ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, July-December 2025, Submitted in July 2025

Cognitive Cryptographic Adaptation for Secure and Sustainable Internet of Things Communication

Sohail, Research Scholar, Computer Science Dept., Sikkim Alpine University, Kamrang, Sikkim
Dr. Sunil Gupta, Associate Professor, Computer Science Dept., Sikkim Alpine University, Kamrang, Sikkim

Abstract

The Internet of Things (IoT) is expanding into domains — smart cities, precision agriculture, remote healthcare, and environmental monitoring — where devices must remain secure for years while operating on scavenged or severely rationed energy. Static security configurations, whether fixed to a strong cipher or a lightweight one, cannot simultaneously satisfy the twin demands of persistent protection and long-term sustainability under such variable conditions. This paper introduces a Cognitive Cryptographic Adaptation (CCA) framework that borrows the sense–reason–act–learn cycle from cognitive radio and cognitive network engineering and applies it to cryptographic decision-making at the network edge. Rather than treating cryptographic selection as a fixed policy or a purely reactive threshold rule, CCA equips each device with a lightweight cognitive engine that perceives its operating environment (energy source type and harvesting rate, battery state, traffic criticality, and observed attack indicators), reasons over this perception using a fuzzy-rule knowledge base to estimate risk and sustainability pressure, acts by selecting a cryptographic configuration from a tiered cipher and key-length portfolio, and learns by reinforcing configurations that historically balanced protection and energy sustainability well. A distinguishing feature of the framework is its treatment of sustainability as a first-class objective alongside security and energy: nodes powered by renewable harvesting sources are cognitively permitted greater security headroom than battery-only nodes nearing depletion, and network-wide sustainability metrics such as harvested-to-consumed energy ratio and projected node survival are folded directly into the reasoning process. Simulation across solar-, vibration-, and battery-powered node populations shows that CCA sustains a security compliance rate above 96% while reducing energy consumption by 29–38% relative to fixed high-security baselines, and increases the proportion of nodes reaching full self-sustainability (harvested energy meeting or exceeding consumption) by roughly 45% compared to non-cognitive adaptive schemes. These findings suggest that embedding cognitive reasoning explicitly around sustainability, not merely energy minimization, yields IoT security architectures that are both resilient and durable over multi-year deployments.

Keywords: Cognitive Networks, Adaptive Cryptography, Sustainable IoT, Energy Harvesting, Fuzzy Inference, Green Security, Edge Intelligence, Resource-Constrained Devices

1. Introduction

Modern IoT devices range from gateways powered by mains electricity to millimeter-scale sensors that collect energy from the surrounding environment in the form of solar radiation, vibration, thermal gradients, or radio-frequency scavenging. This variety presents a challenge that can not be solved by implementing standard security measures; for example, a setup that works for a solar-powered node exposed to direct sunlight might not be viable for a battery-only node planted in dirt for an agricultural deployment that lasts for years, even though the two nodes may encounter similar hostile threats. Sustainability, defined as a device's ability to maintain adequate protection indefinitely within its actual energy budget and harvesting profile, is a more fundamental objective than energy minimization, according to this paper. To achieve sustainability, devices need to be able to cognitively reason about their operating context, not just react to instantaneous battery readings.

This paper borrows the term "cognitive" from the cognitive radio and cognitive network management traditions, wherein a system constantly senses its surroundings, reasons about the optimal action to take given imperfect and changing knowledge, takes action based on that

reasoning, and learns from its mistakes to make better decisions in the future. By incorporating this cycle of sense-making, reasoning-doing, and learning into cryptographic configuration selection, the suggested method stands out from exclusively threshold-based or exclusively learned adaptive schemes. Cognitive reasoning enables a device to make defendable and interpretable decisions in unexpected situations, surpassing the limitations of a threshold table, all while continuously improving through experience.

1.1 Motivation

Cognitive Cryptographic Adaptation (CCA) is a framework that this study proposes in response to three observations. To begin, the power sources used by nodes in an Internet of Things (IoT) deployment can vary greatly, ranging from mains power to batteries to energy harvesting. If a security scheme does not take this variation into account, it will either overprotect nodes that are rich in energy harvesting without providing enough protection or underprotect them out of an abundance of caution. A node that consumes just a little bit more energy than a minimal baseline but is still well within its harvested supply is more sustainable than one that saves energy nominally but quickly depletes a non-rechargeable battery. This is because sustainability, not raw energy savings, is the measure that determines whether a device remains securely operational for its intended service life. Thirdly, for embedded systems that are vital to safety and security but have strict rule tables that can not generalize and opaque deep learning rules that are hard to validate, cognitive, knowledge-based reasoning (like fuzzy inference) provides an auditable and transparent compromise.

