

ALGOPROFESSOR CAMPUS · SKILL & EXPLORATION
FRAMEWORKS



Semester-wise Skill & Exploration Curriculum Framework

B.Tech in Cyber Security

An 8-semester, 8-exploration project model mapping each semester's core skill
to industry, village, state, national and SDG problems

Curriculum suggestions & framework design

Dr. S. Satyanarayana

Founder, CEO & Chief Agentic AI Scientist, AlgoProfessor AI R&D Solutions
campus.algoprofessor.com · ceo@algoprofessor.com

Preface & vision statement

A note for heads of department

The industry does not hire syllabi: it hires **demonstrable capability**. This framework converts every semester of the B.Tech (Cyber Security) programme into a paired unit of *skill acquisition* and *applied exploration*, so that by graduation each student carries not just a transcript but a portfolio of eight real, verifiable, deployed projects that speak directly to placement panels, startup incubators and global research programmes.

Every exploration project is anchored to a **real-world problem statement**, sourced from industry, neighbouring villages, state departments, India's national missions or the UN Sustainable Development Goals, so that students learn to build technology *for* people and places, not merely for assignments.

Guiding principle: "Learn a skill. Solve a real problem. Prove it publicly."

Each semester has three fused components:

1. **Core skill track:** one dominant technical competency, taught to depth.
2. **Exploration project (E1–E8):** a mandatory, individually assigned project applying that semester's skill to a live problem statement.
3. **Public proof of work:** a mandatory e-Portfolio entry and GitHub repository submission under departmental governance.

1 Framework overview

Framework name: *EXPLORE: Eight-semester eXPerience Ladder for Original Research & Engineering*

Applicability: all B.Tech (Cyber Security) students, all batches, mandatory

Mandate: every student completes **8 exploration projects**, one per semester, each mapped to that semester's core skill and to at least one external problem category (industry / village / state / national / SDG).

1.1 Semester → skill → exploration snapshot

Sem	Core skill track	Exploration project	Primary problem lens
I	Programming & Computing Foundations (Python, Linux)	E1: Secure Community Digitisation Utility	Village record-keeping with safe data handling
II	Computer Networks & Data Structures	E2: Network Insight Tool	Connectivity and network visibility
III	Operating-System Security & Cryptography	E3: Secure Systems for Social Good	Protecting health, finance and land records
IV	Web Application Security & Ethical Hacking	E4: Vulnerability Assessment Engine	Authorised testing of MSME, school and public web systems
V	Security Operations, SIEM & Digital Forensics	E5: Security Monitoring Pipeline & Dashboard	Monitoring, fraud and cyber-crime analytics
VI	Cloud Security & AI for Security	E6: Intelligent Threat Defence	AI-driven defence and cloud posture
VII	IoT/OT Security, Zero Trust & Agentic Defence	E7: Autonomous Defence & Cyber-Physical Security	Cyber-physical security and automated response
VIII	Capstone Integration	E8: Combined Capstone Project	Deployable security product: placement, startup or global track

2 Semester-wise skill & exploration details

SEMESTER I | Programming & Computing Foundations (Python, Linux)

Skill outcomes: Python scripting, Linux command line, file permissions, users and processes, basic cyber hygiene and ethics of security work.

Exploration-1 (E1): Secure Community Digitisation Utility

A Python tool that digitises a manual record for a real stakeholder with basic security built in: login, backups and access control.

- *Sample problem statements:* (VILLAGE) Village records digitiser with user login and backups; (INDUSTRY) Password and backup hygiene checker for an MSME; (VILLAGE) School device inventory and patch tracker; (NATIONAL) Phishing-awareness quiz app in a regional language
- *Problem source(s):* Nearest village panchayat, local MSMEs, school administration
- *SDG mapping:* • SDG 4 Quality Education • SDG 16 Peace, Justice & Strong Institutions

SEMESTER II | Computer Networks & Data Structures

Skill outcomes: OSI and TCP/IP, routing and switching, DNS and DHCP, packet analysis, socket programming, core data structures and algorithms.

Exploration-2 (E2): Network Insight Tool

A tool that measures, maps or improves a real network for a community or small organisation.

- *Sample problem statements:* (VILLAGE) Wi-Fi coverage and usage mapper for a gram panchayat; (INDUSTRY) Packet-capture analyser for a small office; (STATE) Fair-share bandwidth scheduler for a school computer lab; (INDUSTRY) Network inventory and topology mapper for a cooperative
- *Problem source(s):* Gram Panchayat, local MSMEs, government schools, cooperative societies
- *SDG mapping:* • SDG 9 Industry, Innovation & Infrastructure • SDG 4 Quality Education

SEMESTER III | Operating-System Security & Cryptography

Skill outcomes: Access control, hardening, logging, symmetric and public-key cryptography, hashing, PKI and secure-coding basics.

