CHETHAN G S

+91 9986796131 | gschethan136@gmail.com | LinkedIn Profile | Bengaluru, KA, India

EDUCATION

PES University Aug. 2024 – May 2027
B.Tech in Computer Science | ***Specialization: Cybersecurity*** Current CGPA: 6.93

Govt Polytechnic, Mulbagal Oct. 2021 – May 2024
Diploma in Computer Science CGPA: 9.47

Jyothi English Medium School, ICSE 2011 – 2021
Secondary Education Percentile: 74

EXPERIENCE

PESU ISFCR SOC, PES University Oct. 2024 – Present
Student Researcher - Part-time Bengaluru, KA

- Write and tune **IDS/IPS rules** (Suricata, Zeek), integrating AI/ML for adaptive threat detection and testing with real and synthetic traffic
- Build **SIEM-like systems** with ELK dashboards, log ingestion, alert pipelines, and Suricata log integrations
- Perform traffic generation, port scanning, and malicious traffic injection for rule validation
- Develop **reinforcement-learning based IDS controllers** with real-time monitoring dashboards
- Research hybrid IDS efficiency metrics including DR, FPR, CPU usage, and latency across datasets

PES University Jan. 2026 – May. 2026
Teaching Assistant – Computer Networks Bengaluru, KA

- Conduct labs and evaluate assignments and projects for the Computer Networks course
- Assist students in understanding core networking concepts and troubleshooting

Center for Information Security, Forensics and Cyber Resilience Jun. 2025 – Jul. 2025
Summer Intern Bengaluru, KA

- Focused on **Network Security and Cyber Threat Intelligence (CTI)**
- Conducted research on advanced IDS architectures and ML integrations for threat detection

Excerpt Technologies Private Limited Jan. 2024 – Apr. 2024
Junior Cyber Security Engineer - Internship Bengaluru, KA

- Built **automation scripts** for threat detection and incident response workflows
- Assisted in endpoint security audits and ensured data protection compliance
- Conducted **web penetration testing** on internal and client-facing products

PROJECTS

Diagnostic Imaging Center SOC Lab Simulation | *Wazuh, Suricata, Shuffle, Docker, DICOM*

- Built a **HIPAA-aware SOC lab** simulating a real diagnostic imaging center with segmented VLANs (Medical, Admin, DMZ) hosting PACS, RIS, MRI/CT simulators, and a patient portal
- Deployed **Wazuh SIEM + Suricata IDS/IPS + Shuffle SOAR** stack with **17 custom HIPAA/DICOM detection rules** and 8 MITRE ATT&CK attack scenarios including ransomware, DICOM exfiltration, and AD enumeration
- Integrated **threat intelligence enrichment** (VirusTotal + AbuseIPDB) and ML-based anomaly detection; SOAR auto-triggers incident creation on breach detection per HIPAA
- Source code: GitHub

Fake Product Identification via QR Code using Blockchain | *Blockchain, SHA-256, JavaScript*

- Built a **real-time counterfeit detection system** where manufacturers generate QR codes using the **SHA-256 algorithm** stored on blockchain
- Users scan the QR code to instantly verify product authenticity, preventing counterfeit goods from reaching consumers
- Source code: GitHub

AI-powered voice assistant-Dhanvantari | *AI, Speech Recognition, NLP*

- Developed an **AI-powered voice assistant** allowing users to ask health-related questions in their local language and receive spoken responses
- Covers hygiene, nutrition, maternal health, and common diseases, targeting **low-literacy and rural users**
- Source code: GitHub

An Adaptive Framework for NID's using XGBoost and Suricata IDS | *Suricata, XGBoost, Python*

- Integrated **XGBoost** with Suricata IDS to classify network alerts using the **UNSW-NB15 dataset** for training
- Achieved high-accuracy threat detection with **significantly reduced false positives** over baseline Suricata rules
- Source code: GitHub

CERTIFICATIONS

ISC2 Certified in Cybersecurity (CC) *Jan. 2026 – Jan. 2027*

Mastering Cyber Threat Intelligence for SOC Analysts | *SOCRadar* *Sep. 2025*
View Certificate

Introduction to Computers, Operating Systems and Security | *Microsoft* *Jul. 2025*
View Certificate

Python (Basic) | *HackerRank* *Apr. 2025*
View Certificate

Network Security | *Great Learning* *Sep. 2024*
View Certificate

Cyber Security Foundation | *Infosys* *Aug. 2023*

ACHIEVEMENTS

Microsoft Windows — P3 Bug Bounty

- Discovered and reported a **P3-level vulnerability** in Microsoft Windows, acknowledged through Microsoft's responsible disclosure program

CyberClash — Organiser, India's First Red vs. Blue Hackathon

- Co-organised **India's first Red vs. Blue 8-hour hackathon**, bringing together offensive and defensive security teams in a live adversarial challenge

CryoVault — National CTF Competition Host

- Core team member for hosting **CryoVault**, a national-level Capture The Flag competition; responsible for challenge design, infrastructure, and coordination

Responsible Vulnerability Disclosure — College Website

- Identified and responsibly disclosed **security vulnerabilities** in the college's official website to the IT administration

VOLUNTEERING

CyberPeace Corps
Oct. 2025 – Present

- Contributing to **cybersecurity awareness** and digital peace initiatives as an active volunteer

Google Cloud Agentic AI Day 2025 | *Hack2skill*
2025

- Managed check-in operations and ensured smooth end-to-end event flow as a **Hack2skill volunteer**
- View Participation Certificate

CSR Club, PES University

- Participated in **community social responsibility** and social service activities organised by the club

SKILLS

Languages : Python, Java, Bash, JavaScript, HTML/CSS, SQL (MySQL)
Tools : Wazuh, Suricata, Zeek, Splunk, Graylog, ELK Stack, AWS, Microsoft Azure, GitHub
Specialized : Network Security, Cloud Security, SOC Operations, Penetration Testing, Cyber Threat Intelligence