https://doi.org/10.30857/2786-5371.2025.5.6

Received: 23.08.2025
Revised: 08.09.2025
Accepted: 22.10.2025

УДК 621.3:004.056.53: 004.738.5

Maksym SAVKA, Volodymyr PILINSKY
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

ADAPTIVE ENERGY-ORIENTED HARDWARE AND SOFTWARE SYSTEM FOR CRYPTOGRAPHIC PROTECTION OF INTERNET OF THINGS FOG NODES BASED ON FUZZY LOGIC

Purpose. *The purpose of the study is to develop and experimentally test an energy-oriented hardware and software method for adaptive management of the protection of electronic edge devices (fog nodes) in the Internet of Things (IoT). The method is based on fuzzy logic and selects the configuration of hardware and software protection tools depending on the current battery charge level and the varying threat level. This approach ensures the energy sustainability of embedded systems in critical infrastructure while simultaneously maintaining data confidentiality and integrity.*

Methodology. *The research was conducted using a specialized hardware and software testbed implemented in a Hardware-in-the-Loop format based on a Raspberry Pi 5 single-board computer, which acted as an autonomous IoT hardware platform. The software architecture was deployed as interacting Docker containers: an API request processing service, an Adaptive Security Manager (ASM) agent, and a monitoring module. A Takagi-Sugeno zero-order fuzzy logic controller was used for decision-making. The input linguistic variables were the state of charge estimation of the power subsystem and the current threat level, while the output was one of four predefined security modes. To evaluate the operational costs, a scalar objective function was developed that considers processing latency, the power consumption of the electronic node, and the security level. The discharge dynamics of the power subsystem were reproduced using an empirical logical discharge model that links the CPU load to the rate of energy consumption.*

Results. *Experimental testing, conducted across four 120-second scenarios, confirmed the advantages of the adaptive approach over static security policies. Fixed policies were shown to be irrational: the application of strong algorithms (e.g., AES-256) leads to accelerated depletion of the power subsystem under heavy traffic, while the continuous use of simplified modes increases device vulnerability risks. The results demonstrated that in normal mode, the adaptive approach reduces the power consumption of the electronic node by approximately 7% compared to fixed maximum protection, while guaranteeing a transition to the highest security level during an attack. In a critical low-charge mode, the system implements a survival strategy by maintaining the most energy-efficient configuration of hardware and software protection tools. This reduces power consumption by 40% and extends the battery life of the hardware platform under load by 1.7 times. Sensitivity analysis proved the stability of the system's physical indicators regardless of changes in the weighting coefficients of the objective function.*

Scientific Novelty. *The evaluation criterion for the performance of IoT hardware platforms was improved by introducing an integral objective function that formalizes the trade-off between processing latency, energy costs, and protection configuration. The study is the first to propose and experimentally validate a fuzzy-logic-based model for managing hardware and software protection tools that implements the concept of predictable survivability (graceful degradation) for embedded IoT systems. Unlike existing solutions, this model dynamically aligns power subsystem constraints with the need for enhanced protection, prioritizing energy savings when the charge is critically low and maximizing protection when sufficient resources are present.*

Practical Significance. *The practical application of the proposed solution significantly increases the reliability and energy survivability of embedded systems and IoT hardware platforms operating under unstable power supply conditions. Extending the battery life in critical situations provides a crucial window of opportunity needed to transmit important alarm notifications or wait for power restoration. The developed architecture allows for flexible modification of management scenarios and can be easily implemented on real electronic edge devices.*

Keywords: *embedded systems; IoT hardware platforms; power consumption of electronic nodes; power subsystem; hardware and software protection tools.*

Introduction. In mobile and peripheral systems of the Internet of Things (IoT), in particular in fog nodes, two interrelated requirements are simultaneously becoming more acute: maintaining performance in conditions of limited or unstable power supply and ensuring an appropriate level of data protection during the growth of cyber threats. Static configuration of cryptographic parameters in such conditions is technologically risky: either an excessive computing load is formed with accelerated energy depletion, or resistance to attacks at critical moments decreases. Therefore, an approach that allows managing the level of cryptographic protection as a function of the current state of the node and the external load is practically significant.

According to M. Sönmez Turan *et al.* (2023), the selection process was completed and it was decided to standardise the Ascon family as a basic solution for lightweight cryptography applications focused on resource-limited platforms where computing and energy efficiency are important [23]. The study emphasised that the choice was based on a combination of security analysis, benchmarking results, and community feedback, and the next step was to form a standard. In the development of this area, M. Sönmez Turan *et al.* (2025) published SP 800-232, which systematised approaches and recommendations for using lightweight cryptography (in particular for authenticated encryption and hashing) in scenarios with severe resource constraints [24]. Thus, in 2023–2025, a regulatory and methodological framework was formed, which makes the issue of practical integration of energy-saving cryptographic primitives into IoT even more applied. According to P. He *et al.* (2024), a generalisation of energy-aware security mechanisms for IoT was performed, where security was considered not as a fixed configuration, but as a controlled function of device resources, communication modes, and the threat environment [9]. The researchers systematised typical "safety-energy-performance" trade-offs and showed that practical solutions often need to be adapted, since there is no universally optimal configuration for all operating modes. This conclusion leads directly to the tasks of managing security profiles depending on the context.

