Johan S Varughese

B.Tech – Computer Science & Engineering (AI), APJAKTU

Thiruvananthapuram, Kerala, India
+91-8921954342 | mail2joshvarkey@gmail.com
linkedin.com/in/johan-s-varughese

Summary

Final-year B.Tech (CS & AI) student with hands-on experience in federated learning security, multi-agent systems, and full-stack development. Published researcher (ICMLA 2026 under review) and civic-tech innovator behind NammadeVote—India's first AI-powered election intelligence platform. IET Chairperson and Kerala THRIVE State Lead actively driving engineering research and community outreach.

Education

Mar Baselios College of Engineering & Technology — *Thiruvananthapuram, Kerala*
B.Tech – Computer Science & Engineering (Artificial Intelligence), APJAKTU — *2023 – 2027*

Navajeevan Bethany Vidyalaya — *Thiruvananthapuram, Kerala*
Senior Secondary – XII, CBSE — *2023*

Navajeevan Bethany Vidyalaya — *Thiruvananthapuram, Kerala*
Secondary – X, CBSE — *2021*

Experience

Chairperson – IET MBCET Student Chapter — *Dec 2025 – Present*
Institution of Engineering and Technology, South Asia Region — *Thiruvananthapuram, India*
- Lead technical events, inter-collegiate collaborations, and innovation programs for the MBCET chapter.
- Represent MBCET at IET South Asia Region Marketing Committee and IET Global Research Group.

Program Lead – THRIVE Initiative (Kerala State) — *May 2026 – Present*
State-Wide Technology & Programme For Tribal Backward Students, MBCET Chapter — *Thiruvananthapuram, India*
- Spearheading a social impact initiative that encourages tribal students to explore technology, higher education, and future career opportunities.

Digital Communication & Media Design Intern — *May 2025 – Nov 2025*
Thiruvananthapuram District Administration, Government of Kerala — *Thiruvananthapuram, India*
- Designed and deployed **NammadeVote**—India's first AI-powered election intelligence platform—with live queue intelligence, AI voter assistance, and constituency-level access.
- Platform received statewide recognition across print, radio, and digital media.

Full-Stack Developer Intern (MERN) — *Dec 2024 – Jan 2025*
ICT Academy of Kerala — *Thiruvananthapuram, India*
- Built production-grade RESTful web modules using React, Node.js, Express, and MongoDB with real-time data handling and responsive UI.

Core Coordinator & Technical Lead — *Jan 2026*
Nexora '26 – All Kerala ISTE Student State Convention
- Directed full technical track planning, speaker coordination, and logistics for a statewide engineering student convention.

Research Projects & Engineering Work

NammadeVote | *Python, MERN Stack, Gemini APIs, Real-Time Queue Intelligence, AI Voter Support* — *2025*
- Deployed an AI civic platform with live queue intelligence, AI voter assistance, and constituency-level access; featured across statewide broadcast and digital media.

GeoTrust-FL | *Python, Streaming PCA, JL Projections, Spectral Dynamics, Online Trust Aggregation* — *2024 – 2025*
- Designed a geometry-driven FL security framework detecting malicious updates via temporal low-rank subspace tracking, optimization trajectory analysis, and spectral dynamics monitoring.
- Engineered scalable online trust aggregation algorithms robust against poisoning and stealth adversarial attacks. [*ICMLA 2026 – Under Review*]

ProtoShield-FL | *Python, Federated Learning, Prototype-Based Learning, SMPC, Differential Privacy* — *2024 – 2025*
- Built a privacy-preserving FL framework integrating prototype-based learning, SMPC, and differential privacy for decentralised model training with minimal information leakage.

CollectiveOS | *Python, MARL, Custom Gymnasium Environments, Governance-Aware Policy Evaluation* *2024 – 2025*

- Engineered a MARL framework for institutional reasoning, governance adaptation, and cooperative decision-making under partial observability in decentralised systems.

MedShield & FlareWatch | *CNN, BiLSTM, Attention, Federated Learning* *2024 – 2025*

- **MedShield:** Hybrid CNN+BiLSTM+Attention architecture in a federated framework for privacy-preserving distributed medical imaging prediction.

Publications & Research

Optimization Trajectory Geometry and Spectral Dynamics for Early Detection of Adversarial Training Attacks
Under Review – Main Track, International Conference on Machine Learning and Applications (ICMLA 2026), Rochester Hills, MI, USA

Technical Skills

Languages: Python, Java, JavaScript, SQL, Bash/Shell

AI / ML: PyTorch, TensorFlow, scikit-learn, Federated Learning, MARL, LLMs, NLP, CNNs, BiLSTM, Attention Mechanisms, Differential Privacy, SMPC

Full-Stack: React.js, Node.js, Express.js, MongoDB (MERN), REST APIs, Streamlit, HTML/CSS

Cloud & DevOps: AWS, Git/GitHub, Docker, Linux

Research Areas: Byzantine-Robust FL, Multi-Agent Systems, Swarm Robotics, Remote Sensing, Privacy-Preserving AI, Cyber-Physical Systems

Tools: Gemini APIs, NumPy, Pandas, Matplotlib, Plotly, OpenAI Gymnasium

Certifications & Training

Drone/UAS Technologies Bootcamp – NIT Calicut (MeitY)

AWS Solutions Architecture – Amazon Job Simulation

Cisco Introduction to IoT – Cisco Networking Academy

EY Climate Change & Sustainability – EY Job Simulation

Accenture Software Engineering – Accenture Job Simulation

CARESTACK BRIDGE Program – Industry Readiness

Achievements & Leadership

Best Organizer Award – IET Kanyakumari Local Network *2025*
Recognized for outstanding contribution to the student technical community.

Media Recognition – NammadeVote *2025*
Statewide coverage across print, broadcast (radio), and digital media for civic AI innovation.

Research Paper Under Review – ICMLA 2026 *2026*
Main Track: adversarial attack detection in FL via spectral dynamics & geometry; Rochester Hills, MI.

IET South Asia Region Marketing Committee Member *Dec 2025 – Present*
Active contributor to regional strategy and engineering outreach across South Asia.

IET Global Member Research Group Committee Member *Dec 2025 – Present*
Participating in international engineering research initiatives at the global IET level.

Languages

English: Fluent **Malayalam**: Native **Tamil**: Native **Hindi**: Conversational