1.2 Contributions

Presented in this paper are the following:

1. An extended formal treatment of energy-only trade-off formulations for sustainable cryptographic adaptation that takes into account long-term node survivability and energy-harvesting dynamics in addition to traditional approaches.
2. A cognitive cycle for cognitive cryptographic adaptation (CCA) was designed, with a core based on fuzzy logic reasoning and a lightweight reinforcement-based learning layer for continual refining. The framework was constructed around this cycle.
3. The type of harvesting source, fluctuation in harvesting rate, battery reserve, and traffic criticality are all factors that are taken into account by a knowledge base and cryptography portfolio that is concerned with sustainability.
4. The Harvest-to-Consumption Ratio (HCR) is a network-wide sustainability indicator that was utilized as an evaluation criterion and as a feedback signal within the cognitive reasoning loop.
5. An extensive simulation-based assessment comparing CCA to fixed-cipher and non-cognitive adaptive baselines, covering populations of nodes powered by solar, vibration, and batteries.

1.3 Paper Organization

In Section 2, we take a look at relevant research in cognitive networking and long-term Internet of Things security. We build the sustainability-aware system and the threat model in Section 3. The structure and cycle of the CCA framework—"sense-reason-act-learn"—are introduced in Section 4. In Section 5, we go over the learning layer and fuzzy reasoning core in detail. In Section 6, the experimental apparatus is detailed. Section 7 presents and delves into the findings. Section 8 examines the robustness of security systems. We cover the constraints in Section 9, and we wrap up with future directions in Section 10.

2. Related Work

2.1 Cognitive Radio and Cognitive Network Management

Instead of working with predetermined channel allocations, radios can now adjust their broadcast parameters based on what they observe in the spectrum thanks to the sense-reason-act-learn paradigm developed in cognitive radio research. By applying knowledge-based

reasoning engines that can function with partial environmental data, cognitive network management expanded this paradigm to address more generalized resource allocation issues, such as routing, congestion control, and quality-of-service management. This work takes its cues from that line of thinking by tackling the under-studied issue of cryptographic setup using the same cyclical reasoning framework.

2.2 Sustainable and Energy-Harvesting IoT Systems

There is a plethora of literature on energy-harvesting-aware system design, covering topics such as harvest-aware duty cycling, adaptive sampling rates linked to predicted harvesting yield, and energy-neutral operation policies that limit a device's average consumption to stay within its long-run harvested supply. This work seeks to fill a gap between sustainable systems engineering and adaptive security research by seeing security as a tunable parameter that can itself be modified to harvesting conditions, rather than an external, fixed cost, as most of the literature has done.

2.3 Fuzzy and Knowledge-Based Approaches to Network Security

The capacity of fuzzy inference systems to reason gracefully under the uncertain and imprecise measurements typical of embedded sensing has made them a valuable asset in several wireless sensor network applications, including intrusion detection, trust management, and access control. The reasoning core created in Section 5 is motivated by the fact that their usage for cryptographic configuration selection is largely unexplored, especially when combined with sustainability indicators generated from energy-harvesting telemetry.

2.4 Adaptive and Learning-Based Cryptographic Selection

On the other hand, previous studies on adaptive cryptographic selection have shown that, compared to static configurations, dynamically varying cryptographic strength according to context can reduce energy consumption. This includes threshold-based cipher switching and reinforcement-learning-driven policies. Two things set this paper apart from similar works: first, it uses an interpretable fuzzy reasoning core as its main decision mechanism, focusing on sustainability (the balance between harvested and consumed energy as well as the projected longevity of the device) instead of instantaneous energy minimization; second, it uses learning only to refine rule weights over time, not as an opaque end-to-end policy.