Exploration-3 (E3): Secure Systems for Social Good

A system that protects sensitive community data using sound cryptography and hardening.

- *Sample problem statements:* (VILLAGE) Encrypted health-record vault for a Primary Health Centre; (INDUSTRY) OTP and two-factor login for a cooperative bank portal; (STATE) Tamper-evident hash ledger for land records; (NATIONAL) Hardened Linux image for public service kiosks
- *Problem source(s):* PHC health workers, cooperative banks, State Revenue Dept., e-governance kiosks
- *SDG mapping:* • SDG 3 Good Health & Well-being • SDG 16 Peace, Justice & Strong Institutions

SEMESTER IV | Web Application Security & Ethical Hacking

Skill outcomes: OWASP Top 10, reconnaissance, scanning, exploitation in lab environments, secure coding fixes and professional reporting. Testing is done only on lab copies or with written authorisation.

Exploration-4 (E4): Vulnerability Assessment Engine

An authorised vulnerability assessment with automated checks and a remediation report for a real or lab-replicated system.

- *Sample problem statements:* (INDUSTRY) Authorised VAPT of a partner MSME website; (STATE) OWASP checker run on a lab copy of a public e-service portal; (NATIONAL) Phishing-URL classifier; (VILLAGE) School website hardening and monitoring
- *Problem source(s):* Industry partners with written scope, lab replicas of public services, CERT-In advisories
- *SDG mapping:* • SDG 9 Industry, Innovation & Infrastructure • SDG 16 Peace, Justice & Strong Institutions

SEMESTER V | Security Operations, SIEM & Digital Forensics

Skill outcomes: Log collection, SIEM rules and dashboards, alert triage, incident response, disk and memory forensics, security analytics.

Exploration-5 (E5): Security Monitoring Pipeline & Dashboard

A live log pipeline and detection dashboard built on real or realistic data for an organisation or public body.

- *Sample problem statements:* (INDUSTRY) Log pipeline and detection dashboard for an MSME; (NATIONAL) Fraud-pattern dashboard for digital payments (synthetic data); (STATE) Cyber-crime complaint analytics from open district data; (VILLAGE) Intrusion alerts for village public Wi-Fi
- *Problem source(s):* Industry partners, open government data, district cyber cells, panchayat Wi-Fi operators
- *SDG mapping:* • SDG 16 Peace, Justice & Strong Institutions • SDG 9 Industry, Innovation & Infrastructure

SEMESTER VI | Cloud Security & AI for Security

Skill outcomes: Cloud IAM and posture management, logging, malware analysis basics, ML for detection, LLM security and red-teaming of AI systems.

Exploration-6 (E6): Intelligent Threat Defence

An AI-assisted or cloud-security system that detects or prevents a real threat pattern.

- *Sample problem statements:* (NATIONAL) ML phishing and spam detector for regional languages; (INDUSTRY) LLM assistant for SOC alert triage; (INDUSTRY) Cloud misconfiguration scanner for a startup; (SDG) Voice-fraud and deepfake awareness detector
- *Problem source(s):* Industry partners, startups, national cyber-awareness programmes
- *SDG mapping:* • SDG 16 Peace, Justice & Strong Institutions • SDG 10 Reduced Inequalities

SEMESTER VII | IoT/OT Security, Zero Trust & Agentic Defence

Skill outcomes: IoT and industrial control security, zero-trust architecture, automated response with agents, and a seminar on post-quantum cryptography.

Exploration-7 (E7): Autonomous Defence & Cyber-Physical Security

A cyber-physical security testbed, an agentic response system, or a supervised research report on emerging threats.

- *Sample problem statements:* (INDUSTRY) Multi-agent incident-response playbook automation; (STATE) Smart-meter security testbed for a state utility; (VILLAGE) Secure drone telemetry for farm surveys; (INDUSTRY) Contribution (PR/issue) to an open-source security tool; (SDG) Post-quantum cryptography migration study
- *Problem source(s):* Industry partners, state power utilities, global open-source community
- *SDG mapping:* • SDG 9 Industry, Innovation & Infrastructure • SDG 17 Partnerships for the Goals

SEMESTER VIII | Capstone Integration

Skill outcomes: End-to-end security product delivery, DevSecOps, documentation, responsible disclosure, pitching and IP awareness.

Exploration-8 (E8): Combined Capstone Project

Students combine their skills and, wherever feasible, earlier explorations (E1–E7) into one deployable security product on a chosen track.