According to M. Barari & R. Saifan (2023), an energy-aware security protocol for IoT devices was proposed, in which the adaptation of security parameters was considered as a means of reducing unnecessary resource costs in non-critical modes [5]. The paper emphasised that the energy price of cryptographic operations significantly affects the life cycle of battery units, and therefore, the security mechanism must be consistent with the resource state of the device, and not just with formal stability requirements. In the adjacent area, R. Kalaria *et al.* (2024) proposed a fog-oriented context-adaptive access control model, where the decision on security policy was made based on the level of risk and contextual parameters of the environment [10]. Although the focus of the study was on risk-based access management, the approach showed a general trend of moving "adaptability" from the cloud layer to the fog/edge layer, which has resource constraints and latency requirements. This creates prerequisites for adaptive management not only of access, but also of cryptographic modes on the gateway. Considering methods of decision-making under conditions of uncertainty, E. Krzysztoń *et al.* (2025) reviewed the applications of fuzzy / neuro-fuzzy approaches in IIoT security and emphasised that fuzzy models are convenient when the input parameters are of a different nature and do not have precise thresholds [13]. The researchers showed that fuzzy systems allowed combining expert knowledge with measurable metrics and maintaining rule interpretation, which is important for engineering implementation. In the context of fog nodes, this makes the Fuzzy Logic Controller (FLC) a suitable mechanism for managing security modes while simultaneously changing resources and threats.

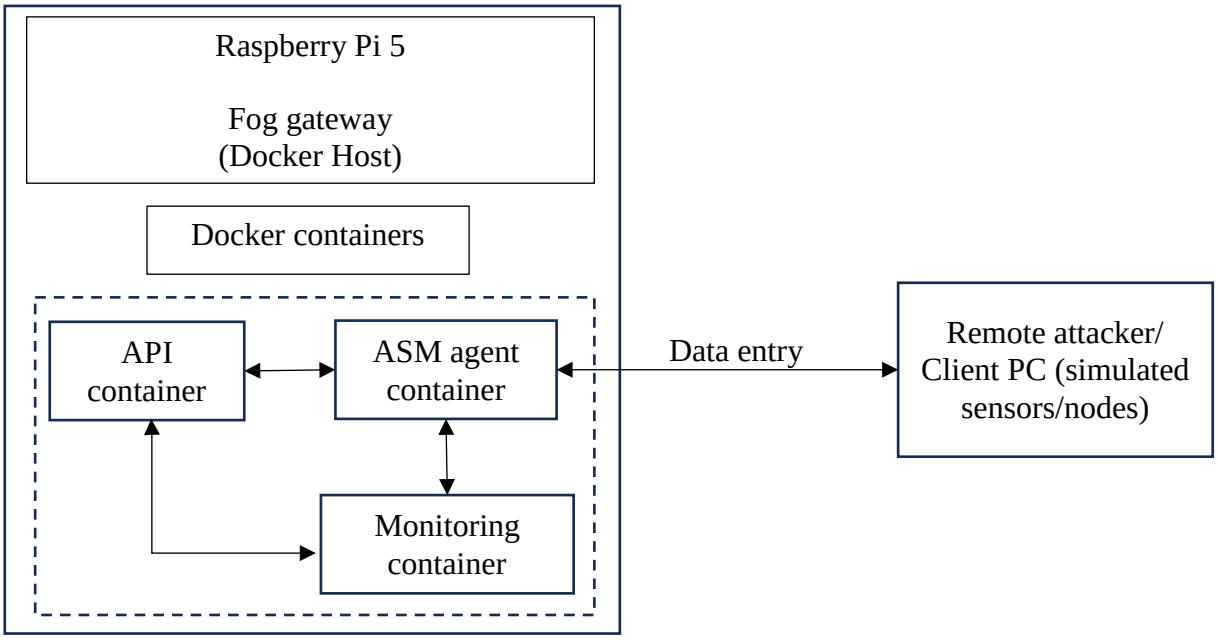
Within the framework of Ukrainian studies, Y. Pidlisnyi (2025) he considered the problem of assessing cybersecurity risks in IoT using fuzzy logic, emphasising the feasibility of fuzzy scales where indicators are partially uncertain or expert [19]. Although the study focused on risk assessment, it confirmed the relevance of fuzzy models for IoT security and supported the logic of moving from "evaluation" to "management" as the next application step. O. Mulesa & Y. Bohdan (2024) developed

a fuzzy production model for assessing the level of information security, where expert rules were turned into a formalised knowledge base with a numerical result indicator [17]. The researchers emphasised reducing subjectivity by structuring factors and rules, which is also fundamentally important for security profile management tasks where reproducibility of decision-making is required. Ultimately, H. Kuchuk & E. Malokhvii (2024) considered architectural approaches to IoT integration with cloud/fog/edge infrastructure from the standpoint of information and communication technologies, emphasising the role of peripheral nodes as an intermediate link between the sensor layer and the cloud [14]. In such architectures, the fog gateway actually becomes a "concentration point" for processing and policies, but the issue of power-oriented security configuration at this level is usually not central, which leaves room for application input.

Generalisation of the above papers showed that in 2020–2025, the prerequisites for energy-saving cryptography and contextual security adaptation at the edge/fog level were established, but the engineering implementation of managing cryptographic profiles of a fog node based on simultaneous consideration of the resource state and the current level of threats with reproducible experimental verification remained insufficiently covered. The purpose of the study was to develop and experimentally test an energy-oriented method for adaptive management of cryptographic protection of an IoT fog node based on fuzzy logic, taking into consideration the resource state of the node and the variable threat situation.

Materials and Methods.

Architecture of the hardware and software stand. For the study, a specialised software and hardware stand was developed that reproduced the scenario of an IoT fog node (mobile gateway) under load. The stand was based on a single-board Raspberry Pi 5 computer with 8 GB of RAM, which served as a stand-alone node, conventionally powered by a battery. It deployed a Docker-oriented software architecture with three containers (Fig. 1).



Note: ASM – Adaptive Security Manager; API – application programming interface.
Source: compiled by the authors.