3. System and Threat Model

Heterogeneous Power-Sourcing Model

The network is modeled as a set of nodes N, each assigned one of three power-sourcing classes: Class H (harvesting-rich, e.g., solar nodes in favorable exposure), Class M (harvesting-moderate, e.g., vibration or intermittent RF scavenging), and Class B (battery-only, non-rechargeable). Each node maintains a rolling estimate of its harvesting rate $H_i(t)$ (mW), instantaneous battery state $B_i(t)$, and a derived sustainability horizon representing the projected number of days until battery exhaustion under current consumption and harvesting trends.

Harvest-to-Consumption Ratio

We define the Harvest-to-Consumption Ratio for node i over a window W as:

$$HCR_i = (\Sigma W H_i(t)\, dt) / (\Sigma W P_i(t)\, dt)$$

where $P_i(t)$ is total instantaneous power draw including cryptographic, sensing, and communication load. An HCR at or above 1.0 indicates energy-neutral or energy-positive operation — the node is fully sustainable at its current configuration — while an HCR below 1.0 indicates a depleting trajectory requiring either reduced consumption or an improved harvesting condition to avoid eventual exhaustion. HCR forms the central sustainability signal consumed by the cognitive reasoning core described in Section 5.

Traffic Criticality and Security Requirements

In this adaptive security study, we expand the sensitivity classification to include weight availability consequences; for instance, a Critical label is applied to actuator commands whose spoofing could cause physical harm, not just to messages carrying sensitive data; the

labels "Routine," "Elevated," and "Critical" reflect the operational consequence of compromise.

Threat Model

During the lifetime of the network, we presume that an adversary with limited computational resources can engage in passive eavesdropping, active packet injection and replay, and physical capture of a limited number of nodes. However, this adversary will not be able to crack correctly parameterized standard cryptographic primitives. In Section 8, we also considered a scenario where an adversary could indirectly force the cognitive engine toward lower-security configurations by manipulating the environment. This could involve shading a solar panel or suppressing a node's harvesting input, for example.

4. Cognitive Cryptographic Adaptation (CCA) Framework

4.1 Overview of the Sense–Reason–Act–Learn Cycle

At each node, the CCA framework arranges cryptographic decision-making as a continuous cognitive cycle, as conceptualized in Table 1. Nodes collect telemetry during the Sense phase, including harvesting rate, battery status, recent HCR, traffic criticality of the awaiting message, and any locally noticed abnormality indications such unusual traffic bursts or repeated authentication failures. After receiving this data, the Reason phase sends it to a fuzzy inference engine to determine the best level of security to implement. The Act step involves applying the suggested tier to the communication using a certain cryptographic portfolio cipher and key-length configuration. In the Learn phase, the reasoning core can improve its recommendations over successive cycles without retraining by adjusting rule confidence weights based on the outcome, which includes actual energy consumed, whether an anomaly followed the transmission, and the resulting HCR trend.

Table 1. The CCA sense–reason–act–learn cognitive cycle

Phase	Function	Key Inputs / Outputs
Sense	Gather environmental and device telemetry	Harvesting rate, battery state, HCR, traffic criticality, anomaly flags
Reason	Fuzzy inference over sustainability and risk	Linguistic rule evaluation → recommended security tier
Act	Apply cryptographic configuration	Cipher + key length selection; message encryption/authentication
Learn	Reinforce or adjust rule confidence	Observed energy cost, anomaly outcome, updated HCR trend

4.2 Cryptographic Portfolio and Security Tiers

You can find a summary of the four security tiers defined by the framework in Table 2. Each tier is associated with a unique cryptographic configuration that strikes a good balance between strength and computational cost. One immediate result of running the Reason phase is the assigning of tiers.

Table 2. Tiered cryptographic portfolio used by the CCA Act phase

Tier	Cipher / Configuration	Key Size	Energy Cost (µJ/block)	Intended Context
T1 — Minimal	SPECK-64/96 (reduced rounds)	96 bits	1.6	Routine data, high-sustainability nodes under stress
T2 — Standard	SPECK-64/128	128 bits	2.6	Routine to elevated data, moderate sustainability

T3 — Elevated	AES-128-GCM	128 bits	5.4	Elevated criticality or degraded HCR trend
T4 — Maximum	AES-256-GCM + ECDSA-P256	256 / 256 bits	8.1 / 41.2	Critical commands, active anomaly indicators

4.3 Deployment Topology

To keep the program memory footprint under a few kilobytes, each end node hosts a lightweight instance of the Sense, Reason, and Act phases. Running the computationally intensive Learn phase at an edge gateway with aggregated, privacy-preserving summaries of node outcomes and pushing updated rule weights back to nodes during low-traffic maintenance windows minimizes the runtime footprint per node while still taking advantage of network-wide learning.

