IEEE BAU COMPUTER SOCIETY

CIPHER

Network detection and response

IEEE COMPUTER SOCIETY

TECHNICAL SHEET / 2026

A security prototype for small offices, shops, and schools. CIPHER learns each device's normal traffic pattern, flags unusual behavior, and explains the evidence so an operator can choose a response.

FROM NETWORK TRAFFIC TO OPERATOR ACTION

01 OBSERVE
Linux router
eBPF / XDP
Traffic hook

→

02 SUMMARIZE
Rust sensor
Sampled traffic
metadata

→

03 ANALYZE
Rust server
Statistics +
AI review

→

04 RESPOND
Web dashboard
Review +
device control

FlatBuffers reports over a TLS WebSocket · Axum server · SQLite persistence

How detection works

50 reports per device establish a baseline of normal activity.

Four signals: incoming bytes, outgoing bytes, dropped events, and port entropy (how varied port use is).

Statistics flag the change. An optional AI reviewer explains the evidence and recommends a response.

Measurements are sampled observations. An anomaly is a reason to investigate, not proof of an attack.

Operator control

Monitor and alert is the default. Operators can trust devices, review incidents, and manually isolate or restore a device.

Cloud auto-isolation requires enforcement mode, an untrusted device, at least two abnormal signals, and a valid block recommendation scored at least 85/100. The incident must remain open and policy unchanged.

The score is the model's own assessment, not a measured probability.

Local edge rules are separate. Monitor mode does not disable packet filters or clear existing blocks.

PROTOTYPE AND DEMO

Working software: detection, incident review, saved baselines, trust controls, acknowledgments, and retries.

Booth demo: simulated sensor and scripted reviewer with the real backend; no live packet blocking. Hardware enforcement and detection accuracy still need validation.

The Four Horsemen · @ieee_bau_cs

Zakaria Alqarra · Belal Hamdan
Raneem Abdullah · Ayham Idais
Contributor: Omar Eid
belalhamdan.com/cipher/

IEEE Al-balqa Applied University
Faculty of Engineering Technology