Figure 1. **Hardware-in-the-loop (HiL) for testing the adaptive framework on Raspberry Pi 5**

The diagram showed the Raspberry Pi 5, which served as an IoT node-gateway with Docker containers: an ASM based on fuzzy logic, an API service with the implementation of cryptoprofiles,

and a monitoring service. A separate PC generated traffic (legitimate and attacking) to the node. Based on the monitoring data, the agent decided which security profile should be active and dynamically changed the API settings. The monitor collected performance and system status metrics for further analysis. In the software and hardware stand, the software part of the fog node was deployed in the form of three interacting containers: a request processing service, an adaptive management agent, and a monitoring and logging module. This decomposition provided a separation of application processing, decision logic, and experimental data collection.

The API container contained a REST service (based on FastAPI) that served incoming HTTP requests from clients and processed data according to the active profile. When processing each request, the service applied a profile-dependent set of computational procedures that implemented (or emulated) a cryptographic load of a certain complexity class, after which it generated and returned a response to the client. Profile switching was performed dynamically by reading the control parameter of the security policy, which was updated by the control agent. The ASM-agent (Adaptive Security Manager) container implemented FLC for adaptive profile selection. The agent with the specified survey period collected current indicators of the node state (in particular, an estimate of the state of charge – SoC, loading the Central Processing Unit (CPU), threat level, and active profile), normalised the data, and fed it to the fuzzy system input. Based on the result of fuzzy output, a profile recommendation was formed; in case of a difference from the current value, the agent updated the security policy by changing the configuration parameter or an internal control call to the API service. The monitoring container provided monitoring and collection of experimental data. It recorded system metrics (CPU load, RPS request intensity (Requests per Second) , average API response delay), and also took the active profile value from the agent, cost functions (J) and other control / state indicators. Data was recorded in timestamped log files (Comma-Separated Value format) in a specific directory; the survey was performed asynchronously with a discreteness of the order of units of a second.

A separate computer (conventionally a client/attack generator) located on the same local network was used to generate the external load. It sent HTTP requests to the API at a certain intensity, simulating normal traffic (background legitimate requests) and attacking traffic (a sharp spike in intensity that simulates a Distributed Denial of Service (DDoS) attack). The stand architecture was designed to easily modify scenarios and configurations. Log files saved by monitoring were processed by a separate analysis script that calculated the total values (for example, the average value J, total battery level drop (SoC), etc.) for each experimental run.

Cryptographic security profiles (API service). In the API service, four data processing profiles were defined, shown in Table 1, ordered by increasing computing and energy costs. All profiles were implemented programmatically within the same service, which provided the same execution conditions and minimised the impact of differences in external implementations. The profile was selected when each request was processed in accordance with the current security policy value passed by the management agent; therefore, the updated profile was applied from the next request.

For accelerated experimental evaluation, a synthetic load module was implemented that generated a controlled series of computational operations on the CPU and reproduced the energy costs representative of the corresponding cryptographic processing classes. This approach was applied taking into consideration the hardware-accelerated execution of individual cryptographic primitives in modern processor platforms, which makes it difficult to interpret short-term measurements of the contribution of individual cryptographic operations to the overall power consumption of the node. The synthetic load parameters were adjusted to preserve the relative proportions of computational complexity between the profiles; in particular, the load factor between the Max and Balanced profiles

was set to 1.66, which corresponds to the complexity ratio of pairs (AES-256 + SHA-512) and (AES-128 + SHA-256) at the model comparison level.

Table 1

Fog node data processing profiles and their characteristics

Profile	Functional purpose	Load model (operation class)	Overhead level
Safe	Control reference mode for estimating the lower limit of resource consumption.	No encryption or minimal integrity control (class CRC32).	Minimum
Survival	Power-saving mode when the battery is critically low or the threat level is low.	Emulated load of the light cryptographic primitives class (class ChaCha20) with simplified integrity control.	Low
Balanced	Operating mode of compromise between resource consumption and the level of protective processing.	Emulated load of medium complexity (class AES-128-GCM) with MAC of medium complexity (class HMAC-SHA256).	Average
Max	High-level protection mode with a high threat level and sufficient charge.	Emulated load of increased complexity (class AES-256-GCM) with MAC of increased complexity (class HMAC-SHA512).	High

Source: compiled by the authors.

FLC for adaptive security (ASM-agent). FLC used two input linguistic variables that reflected the resource state of the node and the current threat/load situation. Both variables were phased with three terms (LOW, MEDIUM, HIGH), and the membership functions were selected to ensure stability in the extreme sections of the ranges and a smooth transition in the middle region. The first battery level variable characterised the node's SoC as a percentage. Its linguistic breakdown included the terms LOW, MEDIUM, and HIGH, and the phasification limits were set according to experimental scenarios: HIGH – for SoC > 60%, MEDIUM – in the range of approximately 20–60%, LOW – for SoC < 20%. For extreme terms (LOW, HIGH), trapezoidal membership functions were used, which formed intervals of constant values and reduced sensitivity to fluctuations near the boundaries, while for the medium term, the triangular membership function was used. In the semantic interpretation, LOW corresponded to a state where the priority was to reduce power consumption, while HIGH meant having sufficient power to perform computationally intensive operations.

The second threat level variable reflected the current threat level or node load. The value of this variable was generated by the monitoring subsystem, taking into consideration the intensity of requests (RPS), the average response delay, and anomaly indicators (in particular, the proportion of failed requests). Phasification was also performed with LOW, MEDIUM, and HIGH terms on a fuzzy scale: LOW corresponded to a background mode without signs of attack and with a low load, HIGH – situations with a significant increase in intensity and deterioration of time indicators, which was interpreted as an active hostile action or abnormal load, and MEDIUM described intermediate states with an increase in load without unambiguous signs of attack. The source variable was Security Profile and displayed the selection of a security profile from the set: Safe, Survival, Balanced, Max. Since this is a discrete variable, a dephasification procedure with special processing was used to obtain it.

