

01 Outage Investigator

Network incident root-cause analysis

DOMAIN	Cybersecurity · Network observability · Incident response
THE PROBLEM	When a large digital service becomes unavailable, the cause may be a network failure, misconfiguration, compromised account, overloaded component or cascading dependency failure. Operators need to distinguish symptoms from root causes quickly.
THE CHALLENGE	Build an incident investigation platform that ingests simulated network events, application logs and service health data, correlates related failures, reconstructs an incident timeline and recommends containment actions.
WHY IT'S HARD	The system must distinguish correlated events from plausible root causes and provide evidence for its conclusions. Teams can use deterministic rules and graph analysis; AI is optional.

02 Selective-Disclosure Digital ID

Verifiable credentials that prove a claim without revealing the document

DOMAIN	Cybersecurity · Privacy · Digital identity
THE PROBLEM	Proving you are over 18, a student or eligible for a service usually means handing over a full ID document containing far more than the verifier needs.
THE CHALLENGE	Build a verifiable credential system that lets users prove selected claims while minimising disclosure, and that supports expiry and revocation.
WHY IT'S HARD	The system must resist forged credentials, replayed proofs and unauthorised verification. Teams must clearly explain the trust assumptions behind their design. Core techniques: public-key cryptography, digital signatures, selective disclosure, optionally zero-knowledge proofs.

03 Continuous Session Authentication

Risk-based identity verification beyond the login

DOMAIN	Cybersecurity · Authentication · Machine learning
THE PROBLEM	Passwords and OTPs are phished, leaked or SIM-swapped, and once a user logs in, the session is trusted blindly. Account takeovers often go undetected until money or data is gone.
THE CHALLENGE	Design a continuous authentication system that verifies users throughout a session using behavioural signals such as typing rhythm, navigation style and device context. It should produce a risk score, trigger step-up verification and give administrators a monitoring dashboard.
WHY IT'S HARD	Behavioural data is itself sensitive, so privacy must be protected. The system must handle legitimate changes (a new device, an injured hand) without locking out real users, while staying robust against an attacker who tries to mimic the user.

04 Deepfake Detection & Takedown Tracker

Detect manipulated media, trace its spread, speed up removal

DOMAIN	Trust & safety · Media forensics · Content provenance
THE PROBLEM	Deepfakes spread across platforms faster than they can be verified, flagged or removed. Victims face a slow, manual takedown process across many sites, and copies keep reappearing.
THE CHALLENGE	Build a system that detects likely manipulated media, tracks its spread across copies and re-uploads, and helps victims file takedown requests efficiently.
WHY IT'S HARD	Detectors are imperfect, so the system needs confidence levels, an appeal path for wrongly flagged content, and a way to prove authenticity at the source. Core techniques: perceptual hashing, similarity search, provenance metadata.

05 Smart Microgrid Energy Scheduler

Real-time energy optimisation for campuses, factories and housing societies

DOMAIN	Smart energy · IoT · Optimisation
THE PROBLEM	Campuses, factories and housing societies are adding solar panels, batteries and EV chargers, but without coordination they still draw peak grid power at peak prices.
THE CHALLENGE	Design a scheduler that decides in real time when to charge, discharge, shift loads or sell energy back, using forecasts of demand, generation and tariffs.
WHY IT'S HARD	Forecasts are always wrong, batteries degrade with use, and critical loads must never be dropped. The system must stay robust under uncertainty and be tested in simulation. Core techniques: optimisation under uncertainty, forecasting.

06 Fictional City Simulator

An interactive digital twin of a city that doesn't exist

DOMAIN	Simulation · Complex systems · Optimisation
THE PROBLEM	Can you build a digital world that behaves realistically enough to experiment with decisions before making them in real life? Policy changes such as new bus schedules or a flooded road have knock-on effects planners struggle to foresee.
THE CHALLENGE	Teams receive specifications for a fictional city with residents, transport networks, businesses, utilities and limited public resources. Build an interactive simulation in which changes to one part of the city affect other parts, for example transport schedules affecting commuter flows, congestion, travel times and demand for other services.
WHY IT'S HARD	Judges introduce a policy change or unexpected event, and teams must use their simulation to predict the consequences and compare possible responses. The test is whether the model represents meaningful interactions between systems, or is just a collection of unrelated charts.

Explore all problem statements & get the PPT template

<https://awsevents.dbit.edu.in/afterhours-1.0/>