YESHWANTH RAJ SELVARAJ

Chennai, India | +91 8122995972 | yeshselva1@gmail.com | LinkedIn | GitHub | Portfolio | Credly

PROFESSIONAL SUMMARY

Computer Science Engineering student (Cyber Security) specializing in AI/ML systems engineering, LLM-driven automation, and cloud security architecture. Proven ability to design and ship production-grade platforms combining **Reinforcement Learning, Generative AI, Graph Neural Networks, and adversarial ML** with **AWS, Kubernetes (EKS), Docker, and Terraform** for secure, scalable infrastructure. Strong foundation in offensive/defensive security (VAPT, threat modeling, DevSecOps, MITRE ATT&CK) paired with deep applied AI expertise. Author of a peer-reviewed ML publication (95.35% accuracy, 0.948 ROC-AUC), multi-hackathon winner, and active researcher in Quantum Machine Learning (QML) and Post-Quantum Cryptography (PQC).

EDUCATION

B.Tech in Computer Science and Engineering (Cyber Security) **08/2023 – 08/2027**
Amrita Vishwa Vidyapeetham, Chennai (Currently in 7th Semester)

PROFESSIONAL EXPERIENCE

Cloud Security Research Engineer (Ongoing) **06/2026 – Present**
Zepto Marketplace Private Limited, Bengaluru, Karnataka, India (On-site)

- Researching and analyzing **cloud security architectures** across AWS, Kubernetes (EKS), and cloud-native environments, with a focus on **Zero Trust** and defense-in-depth security models.
- Conducting **threat modeling, vulnerability assessments, and attack surface analysis** to identify and mitigate risks across cloud infrastructure and containerized applications.
- Evaluating **IAM frameworks, VPC security configurations, WAF policies, and Kubernetes security controls** to strengthen enterprise security posture.
- Investigating **security automation, cloud threat detection, and incident response strategies**, gaining hands-on exposure to modern cloud security operations and risk management practices.

Artificial Intelligence Intern (Selected) **Oct 2026**
Infosys Springboard Internship 7.0 (Virtual)

- Selected for Infosys Springboard Internship 7.0; assigned to Batch 5.

AI & Cloud Services Intern **02/2026 – 05/2026**
VINSINFO, Chennai, Tamil Nadu, India (Hybrid)

- Deployed and operated **cloud-native applications on AWS using Docker and Kubernetes (EKS)**, ensuring high availability and scalable container orchestration.
- Engineered **secure cloud infrastructure** with AWS VPC segmentation, IAM least-privilege policies, and AWS WAF, aligned with cloud security best practices.
- Built **serverless, event-driven workflows** using AWS Lambda and API Gateway for automated backend processing.

Software Development Intern **09/2025 – 12/2025**
Goklyn Pvt. Ltd

- Built and optimized **full-stack web applications** using React.js, Node.js, JavaScript, and Python, improving performance and reliability.
- Strengthened **debugging, testing, and version-control workflows** via GitHub-based collaborative development.
- Implemented **UI/UX components from Figma specifications**, ensuring design-to-code fidelity.

TECHNICAL SKILLS

Programming Languages: Python, Java, C++, Go, JavaScript, SQL, C
AI/ML & Data Science: GenAI, LLMs, Deep Learning, RL, NLP, Computer Vision, GNNs, Multi-Agent Systems, XGBoost, LightGBM, CNNs, RNNs, SHAP, GANs
Frameworks & Libraries: PyTorch, TensorFlow, PyTorch Geometric, FastAPI, Flask, LangChain, Ray Serve, Ray RLlib, vLLM, NumPy, Pandas, Scikit-learn
Cloud, DevOps & MLOps: AWS (EC2, Lambda, API Gateway, IAM, VPC, WAF, CloudTrail), Docker, Kubernetes (EKS), Terraform, CI/CD, Infrastructure as Code (IaC), Zero Trust Architecture
Cybersecurity & Security Tools: OWASP ZAP, Nuclei, Metasploit, Burp Suite, Wireshark, Nmap, Kali Linux, VAPT, DevSecOps, Threat Detection, Network Forensics, MITRE ATT&CK, eBPF
Databases & Analytics: MySQL, PostgreSQL, MongoDB, ELK Stack, ETL Pipelines, Tableau, Power BI, NetworkX
Web & Developer Tools: React.js, Node.js, Express.js, HTML5, CSS3, REST APIs, Linux, Git, GitHub, Bash, Playwright, Streamlit, Android Studio, VS Code, Figma

KEY PROJECTS

Autonomous Adversarial Security Assessment System for VAPT (Digital Twin Framework) *| AI-Driven VAPT*

- Engineered a **digital twin-based platform** enabling production-safe vulnerability discovery, attack simulation, and exploit validation without risking live infrastructure.
- Automated end-to-end **vulnerability scanning, exploit validation, and findings correlation** by integrating FastAPI with OWASP ZAP, Nuclei, and Metasploit into a unified pipeline.
- Applied **DQN-based Reinforcement Learning** to autonomously discover multi-stage attack paths and **GAN-driven anomaly detection** to surface potential zero-day vulnerabilities.

- Architected a **cloud-native Docker/Kubernetes deployment** with real-time security monitoring through the ELK Stack.

