Sudeep Ravichandran

(812) 322-0465 | sudeep7217@gmail.com | sudeepdev.netlify.app

sudeep72 | Sudeep72 |

Professional Summary

Cybersecurity graduate student with hands-on experience building production-grade detection systems, SIEM platforms, and AI-augmented security tooling. Designed and shipped NanoSIEM, a complete open-source SIEM with a custom Sigma rule engine, ML anomaly detection, Gemini AI reasoning, and live threat visualization. Published research on LLM and Knowledge Graph-based log anomaly detection (Springer LNNS 2025) and privacy-preserving medical image retrieval (Springer LNNS 2024). Strong foundation in detection engineering, incident response, adversarial ML, and security automation on Linux environments.

Education

- **Indiana University Bloomington** *2025 - 2027*
  Master of Science in Cybersecurity Risk Management; CGPA: 4.0/4.0 Bloomington, IN, USA
  - **Relevant Coursework:** Risk Assessment & Management, Network Security, Privacy Law

- **College of Engineering Guindy, Anna University** *2021 - 2025*
  Bachelor of Engineering in Computer Science and Engineering; CGPA: 8.59/10.00 (3.716/4.0 US Equivalent) Chennai, TN, India
  - **Relevant Coursework:** Data Structures & Algorithms, Machine Learning, Information Security, Cryptography & Network Security

Research Work

- **LogREx: Reasoning-Enabled LLM and Knowledge Graph Based Anomaly Detection in System Logs**
  Under Dr. V. Vetriselvi (Professor), DCSE, College of Engineering Guindy [📄]
  - Developed LogREx, a detection engineering framework applying machine learning models and LLM-based reasoning over Knowledge Graphs to identify anomalous behavioral patterns in system log data with interpretable, human-readable explanations.
  - Achieved F1-score of 0.867, outperforming DeepLog (0.814) and LogRobust (0.852) baselines; generated 90% accurate anomaly explanations validated against expert annotations using ROUGE, BLEU, and BERTScore metrics. Research paper accepted in Springer LNNS, presented at CIS 2025.

- **PCMedIR: Privacy-Enhancing Cross-Modal Medical Information Retrieval System in Cloud**
  Under Dr. V. Vetriselvi (Professor), DCSE, College of Engineering Guindy [📄]
  - Developed a novel system for secure medical image retrieval using CLIP, Deep Pairwise Hashing (DPH), and hyperchaos-based encryption with steganography to ensure patient privacy and data integrity in cloud environments.
  - Published in Springer's Lecture Notes in Networks and Systems (LNNS, Volume 1374) and presented at ICCIS 2024. Achieved 90% precision for text-to-image retrieval and 80% for image-to-text retrieval.

Projects

- **NanoSIEM: Open-Source AI-Augmented SIEM with Multi-Stage Kill Chain Detection** *Apr 2026 - Jun 2026*
  Tools: Python, FastAPI, React, Sigma, scikit-learn, Gemini 2.5 Flash, STIX 2.1, Kali Linux [GitHub]
  - Built a production-grade open-source SIEM from scratch with a custom Sigma rule AST parser (17 rules, 56% MITRE ATT&CK coverage), sliding-window correlation engine detecting 6 multi-stage kill chains, and an Isolation Forest ML anomaly scorer with 31-feature extraction and SHAP-style XAI attribution across RFC5424, CEF, JSON, and plaintext log formats.
  - Engineered a Gemini 2.5 Flash AI reasoning layer for real-time SOC analyst explanations and ATT&CK context; shipped a 9-tab React dashboard with live WebSocket streaming, canvas-based Threat Map with multi-origin IP geolocation, per-attacker isolated Knowledge Graphs, Attack Replay forensics, and an incident lifecycle state machine with false positive feedback loop triggering automated ML retraining; 485 tests, zero paid APIs.