The fuzzy inference rule base was developed using a fuzzy system such as Takagi-Sugeno Zero-Order, which is computationally efficient for IoT devices. In this model, consequences (rule inferences) are represented by clear numerical values (singletons), rather than fuzzy sets. Dephasisation was performed using the Weighted Average method. A basic numerical value (Score)

was defined for each profile: Safe = 10, Survival = 30, Balanced = 60, Max = 90. The final profile selection was performed using threshold-based selection to avoid frequent switching (chattering). Activation ranges: Safe: $y < 20$, Survival: $20 \leq y < 50$, Balanced: $50 \leq y < 80$, Max: $y \geq 80$. This scheme allowed smoothly changing the output indicator and avoiding "jumps" of the profile with small fluctuations in the input variables (especially when SoC and Threat are at the boundary between the terms).

The fuzzy FLC rule base was formed as a set of products of the form **IF** Battery Level is B_i ***AND*** Threat Level is T_j **THEN** Security Profile is P_k, where $B_i, T_j \in \{\text{LOW, MEDIUM, HIGH}\}$, and $Pk \in \{\text{SAFE, SURVIVAL, BALANCED, MAX}\}$. A generalised representation of term combinations of input variables in the recommended profile is shown in Table 2. The logic of the rules implemented prioritisation of energy consumption at low charge (preference for SAFE/SURVIVAL modes) and strengthening of protective processing at sufficient energy resource and increased threat (transition to MAX).

Table 2

Fuzzy rule base for selecting a security profile

	Battery level		
Threat level	LOW	MEDIUM	HIGH
LOW	SAFE	SURVIVAL	SURVIVAL
MEDIUM	BALANCED	BALANCED	BALANCED
HIGH	BALANCED	MAX	MAX

Note: each cell contains the corresponding Security Profile recommended by FLC. Intermediate values are possible between adjacent terms; the table shows typical rule actuations.
Source: compiled by the authors.

FLC was configured to follow the principle: the system does not switch to the Max profile if Battery = LOW, regardless of other conditions. This guaranteed the "energy survival" mode. In other cases, FLC sought to improve security with the growth of threat level, but in view of SoC – that is, battery affects as a limiting factor. This logic reflected an engineering trade-off between safety and energy survivability.

Model for evaluating the cost function. To quantify the "optimality" or "cost" of the current state of the system, a scalar objective function is introduced J, which combines three normalised indicators: L_{norm} – normalised request processing delay (the longer the delay, the worse, the contribution increases J), P_{norm} – normalised power consumption or battery consumption (the more energy consumed, the larger this term), S_{norm} – normalised indicator of the security level (the higher the security level, the better, therefore, the equation uses $1 - S_{norm}$ so that the increase in security reduces J). A function is defined as a linear combination of these components with weight factors $w_L w_P w_S$:

$$J = w_L \cdot L_{norm} + w_P \cdot P_{norm} + w_S \cdot (1 - S_{norm}). \quad (1)$$

The study used three characteristic sets of weight factors w_L, w_P, w_S, which set priorities between the components of the evaluation function. The coefficient values for the Balanced, Security, and Energy sets are shown in Table 3.

Table 3

Sets of weighting coefficients in the evaluation function

Set	w_L	w_P	w_S
Balanced	0.2	0.4	0.4
Security	0.1	0.2	0.7
Energy	0.1	0.7	0.2

Source: compiled by the authors.

Normalisation of each component is performed as follows:

$$L_{norm} = \frac{L_{current} - L_{min}}{L_{max} - L_{min}}, \quad (2)$$

where $L_{current}$ – current response delay value (ms); L_{min} and L_{max} – respectively, the minimum and maximum permissible delay values (ms), which set the limits of normalisation.

In the experiments conducted, $L_{min} = 0$ мс and $L_{max} = 1{,}000$ мс were accepted in accordance with Quality of Service Requirements (Oracle, n.d.). The normalised share of battery charge consumed from the beginning of the experiment was determined as:

$$P_{norm} = \frac{SoC_0 - SoC_{current}}{100}, \quad (3)$$

where SoC_0 – initial charge level (%); $SoC_{current}$ – current charge level (%).

Normalised security level $S_{norm} \in [0; 1]$ set by displaying the selected security profile in a numerical scale: $S_{norm} = 0$ for the Safe profile, $S_{norm} = 1$ for the Max profile, and for intermediate profiles – by linear interpolation between these boundaries (proportional to the profile level). For example, for $SoC_0 = 100\%$ and $SoC_{current} = 95\%$ – $P_{norm} = 0.05$ was received. The ASM agent calculated J for each of its decisions and passed it to the monitoring service. This is how the J dynamics were tracked and the effectiveness of different scenarios in a multidimensional sense was compared. It is worth emphasising that the fuzzy system itself does not optimise J directly (it operates with the rules set by the expert).

Empirical model of logical battery discharge. Since the Raspberry Pi 5 in the experimental stand used was powered from the mains, direct measurement of the battery level was not possible. In this regard, an empirical logic discharge model is applied, in which the power consumption of a node is approximated as a function of CPU load, assuming an almost linear relationship between the computing load and power consumption under conditions of dominance of computational operations over other sources of power consumption. The model was set by the equation:

$$\Delta SoC/\Delta t = D_{idle} + (D_{max} - D_{idle}) \times \frac{CPU_{load}}{100}, \quad (4)$$

where $\Delta SoC/\Delta t$ – rate of charge reduction (% per second); D_{idle} – basic discharge rate in the idle state; D_{max} – discharge rate at 100% CPU load; CPU_{load} – current CPU usage (%).

