

# KALPESH SOLANKI

☎ (+91) 9265212214 | ✉ skalpesh942@gmail.com | 🗄 KALPESH | 📖 BLOG | 🏠 HTB ELITE HACKER | 🌐  
PORTFOLIO | 🌐 LINKEDIN

## Education

---

<b>Government Engineering College Rajkot</b>	GTU
B.E. in Electronics and Communication Engineering	2021 - 2025
CGPA : 8.04	
<b>Government Engineering College Rajkot</b>	GTU
Specialization in IoT	2021 - 2025
<b>Jawahar Navodaya Vidyalaya Anand</b>	2021
12th Science (PCM) CBSE	78.80%
<b>Jawahar Navodaya Vidyalaya Anand</b>	2019
10th CBSE	74.00%

## Experience

---

**Embedded Linux BSP Engineer** Mantra Softech India Pvt. Ltd. May 2025 - Present

- BSP development and board bring-up on NXP i.MX6 and i.MX8MP platforms using Yocto Project / OpenEmbedded build system.
- Developed and maintained custom Yocto layers, recipes, and machine configurations for production-grade embedded Linux images.
- GStreamer quad-camera pipeline development on i.MX8MP using imxcompositor\_g2d hardware compositing (G2D/GPU accelerated).
- Firmware development for peripheral drivers: I2C, SPI, UART, Wiegand; debugged kernel-space EBUSY and one-shot latching issues.
- Li-Po battery fuel-gauge firmware using 12-bit ADC with hysteresis-based percentage tracking for charge/discharge state transitions.
- U-Boot customization, Device Tree (DTS) modifications, and systemd service integration on embedded Linux targets.

**Research Trainee** SPACE APPLICATIONS CENTRE, ISRO 07 Jan 2025 - 16 April 2025

- A part of the research project of developing Ferrite Microstrip Circulator at Ka Band. Which is an important part of the Navigation and Communication Payload, is designed for the future satellite project of ISRO.
- The internship opportunity I had with SAC ISRO was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be part of it. I am also grateful for having a chance to meet so many wonderful people and professionals who led me through this internship period.
- 100% Achieved the result

**Embedded Systems Engineer** Agastya Electronics and IT solutions 16/06/2024 - 16/07/2024

- Developed an innovative, Digital Weigh Scale using STM32F103C8T6. Developed an advanced digital weighing scale using the STM32F103C8T6 microcontroller and HX711 load cell amplifier for accurate weight measurement. Implemented calibration algorithms to ensure precise readings and efficient real-time weight display
- It was very good experience because I learned many stuffs, working environment and owner, manager and colleagues are very supportive.
- 100% Achieved the result
- 📁 [PROJECT](#)

## Projects

---

**UART-Tools — Serial Exploitation & Embedded Debug Framework**

- **Hardware Pentesting & Debug Toolkit:** Developed a comprehensive Bash-based toolkit for UART/serial interface interaction on embedded targets (Raspberry Pi, STM32, ESP32, Arduino, PLCs, industrial equipment).
- **Modules:** time-sync, file-transfer (XMODEM/YMODEM/ZMODEM), remote shell (rce.sh), firmware flasher (fw-update.sh), AT command controller, traffic logger, and line-level file editor — all accessible via a unified menu interface.
- **AT Command Control:** AT.sh supports SIM/modem enumeration, SMS read/send, GPS tracking, signal quality monitoring, and custom AT command injection for IoT/cellular devices (SIMCom A76XX, ESP8266/ESP32).
- [Github: UART-Tools](#)

### ProjectFlow — Project Management System with Facial ID Authentication

- **Biometric Authentication:** Full-stack web application featuring facial recognition login using HOG face detection and CNN 128-dimensional face encoding (dlib/face\_recognition library), with 0.4 tolerance and 50% confidence threshold for biometric-grade security.
- **Security Features:** CSRF protection, bcrypt password hashing, rate limiting, secure session management, audit logging, and HTTP security headers (HSTS, CSP, X-Frame-Options).
- **Stack & Deployment:** Python, Flask, SQLAlchemy, OpenCV, JavaScript; containerized with Docker/Docker Compose; deployable to Render, Heroku, Railway, or self-hosted.
- [Github: ProjectFlow](#)

### Mechanism to Prevent Road Accidents Between Vehicles

- **Advanced Collision Avoidance:** Promote safer roads and reduce accidents with cutting-edge technology like LiDAR, radar, and cameras. Integrate these sensors (ultra sonic) with powerful processors for real-time analysis and potential interventions (automatic braking, warnings) while adhering to safety regulations.

### Intelligent Glasses for Blinds using Raspberry Pi

- **Intelligent Glasses:** Engineered an assistive device utilizing Raspberry Pi, ultrasonic sensors, and computer vision algorithms with OpenCV for obstacle detection and real-time audio feedback via Text-to-Speech (TTS) integration. Delivered an efficient, embedded system to enhance navigation for visually impaired users.

### Wireless Data Transmission NodeMcu to Arduino Uno

- **Over The Air:** Developed a wireless communication system utilizing NodeMCU and Arduino Uno with OTA (Over-The-Air) updates. Enabled seamless data transmission and real-time integration using ESP8266 Wi-Fi for efficient IoT applications.

### Programming autonomous systems

- Designed and implemented algorithms for autonomous systems, focusing on sensor integration, decision-making, and real-time navigation. Utilized frameworks like ROS and microcontrollers to achieve precision, adaptability, and efficient task execution in dynamic environments.

