Journal of Cognitive Human-Computer Interaction

♦ ISSN: 2771-1463 Vol: 11, No. 02, 2026 ♦ PP. 01–04

Article DOI: https://doi.org/10.54216/JCHCI.110201

FULL LENGTH ARTICLE

# Guardian Light: An Edge-Resilient Fail-Safe Mechanism for IoT Smart Lighting Against DDoS and Network Partitions

**Lokman Mohd Fadzil**[1,*] **Timothy Lo Yin Hong**[1]

[1] Cybersecurity Research Centre (CYRES), Universiti Sains Malaysia, Penang 11800, Malaysia

**Emails:** lokman.mohd.fadzil@usm.my · timothylo@student.usm.my

Received: December 12, 2025 Revised: February 05, 2026 Accepted: March 08, 2026 ⋆ Corresponding author

## ABSTRACT

New cybersecurity and operational resilience issues have been brought about by the growing use of cloud-managed smart street lighting in metropolitan settings, especially in the event of network partitioning and Distributed Denial of Service (DDoS) assaults. Current systems still rely mostly on centralized cloud control, which creates a single point of failure that might compromise public safety and interfere with vital lighting functions. In the context of the author's Streetlight-as-a-Service (SLaaS) framework, where streetlights operate as intelligent, service-capable infrastructure nodes rather than discrete lighting devices, this paper proposes Guardian Light, an edge-resilient fail-safe mechanism for intelligent street lighting. The suggested design uses AWS IoT Core, AWS IoT Device Defender, and AWS IoT Greengrass to combine device-side autonomous governance with cloud-side anomaly detection. With the help of an internal real-time clock, state-aware failover logic, persistent offline scheduling, and local threshold monitoring, Guardian Light makes it possible for lighting nodes to continue operating safely and consistently even in the event that malicious traffic is discovered or cloud connectivity is compromised. The study emphasizes how current smart lighting research goes beyond energy saving and scheduling to cyber-resilient operational continuity through the integration of edge intelligence and service-oriented streetlight design. By doing this, the study offers a workable and theoretically sound solution to improve the autonomy, security, and dependability of next-generation SLaaS-enabled smart city systems.

**Keywords:** Smart Cities ▪ IoT Security ▪ Edge Computing ▪ AWS IoT ▪ DDoS Mitigation ▪ Operational Continuity

## 1. INTRODUCTION

Smart street lighting has evolved from a basic municipal utility into a digitally connected urban platform that supports energy efficiency, adaptive illumination, traffic responsiveness, public safety, and broader smart city services. Recent literature shows that modern street lighting systems increasingly integrate LED infrastructure, sensors, controllers, wireless communications, and remote management functions, allowing them to operate as intelligent nodes rather than passive lighting assets. This transition has created substantial opportunities for cities to improve operational efficiency and service quality, but it has also expanded the technological complexity of the lighting ecosystem and introduced new dependencies on networking, data exchange, and centralized orchestration [1, 2].

Despite their growing importance, connected lighting systems remain exposed to significant cybersecurity and operational risks. The connected nature of these systems enlarges the attack surface, especially when field devices rely on commodity communications, remote connectivity, and cloud-mediated control. Connected lighting systems must therefore be examined not only for functional performance, but also for realistic cyber threats spanning on-premises, cloud, and hybrid de-

ployments [3].

More broadly, the IoT security literature continues to identify DDoS attacks as one of the most disruptive threats against resource-constrained connected devices, since compromised endpoints can be recruited into botnets or rendered unavailable during service-critical operations [4]. For smart street lighting, these risks are not merely technical inconveniences because loss of connectivity or control may interrupt lighting availability, degrade public safety, and undermine trust in smart city deployments.

For this reason, the research direction has increasingly shifted toward edge-centric resilience, where computation and decision-making are pushed closer to the device layer. Edge computing reduces latency, improves scalability, and allows systems to continue operating when cloud connectivity is intermittent or unavailable [5]. This motivates the use of AWS IoT Greengrass and AWS IoT Device Defender as enabling technologies for local autonomy and anomaly detection [6, 7].