By integrating this speed over time, the agent updated the SoC score. The initial SoC value was set at the beginning of the experiment (for example, 100% for a full battery scenario, 35% for a low battery). Model parameters (D_{idle}, D_{max}) selected for the accelerated testing scenario. The $D_{max} = 0.60\%/s$ was set, which corresponded to the full battery life under load $T_{full} \approx 166$ s (approximately 3 minutes). This time scale helped to demonstrate a significant charge drop (up to 70% at full load) within a short 120-second experiment and clearly visualise the impact of energy-saving strategies. These parameters are sufficient for a relative model that does not claim electrochemical accuracy, but allows comparing energy consumption between scenarios. The agent reads the current CPU%, applies a formula that reduces the SoC accordingly, and passes the new value to FLC and monitoring.

Scenarios of experimental loading of the stand. The experimental test was performed in four scenarios lasting 120 seconds each: Adaptive Full Battery (adaptive mode, initial charge level $SoC_0 \approx 100\%$), Adaptive Low Battery (adaptive mode, $SoC_0 \approx 35\%$), Fixed Max (non-adaptive mode with a Fixed Max profile throughout the experiment), and Fixed Balanced (non-adaptive mode with a Fixed Balanced profile). In Adaptive scenarios, the processing profile was defined by FLC

according to current values SoC and threat level; in Fixed scenarios, the profile remained unchanged regardless of the conditions. In all scenarios, the same load time profile was applied, consisting of three intervals: (1) 0–40 s – low-threat background mode (Threat ≈ LOW(2) 40–80 s – increased load interval, which was interpreted as a DDoS-type attack and corresponded to a high level of threat (Threat ≈ HIGH); (3) 80-120 s – restore to background mode (Threat ≈ LOW). The transition between intervals was set deterministically over time, and the load generator parameters were set equally for all starts, which ensured reproducibility of comparison between scenarios. Before each start, the system was brought to its original state: counters were initialised, and the initial level SoC_0 was set according to the scenario, the containers were switched to stable operating mode to reduce the impact of startup effects. Each scenario was repeated 5 times, after which the results were aggregated by measurement logs and averaged.

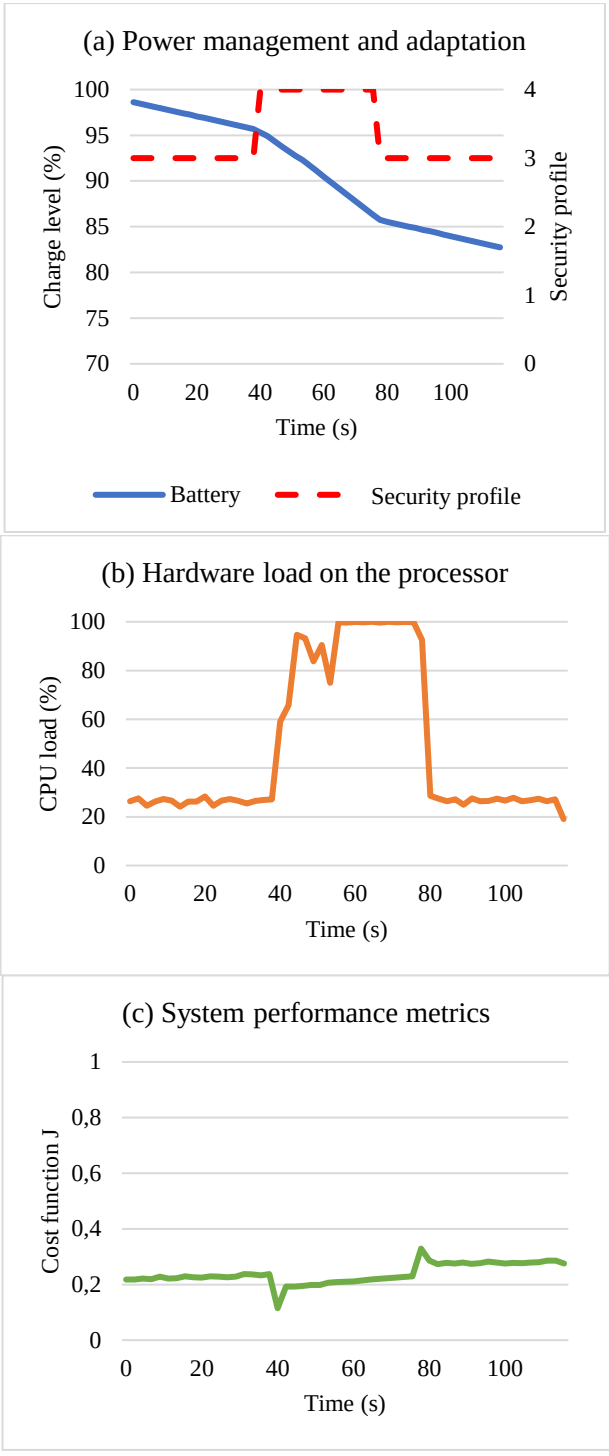
Results and Discussion.