5. Fuzzy Reasoning Core and Learning Layer

5.1 Linguistic Variables

After processing four fuzzy input variables—Battery State (Low, Medium, High), HCR Trend (Depleting, Stable, Surplus), Traffic Criticality (Routine, Elevated, Critical), and Anomaly Signal (None, Suspicious, Active)—the Reason phase generates a single fuzzy output variable, Security Tier. The linguistic values of this variable correspond to the four levels provided in Table 2. To prevent fast, energy-wasting oscillation between cipher configurations, membership functions for continuous inputs (battery status, HCR) are defined as overlapping trapezoidal functions. This prevents abrupt threshold leaps and ensures smooth transitions between tiers.

5.2 Representative Rule Base

Based on the notion that active threat indicators take precedence over sustainability pressure, the rule base incorporates expert-defined heuristics like: IF Anomaly Signal is Active THEN Security Tier is Maximum, irrespective of battery or HCR condition. On the flip side, a node that is actually close to dying can save power for regular traffic if the security tier is minimal, the battery is low, and the HCR trend is dwindling. Table 3 shows a subset of the roughly forty principles of this type that make up the foundational knowledge.

Table 3. Representative subset of the fuzzy rule base governing tier selection

Battery State	HCR Trend	Criticality	Anomaly	Resulting Tier
Low	Depleting	Routine	None	Minimal
Medium	Stable	Elevated	None	Standard
High	Surplus	Routine	None	Standard
Any	Any	Critical	None	Elevated (min.)
Any	Any	Any	Active	Maximum
Low	Depleting	Critical	Suspicious	Elevated

5.3 Defuzzification and Tier Selection

We use the center-of-gravity defuzzification approach to aggregate the rule outputs and get a continuous tier score. For the Act-phase execution, we round it to the nearest discrete tier. While still producing a tangible, implementable cryptographic judgment, this maintains the advantage of smooth, graded reasoning during the inference step.

5.4 Confidence-Weighted Learning

With a uniform initialization and adjustments during the Learn phase based on the observed outcomes of decisions that that rule significantly impacted, each rule has a confidence weight. The weight of rules that caused configurations to maintain a positive HCR trend incident-free has been somewhat raised, whereas the weight of rules that caused configurations to later be

linked with security incidents has been drastically reduced. The knowledge base can adapt to the real-world conditions of a specific deployment over time using confidence-weighted adjustment, a simplified version of reinforcement learning that is applied to rule strength instead of a full action-value table. What is more, the underlying rule structure remains interpretable, so an operator can always check which rules are trusted and why.

6. Experimental Setup

Our simulations included a network of 300 nodes spread out among the three power-sourcing classes mentioned in Section 3. The nodes in Class H and Class M were subject to diurnal and stochastic weather-driven harvesting variation, while the nodes in Class B were battery-only. The network operated over a 180-day deployment horizon. Important parameters used in the simulation are summarized in Table 4.

Table 4. Simulation configuration for CCA evaluation

Parameter	Value / Range	Notes
Node population	300 (120 H / 90 M / 90 B)	Mixed power-sourcing classes
Simulation horizon	180 simulated days	Includes diurnal and stochastic harvesting variation
Solar harvesting rate (Class H)	0.5 – 12 mW	Diurnal profile with weather noise
Vibration/RF harvesting (Class M)	0.05 – 1.5 mW	Intermittent, bursty availability
Initial battery (Class B)	800 mAh	Non-rechargeable
Traffic criticality mix	Routine 65%, Elevated 25%, Critical 10%	Application-representative distribution
Anomaly injection rate	3% of transmission windows	Synthetic attack indicator model
Baselines compared	Static AES-256-GCM, Static AES-128-GCM, Non-cognitive adaptive (threshold-based)	Fixed and simple-adaptive comparators

To isolate the specific contribution of cognitive, sustainability-aware reasoning beyond basic adaptivity, we can use the Non-cognitive adaptive baseline. This baseline employs a simple threshold rule—switch to a lighter cipher below a fixed battery percentage—without HCR awareness, fuzzy reasoning, or a learning layer.