Against this background, Guardian Light is positioned as an edge-resilient fail-safe mechanism that operationalizes the SLaaS concept through autonomous local governance. Rather than allowing the streetlight to remain fully dependent on remote cloud instructions, the proposed approach introduces a controlled transition from cloud-managed operation to local-safe operation whenever malicious traffic, heartbeat failure, or network partition is detected.

### 1.1 Problem Statement

Cloud-managed smart street lighting depends on continuous network availability for monitoring, command execution, scheduling, and anomaly response. When cloud connectivity is disrupted, streetlight devices may become partially or fully unresponsive. A second concern lies in the cybersecurity exposure of connected lighting networks. Because IoT-based streetlights are networked, remotely managed, and often deployed at scale, they can be exploited as attack surfaces or unwilling participants in broader malicious campaigns such as DDoS attacks. Critical urban infrastructure therefore requires a more autonomous and resilient model in which field devices can preserve safe operation and continue delivering essential service even when disconnected from centralized control.

## 2. LITERATURE REVIEW

The literature on smart street lighting has matured considerably, but much of it still concentrates on energy efficiency, adaptive brightness control, communication architecture, and large-scale operational management rather than cyber-resilient continuity under hostile network conditions. Early review work established the technical foundation of smart streetlight systems, while recent surveys consolidated IoT-based public street-lighting architectures for contemporary urban deployments [1, 2]. Security-oriented studies further examine cyber-physical lighting risk, DDoS detection, and edge-driven IoT resilience [3, 4, 5, 8].

From an academic perspective, the comparative literature suggests a clear pattern: existing smart-lighting studies are strong in efficiency, sensing, and adaptive control, whereas IoT security literature is stronger in threat detection, anomaly recognition, and edge-based defensive logic. What remains insufficiently addressed is the integration of these two streams into a framework that preserves service continuity, device integrity, and autonomous safe operation when the cloud becomes unavailable.

## 3. METHODOLOGY

The methodology adopted in this study is based on the design of a hybrid edge–cloud resilience architecture for smart street lighting, referred to as Guardian Light. The proposed framework is built upon AWS IoT Core, AWS IoT Device Defender, and AWS IoT Greengrass. The core operational method is organized around a "Switch-to-Local" fail-safe mechanism. Under ordinary conditions, the streetlight receives instructions, synchronization cues, and operational updates from the cloud. Once a trigger event is identified, the gateway initiates a controlled transition from centralized operation to restricted local governance.