Dynamics of adaptive and fixed scenarios. This section presented the results of experimental verification of the proposed approach in adaptive and fixed scenarios. To illustrate the typical flow of control processes, the time dependencies of key indicators in the Adaptive Full Battery scenario are presented, which is characterised by an initial high charge level and the presence of an interval of increased load (attack) in the middle of the experiment. Figure 2 shows the time dependencies for the Adaptive Full Battery scenario. In the background, the controller held the mid-level profile, while during the attack period, the profile was raised to the maximum. The transition to the maximum profile was accompanied by an increase in the computing load on the CPU and an increase in the rate of decline of SoC compared to the background interval. After the attack was completed, the profile returned to the average level, and the CPU load decreased with a short inertia, which was reflected in the smoothed curve. Dynamics of J was consistent with the change in the profile and the accumulation of energy costs: during transitions between profiles, transient deviations were observed, and after the attack was completed, the baseline level J remained higher than before the attack, which corresponded to a decrease of SoC due to energy consumption during the increased load interval.

Figure 3 showed the time dependences of the main indicators in the Adaptive Low Battery scenario with an initially low battery level SoC ≈ 35%. During the experiment, the active profile was kept at the Survival level, including the attack interval, which was consistent with the condition of low SoC as the dominant factor in choosing a profile. Under these conditions, the CPU load increased moderately during the attack period and decreased after its completion, while SoC changed monotonically with a downtrend without sharp transitions. Function J showed smooth dynamics without jumps, and its growth in the attack zone corresponded to a combination of increased load and further decline of SoC with an immutable security profile.

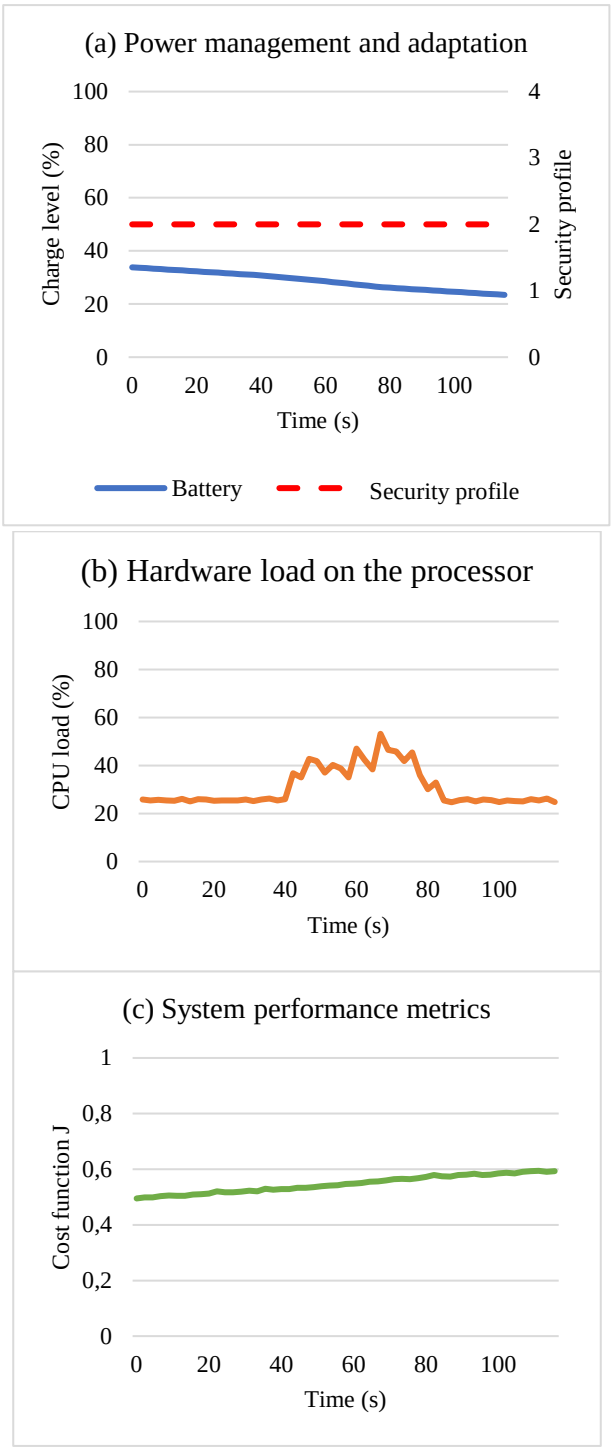
The results of experimental testing showed that adaptive scenarios provide more efficient power management compared to fixed ones, in particular, under variable load conditions and charge levels. In the Adaptive Full Battery scenario, the system demonstrates the ability to increase the security profile during attacks, which leads to an increase in CPU load and a decrease in battery power. In the Adaptive Low Battery scenario, the system maintains stable operation even when the battery level is low, maintaining an optimal balance between safety and power consumption.

Comparative characteristics of the four scenarios. To summarise the results obtained, four control scenarios under the same load conditions and the duration of the experiment were compared. Table 4 showed the average values of indicators for each scenario (a set of Balanced weights). The results showed that the Adaptive Full Battery and Fixed Max scenarios were characterised by a higher average level of security compared to other modes, while Adaptive Low Battery provided minimal energy costs by maintaining a lightweight profile. The Fixed Balanced scenario occupied an intermediate position in terms of the set of indicators under consideration.



Note: a – rated charge level SoC and active security profile; b – CPU load (instant and smooth); c – value of the cost function J, calculated for the basic Balanced weight set.
Source: developed by the authors.

Figure 2. **Adaptive Full Battery scenario dynamics**



Note: a – rated charge level SoC and active security profile; b – CPU load (instant and smooth); c – value of the cost function J, calculated for the basic Balanced weight set.
Source: compiled by the authors

Figure 3. **Time dependencies of metrics in the Adaptive Low Battery scenario**

Table 4

Comparison of four scenarios (Balanced weight factor set)

Set of weight factors	Scenario	J (average)	Energy consumed (%)	Average CPU load (%)	Security level indicator (average)
Balanced	Adaptive Full Battery	0.238	15.527	49.65	70.0
Balanced	Adaptive Low Battery	0.549	10.039	31.06	40.1
Balanced	Fixed Max	0.2085	16.71	53.69	90.0
Balanced	Fixed Balanced	0.2486	12.096	38.86	60.0

Source: compiled by the authors.