- *Tracks:* **Placement track** (Industry problem statement, mentored jointly by department faculty and a recruiting partner.); **Startup track** (Student-founded idea pitched to the institution's incubation cell, guided by industry mentors.); **Global Exposure track** (Co-supervised with international postdoctoral and Ph.D. research collaborators.)
- *Deliverables:* Deployed application, technical report, demo video, pitch deck, complete GitHub repository and e-Portfolio capstone entry.
- *Example capstone themes:* (INDUSTRY) SOC-in-a-box for an MSME client (authorised); (VILLAGE) Cyber-hygiene and fraud-alert service for rural banking customers; (STATE) Zero-trust reference architecture for a state e-service (lab replica); (SDG) Post-quantum migration toolkit with international collaborators
- *Problem source(s):* Recruiting partners, incubation cell, international research collaborators
- *SDG mapping:* aligned to whichever SDGs the chosen capstone theme serves; declared at proposal stage.

3 Compulsory subjects, programming languages & tools, and global certification roadmap

Basis of this mapping

Compiled by aligning (a) global-standard practice for computing programmes: core theory before applied specialisation, with a mandatory capstone; (b) ABET / NBA-style outcome-based subject sequencing; and (c) the skill sets most consistently sought by leading employers, so that learning outcomes and industry-recognised certifications reinforce each other every semester.

3.1 Semester-wise mapping table

Sem	Compulsory subjects	Programming languages & tools	Recommended global certifications
I	Python Programming; Mathematics I; Computer Fundamentals & Linux; Cyber Hygiene, Law & Ethics	Python 3; Linux shell; Git & GitHub; VirtualBox	ISC2 Certified in Cybersecurity (CC); Cisco Introduction to Cybersecurity
II	Computer Networks; Data Structures & Algorithms; Discrete Mathematics & Number Theory; Database Management Systems	Wireshark; Python Scapy; Cisco Packet Tracer; SQL	CompTIA Network+; Cisco Networking Basics
III	Operating Systems & Security; Cryptography; Linux Administration; Web Technologies	Linux; OpenSSL; GPG; Bash; Python cryptography	CompTIA Security+; Linux Foundation Certified IT Associate (LFCA)
IV	Web Application Security; Ethical Hacking; Software Engineering; Secure Coding	Burp Suite; OWASP ZAP; Nmap; Metasploit (lab); Kali Linux	eLearnSecurity Junior Penetration Tester (eJPT); EC-Council Certified Ethical Hacker (CEH)
V	Security Operations; Digital Forensics; Cloud Computing; Data Analytics for Security	Wazuh/Splunk/Elastic; Microsoft Sentinel; Sigma rules; Autopsy; Volatility	CompTIA CySA+; Splunk Core Certified User; Microsoft Security Operations Analyst (SC-200)
VI	Cloud Security; Machine Learning for Cyber Security; Malware Analysis; AI Security & LLM Red-Teaming	AWS/Azure security services; Prowler/ScoutSuite; scikit-learn; Ghidra; Garak/PyRIT	Microsoft Azure Security Engineer Associate (AZ-500); CSA Certificate of Cloud Security Knowledge (CCSK)
VII	IoT & OT Security; Zero Trust Architecture; Agentic AI for Security Operations; Post-Quantum Cryptography Seminar	Raspberry Pi/ESP32; MQTT; Zeek/Suricata; LangGraph; liboqs	GIAC Certified Incident Handler (GCIH); ISO/IEC 27001 Lead Implementer
VIII	Capstone Engineering Project; Security Architecture & Risk Management; Cyber Law, IP & Technical Communication; Industry Internship	SIEM + cloud security stack; DevSecOps pipeline; Docker/Kubernetes; cloud deployment (AWS/Azure)	OffSec Certified Professional (OSCP); AWS Certified Security – Specialty

3.2 Cross-cutting skill ladders

These skills do not belong to a single semester. Employers expect them as continuous, compounding skills, so each is introduced, applied and brought to production grade across the eight semesters.

Skill track	Introduced	Applied	Production-grade	Core tools & certifications
-------------	------------	---------	------------------	-----------------------------

Cloud Security	Sem III (Linux and identity fundamentals)	Sem VI (cloud posture, IAM, logging)	Sem VII–VIII (zero trust, secure capstone hosting)	AWS/Azure security services, Prowler; CCSK, AZ-500
Detection Engineering	Sem II (packet analysis)	Sem V (SIEM, Sigma rules, dashboards)	Sem VII–VIII (automated response, agentic SOC)	Wazuh/Splunk/Sentinel, MITRE ATT&CK; CySA+, SC-200
Secure Development (DevSecOps)	Sem III (cryptography and secure-coding basics)	Sem IV (OWASP Top 10, SAST/DAST)	Sem VII–VIII (pipeline security, supply chain, SBOM)	Semgrep, OWASP ZAP, Trivy, GitHub code scanning

4 Problem-statement sourcing matrix

How the HoD curates individual problem statements each semester

For every semester, the HoD (with mentor faculty, industry liaisons and local administration contacts) compiles and *individually assigns* one problem statement per student from the five lenses below, so that no two students in the same batch receive an identical statement.