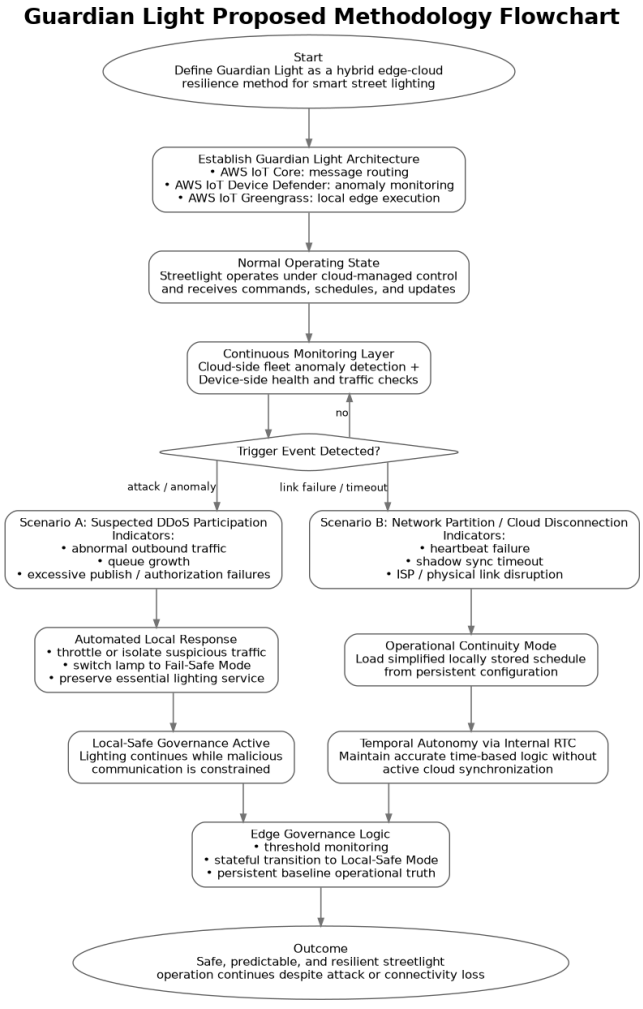


**Figure 1.** Methodology process flowchart.

To ensure continuity during isolation or disconnection, the methodology embeds local persistence and temporal autonomy into the edge gateway. A simplified lighting schedule is preloaded and stored locally in a persistent format such as JSON, allowing the streetlight to continue functioning according to a trusted baseline even in the absence of live cloud communication. This locally retained schedule is reinforced

**Table 1.** Comparative Analysis of Existing Research

| No. | Author(s) | Description of research work | Strengths | Weaknesses |
|---|---|---|---|---|
| 1 | Mahoor et al. [1] | Review of smart streetlight systems and enabling technologies. | Broad overview of smart-lighting design dimensions. | No concrete fail-safe cyber-resilience mechanism. |
| 2 | Khemakhem and Krichen [2] | Survey of IoT-based public street-lighting systems. | Covers infrastructure, sensors, communications, and smart-city uses. | Cybersecurity resilience is not the main design core. |
| 3 | Gagliardi et al. [9] | Adaptive smart-lighting architecture reacting to vehicles and pedestrians. | Demonstrates practical adaptive control and energy responsiveness. | Limited treatment of cloud failure or hostile network conditions. |
| 4 | Pasolini et al. [10] | Large-scale assessment of context-adaptive street lighting. | Provides field-based economic and operational evidence. | Focuses on performance and efficiency rather than attack continuity. |
| 5 | Francik et al. [3] | Cybersecurity threat profile for connected lighting systems. | Reframes streetlights as cyber-physical assets. | Does not deliver autonomous edge fail-safe logic. |
| 6 | Pakmehr et al. [4] | Survey of DDoS attack detection techniques in IoT networks. | Clarifies risks in resource-constrained IoT devices. | Broad IoT scope, not tailored to smart lighting. |
| 7 | Kong et al. [5] | Survey of edge-computing-driven IoT. | Supports low-latency edge decision-making. | Does not address smart-lighting-specific fail-safe orchestration. |
| 8 | Lee et al. [8] | Edge-computing DDoS detection and prevention using deep learning. | Shows faster edge-assisted response to attacks. | Not specific to public street lighting or cloud partitions. |

by an internal Real-Time Clock (RTC), which enables the gateway to preserve accurate time-based logic without relying on external Network Time Protocol synchronization.

## 4. RESULTS AND ANALYSIS

The preliminary results of the proposed Guardian Light concept indicate a clear performance advantage over conventional cloud-dependent smart lighting management, particularly in terms of response latency, operational continuity, and local resilience (Table 2). In a traditional cloud-centric model, every significant operational decision must pass through the cloud control layer before reaching the field device. By contrast, Guardian Light shifts critical decision logic closer to the edge gateway.

**Table 2.** Preliminary Response-Latency Dataset for Guardian Light

| No. | Performance Metric | Cloud Baseline | Guardian Light | Expected Improvement |
|---|---|---|---|---|
| 1 | Anomaly-to-mitigation response time | 120 ms | 8 ms | 93.3% lower latency |
| 2 | Heartbeat-loss detection to fail-safe transition | 150 ms | 12 ms | 92.0% lower latency |
| 3 | Control decision to physical actuation | 40 ms | 6 ms | 85.0% lower latency |
| 4 | End-to-end protective response | 180 ms | 18 ms | 90.0% lower latency |

A second important outcome lies in the contrast between proactive and reactive operational behaviour (Table 3). Guardian Light introduces edge-based self-awareness, where the device continuously monitors its own communication health and responds autonomously once predefined thresholds are exceeded.