The results of the scenario comparison were consistent with adaptive control logic: when there was an energy resource, the controller raised the profile in the attack zone, and when the charge was critically low, it kept the lightweight profile, minimising the computational load and slowing down charge depletion. Thus, adaptive regimes implemented two different strategies – "protection with acceptable energy consumption" (for a high initial charge) and "survivability with an energy deficit" (for a low charge), which is fundamentally inaccessible to static policies. Integral metric behaviour J did not reflect the "absolute superiority" of a particular mode, but the chosen priorities of the Balanced weight set: with a relatively significant contribution of the safety component, the static maximum profile received the least penalty precisely due to a consistently high level of safety, even despite increased energy costs. But in the energy deficit mode, the adaptive strategy deliberately accepted an increased penalty for the security component, since it maintained the node's performance due to the limitation of computational load and discharge rate. Thus, the comparison by J should be interpreted as a weight-sensitive generalisation of the "security-energy-performance" trade-off, while the practical conclusion was the ability of adaptive control to change the profile according to the available energy and the presence of an attack.

Comparative analysis of power consumption (Adaptive vs Fixed Max). According to the experimental data obtained, in a high-threat scenario, the Fixed Max static profile results in a consumption of 16.71% of the battery capacity per experiment cycle. But the proposed adaptive method (Adaptive Full Battery) under similar conditions spent 15.53% of the charge. Although the absolute difference was $\approx 1.2\%$, the relative energy savings at the stage of active counteraction to an attack reached ~7% while maintaining the maximum level of protection at critical moments. In the long run (for example, when the device runs for hours), such savings are converted into longer battery life without compromising security. In some series of experiments (as shown by sensitivity analysis), the difference reached higher values, which indicates the dependence of efficiency on the load profile. The Adaptive Low Battery scenario demonstrated a key advantage of the developed method – the ability to ensure the survivability of the node. Based on the measurement results, under low charge conditions ($SoC \approx 35\%$) the system reduced power consumption to 10.04% per session, which is 40% less than in Fixed Max mode (16.71%). This allows formulating the concept of predicted survivability. It is assumed that the node has a residual charge of 35% and is subjected to a constant load: in Fixed Max mode, it will completely drain the battery in about 2 full cycles ($16.7\% \times 2 > 33\%$). Time to complete failure: ≈ 4–5 minutes. In Adaptive Low Battery mode, the node consumes only 10% per cycle, which allows it to last 3.5 cycles. This increases the life of the device by almost 1.7 times. In fact, the adaptive method provides additional time, which can be crucial for transmitting critical alarms or waiting for power to resume. In terms of average performance, Adaptive Low Battery kept the CPU load at 31%, while Fixed Max kept it at 54%. This confirmed the compliance of the proposed method with the ideology of “graceful degradation” (soft degradation). Under the

pressure of resource constraints, the system significantly reduces the quality of security service (switching to ChaCha20), but guarantees the continuation of the node's operation. For critical infrastructure in a blackout environment, this is a more acceptable scenario than a sudden complete device failure due to battery depletion with perfect encryption.

Function sensitivity analysis J before changing the weight. To check the weight settings w_L, w_P, w_S (priorities) affect the behaviour of the system, repeated experiments were performed in all 4 scenarios for three sets of weights: Balanced, Security, Energy (Table 5).

Table 5

Average value of J and relative changes in physical metrics for different weight factors

Weight_Set	Scenario	Avg_J	Energy_Delta (%)	Avg_CPU (%)	Avg_Sec_Score
Balanced	Adaptive Full Battery	0.238	15.527	49.65	70.0
	Adaptive Low Battery	0.549	10.039	31.06	40.1
	Fixed Max	0.2085	16.71	53.69	90.0
	Fixed Balanced	0.2486	12.096	38.86	60.0
Security	Adaptive Full Battery	0.2674	15.381	51.29	70.4
	Adaptive Low Battery	0.5731	9.945	31.42	40.2
	Fixed Max	0.1529	15.862	53.04	90.0
	Fixed Balanced	0.3229	11.671	38.23	60.0
Energy	Adaptive Full Battery	0.1617	14.816	51.54	70.2
	Adaptive Low Battery	0.6295	9.514	31.34	40.4
	Fixed Max	0.1505	15.811	55.25	90.0
	Fixed Balanced	0.1592	11.451	39.21	60.0

Note: the average value is shown for each scenario J for Balanced, Pro-Security, and Pro-Energy weight sets.
Source: compiled by the authors.

The most important result was that the physical performance of the system remains stable regardless of the settings of the evaluation function. Power consumption (Energy_Delta): for the Adaptive Full Battery scenario fluctuations are $15.5\% \ldots 14.8\%$. For Fixed Max – $16.7\% \ldots 15.8\%$. Security level (Sec_Score): for Adaptive Full Battery, the indicator is consistently kept at the level of $\approx 70.0..70.4$. This confirmed that the FLC makes decisions based on objective input data (charge, threat), and does not adapt to subjective metrics J. The system demonstrated high reliability of behaviour. Function value J changed, reflecting a change in priorities ("fines"). Set 2 (Pro-Security, $w_S = 0.7$): for Fixed Max value J dropped to a low (0.1529) as this mode provides maximum safety (90.0), which is a priority in this set of weights. For Adaptive Full Battery value J increased a little ($0.238 \rightarrow 0.267$), as the system sometimes used "lighter" profiles, which is regarded as a "penalty" under strict security requirements. Set 3 (Pro-Energy, $w_P = 0.7$): for Adaptive Full Battery value J significantly decreased ($0.238 \rightarrow 0.162$). This means that in terms of energy savings, the adaptive system behaviour is highly efficient. For Adaptive Low Battery value J remains high (0.63), which mathematically reflects the compromise state of the system: although energy is saved, a low level of security (40.0) creates a large penalty, even with a reduced coefficient w_S. The proposed control model is resistant to changes in the evaluation parameters, and the function J adequately reflects the degree of compliance of the system behaviour with the chosen strategy (safety or energy saving).

