FIGURE 3: Edge Computing Behavioral Cryptography Workflow

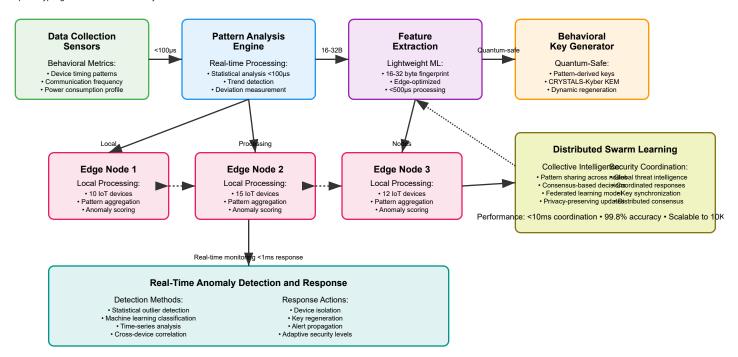ction <500µs • Crypto generation <1ms • Memory <1KB • Power <1mW

Data Collection Sensors

Behavioral Metrics:
• Device timing patterns
• Communication frequency
• Power consumption profile

<100µs →

Pattern Analysis Engine

Real-time Processing:
• Statistical analysis <100µs
• Trend detection
• Deviation measurement

16-32B →

Feature Extraction

Lightweight ML:
• 16-32 byte fingerprint
• Edge-optimized
• <500µs processing

Quantum-safe →

Behavioral Key Generator

Quantum-Safe:
• Pattern-derived keys
• CRYSTALS-Kyber KEM
• Dynamic regeneration

Local

Processing

Nodes

Edge Node 1

Local Processing:
• 10 IoT devices
• Pattern aggregation
• Anomaly scoring

Edge Node 2

Local Processing:
• 15 IoT devices
• Pattern aggregation
• Anomaly scoring

Edge Node 3

Local Processing:
• 12 IoT devices
• Pattern aggregation
• Anomaly scoring

Distributed Swarm Learning

Collective Intelligence: / Security Coordination:
• Pattern sharing across nodes / • Global threat intelligence
• Consensus-based decisions / • Coordinated responses
• Federated learning models / • Key synchronization
• Privacy-preserving updates / • Distributed consensus

Performance: <10ms coordination • 99.8% accuracy • Scalable to 10K

Real-time monitoring <1ms response

Real-Time Anomaly Detection and Response

Detection Methods:
• Statistical outlier detection
• Machine learning classification
• Time-series analysis
• Cross-device correlation

Response Actions:
• Device isolation
• Key regeneration
• Alert propagation
• Adaptive security levels

Behavioral Pattern Recognition Examples

Normal Behavior

Pattern Profile:
• Transmission: Every 30s±5s
• Power: 15-20mA active
• Data size: 32±8 bytes
• Response time: 5-10ms
• Confidence: 98.2%

Suspicious Behavior

Anomaly Indicators:
• Transmission: Irregular
• Power: 25-30mA spike
• Data size: 128+ bytes
• Response: >50ms delay
• Threat score: 7.2/10

Attack Patterns

Malicious Activity:
• Flooding attempts
• Timing manipulation
• Replay attacks
• Protocol violations
• Block immediately

Adaptive Learning

Continuous Updates:
• Model refinement
• Threshold adjustment
• Pattern evolution
• False positive reduction
• 24/7 learning cycle

Efficiency

Ultra-Low Impact:
• RAM: <1KB
• CPU: <5% load
• Power: <1mW
• Latency: <1ms
• Real-time