Tech Stack: *Python, FastAPI, OWASP ZAP, Nuclei, Metasploit, Docker, Kubernetes, DQN, GANs, ELK Stack, DevSecOps*

Cloud IAM Forensics Framework for Threat Detection & Incident Investigation *| Cloud Security & Digital Forensics*

- Built a **multi-cloud IAM forensic framework** spanning AWS, Azure, and GCP to detect identity-based threats, privilege misuse, and misconfigurations at scale.
- Combined **graph analytics with ML-based threat classification**, mapping detected behaviors to the MITRE ATT&CK framework and generating automated forensic reports.

Tech Stack: *Python, Flask, Scikit-learn, NetworkX, AWS CloudTrail, Azure Logs, GCP Audit Logs*

TorViz – Tor & VPN Traffic Deanonymization Engine *| Network Forensics & Intelligence Platform*

- Developed a **network forensics platform** for deep packet inspection (DPI) and analysis of Tor, VPN, and encrypted traffic using NetFlow/IPFIX and PCAP processing.
- Implemented **JA3 TLS fingerprinting, eBPF-based traffic attribution, and C2 channel detection** for real-time forensic monitoring and adversary identification.

Tech Stack: *Python, FastAPI, React.js, Scapy, eBPF, NetFlow/IPFIX, JA3, Docker, Linux*

Multi-Agent Reinforcement Learning System for Autonomous Warehouse Robotics *| AI – Robotics – RL*

- Built a **digital twin warehouse** for autonomous navigation, inventory management, and task allocation.
- Designed **MARL policies using MAPPO and GNN-based inter-agent communication** for path planning, congestion avoidance, and real-time multi-robot coordination, optimizing throughput and route efficiency.

Tech Stack: *Python, C++, ROS2, NVIDIA Isaac Sim, Ray RLlib, MAPPO, Reinforcement Learning, GNNs, Multi-Agent Systems*

AI-Driven LEO Satellite Mesh Routing & Space Edge Computing Platform *| Graph ML – Networking – Edge Computing*

- Designed a **software-defined networking (SDN) platform** for dynamic, fault-tolerant routing across Low Earth Orbit (LEO) satellite constellations.
- Built a large-scale orbital simulation framework and applied **Temporal GCNs** for traffic prediction, congestion forecasting, and route optimization.

Tech Stack: *Go, Python, PyTorch Geometric, Temporal GCNs, GNNs, Docker, WebSockets, Distributed Systems, Edge Computing*

AI-Driven Job Intelligence & Automation Platform *| Applied AI – Automation Systems*

- Built an **LLM-powered platform** for automated resume parsing, skill extraction, and role-suitability scoring.
- Automated **job discovery workflows end-to-end** using secure authentication, browser automation (Playwright), and intelligent web data extraction.

Tech Stack: *Python, Playwright, LangChain, Streamlit, LLMs*

PUBLICATIONS & RESEARCH

Gradient Boosting-Based Framework for Alzheimer's Disease Prediction Using Clinical and Lifestyle Data
Accepted – ICPC2T 2026, NIT Raipur (Publication expected June 2026)

- Designed an **interpretable ensemble ML pipeline using XGBoost and LightGBM** on 2,149 patient records spanning 35 clinical, cognitive, and lifestyle features.
- Achieved **95.35% accuracy and 0.948 ROC-AUC** through ensemble learning and stratified cross-validation.
- Applied **SHAP** to interpret key predictive features including MMSE, ADL, and Functional Assessment scores.

CERTIFICATIONS & DIGITAL BADGES

- Oracle Cloud Infrastructure (OCI): Architect Associate, Networking, and Generative AI Professional Certifications (2025)
- Infosys Springboard: Artificial Intelligence Primer Certification; Principles of Generative AI Certification; OpenAI GPT-3 for Developers; Deep Learning for Developers
- NPTEL, IIT Kharagpur: DSA in Java, Cloud Computing (Elite), Ethical Hacking
- Cisco Networking Academy: Ethical Hacking, Cyber Threat Management, Endpoint Security, Network Defense
- Palo Alto Networks: Network Security, Cybersecurity, SecOps, and Cloud Security Fundamentals
- Ethical Byte: Penetration Pro Essential (PPE) – Credential ID: EBPPE12AMR25029
- INE Security: eJPT (eLearnSecurity Junior Penetration Tester) – Currently Preparing for Certification Exam

ACHIEVEMENTS & LEADERSHIP

- **Infineon Technologies Hackathon – "Defend the Kingdom" (Jan 2026): First Prize Winner, DSA Track** – won among 10+ teams (40+ participants) by engineering a time-based simulation system using **Dijkstra's Algorithm** (evaluated against A*) with event-driven logic, resource-constraint handling, and robust XML input parsing.
- **Club Coordinator, AMIGOS Amrita (Game Development Club), Amrita Vishwa Vidyapeetham (Nov 2023 – Nov 2025):** Mentored members in Blender, Unity, and C# scripting; organized technical workshops and hackathons; coordinated **BotBattleX 2025** under Amrita CyberNation (ACN 2025), a 2.5-hour national-level design sprint with 50+ participants.
- Solved **150+ problems on LeetCode** across DSA, graphs, dynamic programming, trees, and greedy algorithms.
- Hands-on knowledge of the **OWASP Top 10** web application vulnerabilities, secure coding principles, and vulnerability remediation techniques.