Problem lens	Source channel	Coordinating body
Industry	Live or simulated challenges from industry partners and R&D collaborators	Industry partners and MoUs, startup network, alumni network
Village	Field visits, panchayat consultations, farmer and artisan interviews	Gram Panchayat, NSS unit, faculty field coordinators
State	Departmental open-problem calls and e-governance portals	State Agriculture, Rural Development, Water Resources and Health departments
National	Alignment with Digital India, Smart Cities, Skill India and NEP 2020 missions	Ministries' open datasets and challenge portals, AICTE / NBA guidance
SDG	UN Sustainable Development Goals framework (17 goals)	Department SDG cell, mapped explicitly to each exploration

Duplication-avoidance rule: every assigned problem statement is logged in the **Central Exploration Register** (section 5) with semester, academic year, roll number and status. Before any new statement is issued, the register is checked so that the same problem is never reassigned to a later batch unless the HoD explicitly marks it "open for extension", encouraging students to pick unsolved or extension-worthy problems from the growing repository.

5 e-Portfolio & GitHub governance

5.1 Departmental GitHub organisation

- **Organisation:** one department-owned GitHub organisation (suggested: YourInstitution-CYS-Explorations) with one repository per student per semester.
- **Repository naming convention:** SEM<n>_<AcademicYear>_<RollNo>_<ShortProjectTitle>, e.g. SEM4_2026-27_21CY045_MSMEVAPTRReport
- **Mandatory repository contents:** problem statement, readme with objective, approach and results, source code, dataset or data-source citation, results and screenshots, short reflection on skill outcomes achieved.
- **Access:** mentor faculty and HoD as organisation owners and reviewers; the student as repository maintainer.

5.2 Student e-Portfolio

- An e-Portfolio page per student, updated at the end of every semester with that semester's exploration summary, skill badge and GitHub link.
- By the end of Semester VIII each student has a public, chronological, eight-project portfolio for placement interviews, startup pitches and international collaboration applications.

5.3 Central Exploration Register (sample structure)

Sem	A.Y.	Roll No.	Project title	Problem lens	GitHub repo	Status
-----	------	----------	---------------	--------------	-------------	--------

IV	2026-27	21CY045	MSME VAPT Report	Industry + SDG 9	SEM4_...	Completed
IV	2026-27	21CY046	Eportal OWASP Checker	State + SDG 9	SEM4_...	In progress

Maintained live by the department office; illustrative rows only.

6 Assessment & evaluation rubric (per exploration project)

Criterion	Weight	Descriptor
Problem understanding & real-world fit	15%	Correct interpretation of the assigned industry, village, state, national or SDG problem statement
Skill application (semester's core skill)	25%	Depth and correctness of the semester's designated technical skill in the solution
Implementation & functionality	25%	Working prototype or system, code quality, reproducibility
Data / evidence basis	10%	Use of real or realistic data, field inputs, or validated assumptions
Documentation (README, report)	10%	Clarity, completeness, reproducibility instructions
GitHub & e-Portfolio compliance	10%	Correct repository structure, timely submission, portfolio update
Presentation / viva	5%	Communication of approach, results and learnings to a mentor or panel

7 Governance roles

Role	Responsibility
Head of Department	Curates and individually assigns problem statements each semester; maintains the Central Exploration Register; approves Semester VIII capstone tracks
Mentor faculty (per section)	Weekly technical mentoring, mid-semester review, GitHub and portfolio compliance checks
Industry / startup liaison	Supplies live industry problem statements; co-mentors Semester VII–VIII projects
International co-supervisors	Research partners who co-mentor selected Semester VII–VIII students on the Global Exposure track
Student	Executes the exploration project, maintains the GitHub repository and e-Portfolio, presents at the semester-end review

8 Implementation roadmap

Suggested roll-out timeline
Phase 1: Framework approval: Present the framework to the Board of Studies / Academic Council for formal adoption into the B.Tech curriculum. Phase 2: Infrastructure set-up: Create the departmental GitHub organisation, e-Portfolio hosting space and the Central Exploration Register. Phase 3: Problem bank seeding: HoD, faculty and industry, village and state liaisons jointly seed the first problem statements across all five lenses for every semester. Phase 4: Pilot batch roll-out: Launch with the current Semester I–II cohort and run E1–E2 as pilot explorations. Phase 5: Full-scale adoption: Extend E1–E8 across all active batches; integrate exploration outcomes into OBE / CO–PO attainment and NBA / NAAC documentation. Phase 6: Annual review: Review the register and rubric every academic year to retire saturated problem statements and induct new ones.

Curriculum suggestions & framework design

Dr. S. Satyanarayana

AlgoProfessor AI R&D Solutions, Hyderabad
ceo@algo professor.com · campus.algo professor.com