7. Results and Discussion

7.1 Energy Consumption and Sustainability Outcomes

By the conclusion of the 180-day timeframe, Table 5 displays the average daily energy consumption and the percentage of nodes that achieved HCR ≥ 1.0 (complete sustainability) for all four schemes that were tested.

Table 5. Energy consumption and long-term sustainability outcomes across schemes

Scheme	Avg. Daily Energy (mJ/node)	% Nodes with HCR ≥ 1.0 at Day 180
Static AES-256-GCM	798.5	41.3%
Static AES-128-GCM	601.2	58.7%
Non-cognitive adaptive	544.9	63.5%
CCA (Proposed)	567.8	92.1%

By day 180, 92.1% of nodes achieve full sustainability (HCR ≥ 1.0) under CCA, compared to 63.5% under the non-cognitive baseline, a relative improvement of roughly 45%. This is

despite the fact that CCA's average daily energy consumption (567.8 mJ/node) is only slightly lower than the non-cognitive adaptive baseline (544.9 mJ/node). The main argument of the paper is that maximizing sustainability does not mean minimizing raw energy consumption. This is because nodes that are not good at harvesting end up depleting their energy supply, while nodes that are good at harvesting have extra security headroom that they do not use.

7.2 Ensuring Security Compliance

For each scheme we looked at, we calculated what percentage of communications marked as Critical really got at least Tier 3 (Elevated) security. In comparison to the non-cognitive adaptive baseline, which under-protected Critical traffic on nodes with limited battery life owing to its crude, one-variable threshold logic, CCA attained 96.4% compliance, which is second only to static AES-256-GCM (100% by build).

7.3 How Different Classes of Power Sources Act

When we break down the data by social class, we see that CCA's reasoning led to quite distinct, situationally appropriate actions: Class H nodes, which are abundant in solar power, ran at Tier 3-4 for the majority of transmissions, with an average HCR of 2.1 and minimal impact on sustainability. On the other hand, Class B nodes, which are powered solely by batteries, were directed to Tier 1-2 for the majority of routine transmissions, with Tier 3-4 reserved for critical and elevated traffic. By the end of the horizon, these nodes had achieved an average HCR of 0.94, which is close to energy neutrality even though they did not use any harvesting input. This was made possible through disciplined average consumption relative to a conservatively budgeted battery lifetime target.

7.4 The Learning Layer's Resistance to Non-Stationary Factors

Starting on day 90, we simulated a 30-day monsoon-season decrease in solar gathering (a 60% rate reduction for Class H nodes) to assess adaptation. The confidence-weighted learning layer of CCA was able to notice the change in the HCR trend within four to six days. During the low-harvesting period, it reverted to the tier distributions that had been in place before the event, about five days after the rates of harvesting had normalized. Despite being less complex than complete reinforcement learning, the confidence-weighted learning mechanism may adapt to significant non-stationary changes in the environment, as seen below.

8. Security Analysis

8.1 Environmental Manipulation Attacks

Given that CCA uses harvested data to support its logic, an attacker who can physically block a node's energy source (by shading it, for example) could try to force a depleting-HCR signal and decrease the node's security tier. CCA reduces this risk by using the overriding anomaly-signal rule from Section 5.2 (IF Anomaly Signal is Active THEN Security Tier is Maximum) to prioritize sustainability pressure over active probing or injection attempts, regardless of harvesting state, and by using rate-limited, averaged HCR inputs to resist rapid single-event manipulation.

8.2 Replay, Injection, and Authentication Integrity

Following best practices in authenticated encryption, each of the four levels of the cryptographic portfolio uses either GCM or explicit digital signatures (Tier4) to guarantee message integrity and replay resistance.

8.3 Rule-Base Integrity

A vulnerable gateway might theoretically skew rule weights toward consistently weaker configurations since the Learn phase modifies rule confidence weights using aggregated node outcomes at the edge gateway. We suggest implementing a system where rule-weight updates are signed and versioned using the network's existing key hierarchy. Nodes should be required to reject updates that change more than a certain percentage of rule weights in one update cycle. This way, the impact of a single compromised update can be limited.

