Adaptive Contextual Trust (ACT)

Progressive Challenge Escalation

Instead of blocking users outright, the system applies progressive challenges based on the trust score.

This ensures that only suspicious or high-risk sessions face additional scrutiny.

Adaptive Trust Scoring

Each user session is assigned a dynamic "trust score" based on the contextual fingerprint and behavioral analysis.

Collaborative Threat Intelligence

The system integrates with a global threat intelligence network to share and receive real-time data about emerging threats.

This allows the system to proactively block known malicious IPs, devices, or behavioral patterns before they can cause harm.

Real-Time Behavioral Analysis

Machine learning models analyze patterns such as:

- Navigation flow (e.g., how users move through the site).
- Interaction timing (e.g., time between clicks or keystrokes).
- Session duration and activity intensity.

Decoy Architecture

The system deploys invisible decoy elements (e.g., hidden links, fake API endpoints) within the application.

This provides an additional layer of detection without impacting user experience.

Contextual Fingerprinting

The system passively collects contextual data about the user's device, network, and behavior.

This data is used to create a unique "contextual fingerprint" for each user session.

The ***Adaptive Contextual Trust (ACT)*** replaces rigid zero trust with a dynamic, context-based model that assesses user trustworthiness in real time.

It blocks malicious traffic while ensuring a frictionless experience for legitimate users—no challenges or interaction required.