University–Kingsville (US \$1,600 p.a.)	2021–2022
Computer Science Graduate Scholarship , Texas A&M University–Kingsville (US \$1,000 p.a.)	2021–2022
Rockwell International Scholarship , Texas A&M University–Kingsville (US \$1,000 p.a.)	2021–2022
MCM Scholarship , IIT–Dhanbad (IND ₹72,000 p.a.)	2013–2016

Community Service

Reviewer

ACM Transactions on Privacy and Security (TOPS)	2024
IEEE Energy Conversion Conference and Exposition (ECCE)	2024
IEEE Transactions on Smart Grid (TSG)	2025
IEEE Transactions on Artificial Intelligence (TAI)	2025

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, B.S. Student, Texas A&M University	2024–Present
Zachary Laguna, M.S. Student, Texas A&M University	2025–Present

Professional Membership

Association for Computing Machinery (ACM)	2025–Present
---	--------------

Technical Skills

Programming Languages: [Fluent] Python, [Familiar] C#, Go, SQL, C++, Java, [Learning] CUDA

Machine Learning: PyTorch, Jupyter Notebooks, scikit-learn, Huggingface, Numpy, Pandas, [Familiar] TensorRT

Technologies: Docker, Kubernetes, Git, Linux, [Familiar] AWS, GCP, Microsoft Azure, [Learning] NVIDIA Triton

References

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