CYBERSECURITY & IOT

S.No	Problem Statement	Why This Problem Matters (Description)
1️⃣	**Quantum-Resistant Cybersecurity for Smart Cities 🆕**	Quantum computing threatens traditional encryption. Cities using IoT for utilities, transport, and governance must prepare with future-proof protection.
2️⃣	**Cybersecurity for Space Tech & Satellite Infrastructure 🆕**	Satellite systems are vulnerable to spoofing, jamming, and cyberattacks. Protecting space assets is vital for communication, defense, and navigation.
3️⃣	**Bio-Digital Identity Vault with Blockchain ☑**	Biometric data breaches are irreversible. A decentralized vault to store and secure bio-data with blockchain ensures digital sovereignty.
4️⃣	**Dark Web Threat Intelligence Engine ☑**	Critical threats originate from the dark web. A scraper + NLP-powered analyzer can detect early signs of cybercrime, drug trade, and cyberterrorism.
5️⃣	**IoT Disaster-Rescue Drone Mesh Network ☑**	In post-disaster zones, centralized comms fail. Drones forming a self-sustaining IoT network can find survivors and relay distress signals.
6️⃣	**Post-Quantum Voting System with Secure Contracts ☑**	Elections need trust. A quantum-resistant, blockchain-based voting platform ensures vote integrity and voter privacy even in future-proof threats.
7️⃣	**AI-Powered Behavioral Authentication System 🆕**	Traditional passwords are weak. Continuous biometric + behavior-based access (typing pattern, gait, voice) offers enhanced, invisible security.
8️⃣	**Zero-Day Threat Detection Simulator 🆕**	Zero-day exploits bypass known defenses. An AI-based simulation engine that mimics attack patterns can help pre-train systems against the unknown.

9️⃣	**Secure IoT Device Lifecycle Manager 🆕**	IoT devices are often unsecured after deployment. A system to track, update, and revoke access to edge devices prevents mass botnet risks.
🔟	**AI-Powered Phishing Simulation & Detection Extension ☑**	Phishing is the top entry point for attacks. A browser extension that simulates phishing attacks and educates users in real-time enhances resilience.
1️⃣1️⃣	**Ethical Hacking Evaluator Bot ☑**	Universities and companies often lack objective code audits. A bot that evaluates submissions for ethics, plagiarism, and bias can standardize trust.
1️⃣2️⃣	**AI Cyberbullying & Toxic Content Detector ☑**	Online abuse damages mental health. NLP-driven tools that flag harmful content in real time can prevent harm across social platforms.
1️⃣3️⃣	**Secure IoT Home Network Intrusion Monitor ☑**	Home automation often opens the door to attacks. A system to detect traffic anomalies and trigger alerts secures personal networks.
1️⃣4️⃣	**Blockchain-Backed Digital Identity & Reputation System 🆕**	Digital identities lack trust layers. A blockchain-backed system that verifies credentials, achievements, and online behavior can restore trust online.
1️⃣5️⃣	**Cybersecurity Dashboard for Renewable Energy Grids 🆕**	Renewable grids rely on connected systems. A dashboard to detect and respond to attacks in wind, solar, and smart grids can prevent national-scale outages.