- **ZeroSight: Behavioral Anomaly Detection for Zero-Day Protocol Exploits** *Mar 2026 - Apr 2026*
  Tools: Python, FastAPI, scikit-learn, JavaScript, CICIDS2017, Wireshark, Kali Linux [GitHub]

- Built ZeroSight, a network behavioral anomaly detection platform combining Isolation Forest (unsupervised, BENIGN-only trained) and Random Forest (18-class supervised) models on 19,950 synthetic CICIDS2017 flows with 31 features across 17 attack categories; deployed via FastAPI with an interactive dashboard.
- Achieved 89.9% F1-score for anomaly detection and 94.4% macro-average recall across 18 traffic classes; implemented SHAP-style per-flow explainability highlighting top contributing features for every alert and a browser-native, zero-upload PCAP parser that extracts bidirectional flows via real timestamps and 5-tuple grouping, validated on live Firefox traffic where DNS flows were classified as CLEAN and CDN bursts were attributed to Backward Packets/s.

- **SecureZone: Multi-Layer Network Security System with Automated SDN Response** *Aug 2025 - Dec 2025*
  Tools: Python, Linux, Flask, scikit-learn, SDN, UEBA, SSL/TLS, DNS Security [GitHub]
  - Built SecureZone, a 7-layer threat detection platform integrating ensemble ML (Isolation Forest, MLP, DBSCAN), SSL/TLS inspection, DNS security, UEBA, and threat intelligence correlation on Linux; developed a Flask dashboard for real-time threat monitoring and network visualization.
  - Achieved 91.2% detection accuracy with an 8.2% false-positive rate; implemented risk-adaptive SDN-based incident response with <0.4 ms latency, continuously improving detection quality through alert outcome and log analysis.

Skills

- **Cybersecurity Tools & Technologies:** Kali Linux, Linux (Ubuntu), Burp Suite, Wireshark, Metasploit, Nmap, OWASP ZAP, Splunk, Snort, NanoSIEM (author)
- **Detection & Analysis:** Anomaly Detection, Behavioral Analytics, Log Analysis, Threat Intelligence, Kill Chain Correlation, Incident Response, Vulnerability Analysis
- **Security Frameworks & Standards:** MITRE ATT&CK, Sigma Rules, STIX 2.1, OWASP Top 10, NIST CSF, Zero Trust
- **AI & Data Science:** Machine Learning, scikit-learn, Knowledge Graphs, LLM Reasoning, Gemini 2.5 Flash, AI-Augmented SOC Tooling
- **Programming & Development:** Python, C, C++, JavaScript, Java, React.js, FastAPI
- **Cloud & Databases:** AWS, Azure, MySQL, PostgreSQL, MongoDB, Git

Certifications

- **Google Cybersecurity Specialization** *June 2023 - Dec 2023*
  Google
  A professional course covering SIEM tools, incident response, and network security to protect against cyber threats and illegal access.

- **Fundamentals of Computer Network Security Specialization** *Oct 2022 - Feb 2023*
  University of Colorado System
  A professional course to master security principles and tools for securing networks, systems, and data.

- **GenAI 101 Certified Pathway** *Nov 2025*
  Indiana University Bloomington
  A university-issued professional certification covering Generative AI foundations, prompting, applied AI workflows, and responsible AI practices.

Achievements

- **Winner of Startup Weekend Chennai 2022** *Feb 2022*
  Techstars [Web]
  - Built a 54-hour prototype of a barcode-scanning mobile app that delivers dietary compatibility and nutrient insights with a strong focus on user experience.

Positions of Responsibility

- **Student Director - TechOps** *Jul 2024 - Jul 2025*
  CEG TECH FORUM
  - Led the TechOps domain of an ISO-certified student organization with 900+ members, overseeing technical operations for Kurukshetra, a UNESCO-recognized international technical festival.
  - Managed technical infrastructure, event systems, and team operations for workshops, competitions, and exhibitions; led system setup, troubleshooting, and security efforts to ensure seamless festival execution.