Adaptive Zero Trust Model with Context-Aware Trust Scoring for Heterogeneous IoT

Outline

1. **Architectural Design**
   - Micro-segmentation to isolate network segments for improved security.
   - Software-defined networking (SDN) for programmable, flexible management.
   - Centralized management to oversee all IoT devices and security policies.
   - Integration with a context collector to gather real-time data and feed a trust scoring mechanism.
2. **Trust Computation and Scoring**
   - Trusted computation engine analyzes contextual inputs.
   - Use of Blockchain for secure, transparent, and tamper-evident trust records.
   - Regularly updates trust scores based on device behavior, context, and history.
3. **Policy Enforcement Engine**
   - Applies dynamic security policies based on trust scores.
   - Implements micro-segmentation: low-trust devices can be isolated automatically.
   - Feeds results into an evaluation process for ongoing system improvement.
4. **Device Join and Authentication**
   - Devices join through a secure connection.
   - Authentication via Access Control Server (ACS).
   - Each device is assigned an initial trust score upon joining the network.
5. **Data Collection and Monitoring**
   - Device context and behaviors are monitored using edge agents and SDN controllers.
   - Trust scores are computed continuously, factoring in behavior, context, and historical trends.
   - Efficient data collection enables rapid detection of anomalies.
6. **Dynamic Policy Enforcement**
   - SDN controller can dynamically reprogram network flows in response to trust evaluations.
   - Security policies are adaptive and can change as trust scores evolve.
   - Continuous monitoring assures real-time responsiveness.
7. **Multi-Layered System Structure**
   - **SDN Controller Layer:** Central decision and policy management.
   - **SDN Layer:** Enforces network flow rules and micro-segmentation based on trust.
   - **Edge Gateway (G/W) Layer:**
     - Performs lightweight anomaly detection with TinyML models.
     - Collects contextual metadata (location, time, behavior).

- **Gateway (G/W):** Protocol integration (e.g., Zigbee, LoRa) for heterogeneous device connectivity.
- **IoT Devices:** Diverse endpoint sensors/actuators in the system.

8. **Process Workflow**

   8.1. Device connects and is authenticated (via ACS).

   8.2. Initial trust score is assigned.

   8.3. Device context and behavior are monitored.

   8.4. Trust score is computed based on updated context.

   8.5. SDN controller and policy enforcement engine reprogram the network if trust score changes.

   8.6. Continuous monitoring to adjust trust and respond to anomalies in real-time.

9. **Assumptions**

   - System evaluated with various network/mobility settings (N/M, S/M).
   - Designed for heterogeneous protocols and device types.

10. **Related Work**

    - Note to reference relevant papers for implementation guidance and benchmarking.