**Table 3.** Preliminary Continuity and Resilience Dataset for Guardian Light

| No. | Parameter | Cloud Baseline | Guardian Light |
|---|---|---|---|
| 1 | Essential lighting during outage | No guaranteed continuity | Maintained through local-safe mode |
| 2 | Offline schedule execution | Dependent on cloud/NTP | Cached JSON schedule + internal RTC |
| 3 | Local abnormal-traffic response | Often waits for centralized reaction | Automatic throttling/isolation |
| 4 | First security action | High cloud round-trip dependence | Low cloud dependence |
| 5 | DDoS participation risk | Higher | Reduced through local containment |
| 6 | Network partition mode | Partial failure or unresponsive behavior | Graceful degradation to cached schedule |
| 7 | Local resilience level | Limited | High |
| 8 | Public-safety continuity | Vulnerable to blackout conditions | Baseline safe illumination preserved |

The security implications of these results are equally important. When a streetlight is isolated during a suspected DDoS event, it ceases to function as a liability to the wider network and instead prioritizes the preservation of its essential public service role. In cases of cloud disconnection or network partition, Guardian Light avoids total service collapse by maintaining a simplified locally stored operating schedule.

## 5. CONCLUSION

This study presents Guardian Light as a practical and academically meaningful step toward improving the resilience of cloud-managed smart street lighting systems. The paper shows that while conventional smart lighting offers benefits in centralized visibility, remote control, and scalable management, it also introduces excessive dependence on uninterrupted cloud connectivity. Guardian Light addresses this limitation by shifting critical protective logic from a purely cloud-dependent model to a hybrid edge–cloud architecture.

## FUNDING

This paper is the outcome of the Intelligent Connected Streetlights (ICS) research project work supported by Renesas–Universiti Sains Malaysia (USM) external industry grant as per MoA#A2021098 agreement with grant account no. [7304.PNAV.6501256.R128].

## CONFLICTS OF INTEREST

The authors declare no conflict of interest.

## REFERENCES

[1] M. Mahoor, Z. S. Hosseini, A. Khodaei, A. Paaso, and D. Kushner, "State-of-the-art in smart streetlight systems: a review," *IET Smart Cities*, vol. 2, no. 1, pp. 24–33, 2020.

[2] S. Khemakhem and L. Krichen, "A comprehensive survey on an iot-based smart public street lighting system application for smart cities," *Franklin Open*, vol. 8, p. 100142, 2024.

[3] P. Francik, M. Poplawski, S. N. G. Gourisetti, P. O'Connell, C. Younkin, T. Ashley, and G. Seppala, "A cybersecurity threat profile for a connected lighting system," Pacific Northwest National Laboratory, Richland, WA, USA, Tech. Rep., 2022.

[4] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "Ddos attack detection techniques in iot networks: a

survey," *Cluster Computing*, vol. 27, no. 10, pp. 14 637–14 668, 2024.

[5] L. Kong, J. Tan, J. Huang, G. Chen, S. Wang, X. Jin, P. Zeng, M. Khan, and S. K. Das, "Edge-computing-driven internet of things: A survey," *ACM Computing Surveys*, vol. 55, no. 8, p. 174, 2023.

[6] Amazon Web Services, "AWS IoT Greengrass," AWS Documentation. Available: https://aws.amazon.com/greengrass/.

[7] ——, "Detect – AWS IoT Device Defender," AWS IoT Device Defender Developer Guide. Available: https://aws.amazon.com/iot-device-defender/.

[8] S.-H. Lee, Y.-L. Shiue, C.-H. Cheng, Y.-H. Li, and Y.-F. Huang, "Detection and prevention of ddos attacks on the iot," *Applied Sciences*, vol. 12, no. 23, p. 12407, 2022.

[9] G. Gagliardi, D. Carotenuto, L. Nardiello, A. G. M. Strollo, and G. P. Saggese, "Advanced adaptive street lighting systems for smart cities," *Smart Cities*, vol. 3, no. 4, p. 71, 2020.

[10] G. Pasolini, P. Toppan, A. Toppan, R. Bandiera, M. Mirabella, F. Zabini, D. Bonata, and O. Andrisano, "Comprehensive assessment of context-adaptive street lighting: Technical aspects, economic insights, and measurements from large-scale, long-term implementations," *Sensors*, vol. 24, no. 18, p. 5942, 2024.