### Build a Smart Irrigation System using Raspberry Pi

- **Effortless Plant Care:** Automate watering with an Arduino microcontroller, a soil moisture sensor, and a water pump for healthy plants without overwatering.

### Robotics

- **Robots:** Developed and programmed robotic systems integrating sensors, actuators, and microcontrollers for autonomous operations. Focused on real-time control, path planning, and object detection using frameworks like ROS and OpenCV to enhance functionality and precision.

### Shieldme Anti-Theft Android App

- **Track-it-Even-it-is-off:** Shieldme Security offers the unique feature of Fake Shutdown as part of Anti-Thief which actually allows you to not only track your lost phone location, but also retrieve surrounding images, audio or video files to help with police investigation. Including Features Fake Shutdown, Intruder Alerts, Lost Phone Tracking, Fake Airplane Mode, Emergency SOS, Low Battery Alerts.

### SPARKY-VPN / xploitoverload — Self-Hosted VPN Infrastructure

- **Multi-Protocol VPN Stack:** Self-hosted VPN and tunneling server on Oracle Cloud (ARM VM.Standard.A1.Flex, Mumbai region) running Xray, SSLH, Nginx, Stunnel4, OpenVPN, Dropbear, BadVPN UDPGW, and SSH WebSocket.
- **Automated SSL & Deployment:** Certificate management via acme.sh with Cloudflare DNS challenge; full systemd service orchestration via AutoScriptXray; ECC cert with auto-renewal.

## Awards and Honors

---

<b>SPARK EVENT WINNER, <i>CollegeCompetetion</i></b>	2024
<b>SSIP HACKATHON 2022</b>	2022
<b>AKERVA, <i>HTBAkervaminiprolabpwned</i></b>	2025 (HTB)
<b>SOLAR, <i>HTBSOLARminiprolabpwned</i></b>	2025 (HTB)
<b>JET, <i>JETfortresspwned(7Flagsowned)</i></b>	2025 (HTB)
<b>CONTEXT, <i>CONTEXTfortresspwned(10flagsowned)</i></b>	2025 (HTB)
<b>FARADY, <i>FARADAYfortresspwned(10flagsowned)</i></b>	2025 (HTB)
<b>AWS, <i>AWSfortresspwned(10flagsowned)</i></b>	2025 (HTB)
<b>SYNCACTIVE, <i>SYNCACTIVEfortresspwned(11flags)</i></b>	2025 (HTB)
<b>HTB Global Rank</b>	46th
<b>HTB India Rank</b>	6th
<b>HTB Season 10 Holo Tier — Rank #153</b>	2026 (HTB)

## Skills

---

**Programming Languages:**  Python,  JavaScript,  C,  C++,  Java,  php,  sql,  Bash,  PowerShell,  vhdl,  verilog

**Embedded & BSP:** NXP i.MX6, NXP i.MX8MP, Yocto Project, OpenEmbedded, U-Boot, Device Tree (DTS/DTSI), GStreamer, Linux Kernel Drivers, systemd, STM32, ESP32/ESP8266, Arduino, Raspberry Pi, NodeMCU

**Protocols & Interfaces:** UART/RS-232, I2C, SPI, Wiegand, JTAG, SWD, USB, AT Commands, XMODEM/YMODEM/ZMODEM, OTA (Over-The-Air)

**Tools and Frameworks:** Linux, Sliver C2, Cobalt Strike, Metasploit Framework, Havoc C2, Mythic, BloodHound CE, Ghidra, IDA Pro, MT Manager, Reverse Engineering Tools, GitHub, VS Code, HFSS, CST Studio, Hexo, Proteus, Android Studio, Arduino IDE, STM32 Cube IDE, ESP8266, ESP32Cam, Arduino Boards, Raspberry Pi, NodeMCU Flasher, ~~LaTeX~~, MS Office, Docker, Nginx, Oracle Cloud, Cloudflare

**Red Team & C2:** Sliver C2 (beacon modes, implant generation, HTTPS/DNS/mTLS C2), Cobalt Strike, Havoc C2, Metasploit / Meterpreter, Mythic, Covenant

**Active Directory:** Rubeus (Kerberoasting, AS-REP Roasting, RBCD, Golden/Silver Ticket, KeyList Attack), impacket (secretsdump, psexec, wmiexec, getTGT, smbclient), bloodyAD, certipy (AD CS / ESC attacks), CrackMapExec / NetExec, Responder (LLMNR/NBT-NS poisoning, NTLMv2 capture), evil-winrm

**Web & Network:** Burp Suite, sqlmap, ffuf, feroxbuster, Nuclei, Nmap, Masscan, Subfinder, amass, Nikto, BeEF

**Post-Exploitation & Pivoting:** Ligolo-ng, Chisel, socat, pwncat, Mimikatz, LaZagne

**Password Attacks:** Hashcat, John the Ripper, Hydra, Medusa, CeWL

**Android RE & Mobile:** jadx, apktool, Frida, objection, PCAPdroid, MobSF, adb, UIAutomator

**Forensics & Firmware RE:** Binwalk, Volatility, strings, ltrace, strace, file, hexdump

**Cyber Security:** Network Penetration Testing | Vulnerability Scanning | Information Gathering | Active Directory Exploitation | Pre & Exploitation | Android and PC hacking | Game Hacking Online and Offline | Offensive Security | IDORs | WAP | CSRF | SSRF | Password Spraying | Virtualization | HTB Player | Red Teaming | C2 Infrastructure | Lateral Movement | Privilege Escalation | Firmware Analysis | Mobile Application Security | OSINT

**Languages:** *Gujarati(native), Hindi(proficient), English(proficient)*