8.4 Node Capture

To limit the effect of a single capture event to the compromised node's own traffic history, adaptive cryptographic schemes like these adhere to the hierarchical key derivation approach, which means that nodes' locally cached rule weights and session keys are exposed during physical capture. However, nodes' master key material is not exposed.

9. Discussion and Limitations

Section 7's results back up the paper's main argument: it is better to think about sustainability explicitly than to treat energy minimization as a proxy for it. This is especially true for heterogeneous IoT deployments, where a purely reactive scheme tends to mismanage nodes with limited harvesting capabilities. A number of caveats need to be mentioned. First, a more systematic derivation, maybe by expert elicitation or rule-mining from field deployment data, would be beneficial for the fuzzy rule base. It is interpretable, but it was hand-authored based on domain heuristics for this study. Second, site-specific variability in harvesting, especially for RF and vibration scavenging, can be much more irregular in actuality; the utilized models, which are representative but simplified, are daily solar with weather noise and intermittent vibration/RF. Thirdly, while the confidence-weighted learning mechanism is computationally inexpensive, it lacks the expressiveness of a full reinforcement-learning policy and may converge more slowly in extremely non-stationary or adversarial environments. A potential avenue for future improvement could be to combine it with the more expressive Q-learning approach discussed in related adaptive security literature.

10. Conclusion and Future Work

In this paper, we presented Cognitive Cryptographic Adaptation (CCA), a paradigm that repurposes the sense-reason-act-learn cognitive cycle from cognitive radio and network management for Internet of Things (IoT) security adaptation. CCA prioritizes sustainability, as measured by the Harvest-to-Consumption Ratio, as a reasoning objective alongside security compliance. Concurrently, CCA reduced energy consumption by 29-38% compared to fixed high-security configurations, increased the proportion of nodes reaching full long-term sustainability by about 45% compared to a non-cognitive adaptive baseline, and achieved a security compliance rate for critical traffic of 96.4% using a fuzzy inference reasoning core in conjunction with lightweight confidence-weighted learning. These findings suggest that for diverse, harvesting-dependent Internet of Things (IoT) deployments, long-term sustainability is best addressed as a primary goal in its own right, rather than as a side effect of energy-aware security.

In the future, we aim to improve the cognitive reasoning core to optimize cryptographic tier selection and other sustainability-relevant parameters like sensing rate and radio duty cycle. We will also investigate hybrid reasoning architectures that combine the interpretability of fuzzy rule bases with the expressiveness of deep reinforcement learning to adapt faster to non-stationary conditions. Finally, we will validate our models on physical energy-harvesting testbeds to confirm that our models accurately capture real-world environmental variability. Ultimately, we want to create a unified cognitive sustainability controller for IoT devices.

References

1. J. Mitola and G. Q. Maguire, "Cognitive Radio: Making Software Radios More Personal," IEEE Personal Communications, vol. 6, no. 4, 1999.
2. R. W. Thomas, D. H. Friend, L. A. DaSilva, and A. B. MacKenzie, "Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives," IEEE Communications Magazine, vol. 44, no. 12, 2006.
3. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power Management in Energy Harvesting Sensor Networks," ACM Transactions on Embedded Computing Systems, vol. 6, no. 4, 2007.

4. A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," Proceedings of the Cryptographic Hardware and Embedded Systems Workshop, 2007.
5. R. Beaulieu et al., "The SIMON and SPECK Families of Lightweight Block Ciphers," IACR Cryptology ePrint Archive, 2013.
6. L. A. Zadeh, "Fuzzy Sets," Information and Control, vol. 8, no. 3, 1965.
7. S. Chen, G. Zhang, and F. Yang, "A Fuzzy Logic-Based Trust Management Scheme for Wireless Sensor Networks," International Conference on Wireless Communications, Networking and Mobile Computing, 2010.
8. C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," Proceedings of ACM SenSys, 2004.
9. M. Rouhani et al., "Energy-Aware Security Protocols for Constrained IoT Devices: A Survey," IEEE Internet of Things Journal, 2021.
10. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, 2017.
11. X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless Networks with RF Energy Harvesting: A Contemporary Survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 2, 2015.
12. National Institute of Standards and Technology, "Lightweight Cryptography Standardization Process," NIST Special Publication, 2023.