Discussion of results in the context of similar scientific studies. The experimental results obtained can be interpreted in the context of two research lines: (1) quantifying the energy cost of cryptographic transformations on peripheral computers and (2) searching for mechanisms for contextual/risk-oriented security adaptation in edge/fog, when the security policy changes depending on the state of the resource and threats. According to I. Radhakrishnan *et al.* (2024), in the study on

energy profiling of cryptography on edge devices, it was shown that the real cost of energy and time was determined not only by the class of the algorithm, but also by the specific implementation, the mode of authenticated encryption and interaction with the hardware capabilities of the platform (in particular, acceleration instructions), as a result of which the "always maximum" approach in many cases turned out to be engineering suboptimal, despite the formally highest level of protection [20]. A.N. Alvi *et al.* (2024) came to a conclusion about the cumulative effect of cryptographic load in long-term or intensive scenarios of traffic processing on the periphery; accordingly, in the author's study, the increase in the average CPU load and the share of energy spent in static maximum mode reflected just such a cumulative nature of the impact of crypto operations [3].

Comparing an adaptive strategy scenario with a static maximum should not be interpreted as "against" maximum safety, but as confirmation that an equivalent level of incident response can be achieved with lower total costs due to the limited time spent in heavy mode. As emphasised by S. Ramagundam *et al.* (2025) in the literature on energy-saving cryptography and energy-oriented cryptographic frameworks for IoT, a practical advantage was often provided by the regime organisation of protection, when the parameters were applied selectively (for example, in a high-risk window), and the rest of the time a balanced profile was used, which reduced the energy load without completely abandoning cryptographic protection [21]. Consistent with this approach, in this formulation, the adaptive strategy reproduced the peak level of protection in the attack zone, but reduced integral costs outside it, which was reflected in the aggregated energy/CPU metrics and interpreted as an advantage of mode profile management.

The low-charge scenario requires a separate discussion, since it translates the problem from the "efficiency" plane to the survivability plane. L. Mottola *et al.* (2024) described a class of attacks and degradation modes for battery-powered IoT nodes in threatened environments, in which the enemy (or environmental conditions) caused resource consumption and accelerated power depletion, which led to service loss even without compromising data [16]. This implies an engineering principle: with a critically low resource, the strategy should minimise the risk of complete disconnection, even if this means a temporary reduction in cryptographic "rigidity". A. Upadhiyay & A. Jain (2025) considered this logic, sometimes formalised as graceful degradation or survivability-oriented security, as acceptable for fog/edge systems in situations where continuity was a higher priority than maximising cryptographic stability at any given time [25]. That is why the stable retention of the energy-saving profile in conditions of low SoC in the author's experiment should be interpreted as behaviour consistent with the survivability-policy class: the system retained manageability and the ability to perform the main function, without entering the "self-destruction" mode from an excessive cryptographic price.

K. Sohan Jayram Reddy & K. Bhargavi (2025) in the study on countering botnets and DDoS, fog/edge emphasised that attacks at the peripheral level were often of a dual nature, combining a security threat with a sharp increase in computing load at the point of traffic aggregation [22]. S.P.K. Gudla *et al.* (2022) in publications on modelling and evaluating DDoS intensities for the fog level emphasised that even short-term load peaks formed processing queues and could retain inertia after the active attack phase was completed [8]. This was consistent with observations of CPU load transients after the threat disappeared and explained why returning the profile to a more economical mode does not immediately restore low computing load: the system still unloads the accumulated queue of cryptographic operations for some time.

The interpretation of the behaviour of an integral metric (cost function) should be based not on the better or worse value of a single run, but on its role as an indicator of the consistency of a compromise. The study by A. Alotaibi *et al.* (2025), based on the analysis of the energy trace of cryptography on edge devices, showed that the reduction in energy and latency often comes at the cost of a lower cryptographic load, and vice versa; because of this, composite indicators and their

trends over time are important for practice, which signal when the system enters the zone of unacceptable compromise [2]. In this implementation, this meant that short-term deviations of the metric at the moments of switching profiles were naturally interpreted as a consequence of different time scales: the discrete logical solution changes rapidly, while the physical load/energy response is inertial. J. Baek & G. Kaddoum (2023) showed that time scale differences were typical for systems where decisions were made by the controller or policy, while actual execution depended on the state of queues, scheduler, and implementation features of crypto libraries [4].

As for the decision-making mechanism, studies on interpreted models for IoT security show a tendency towards approaches where rules or logical structures remain explicable and suitable for engineering validation. C. Kim *et al.* (2024) proposed logic-oriented (in particular, fuzzy and hybrid) knowledge representations for the IoT domain, which combined risk formalisation, integration of heterogeneous parameters, and transparency of causal relationships [12]. H.B. Akande *et al.* (2025) in IoT attack detection tasks, models were used where fuzziness was used to describe transient states and unstable network modes, which allowed reducing the manifestations of sharp threshold effects in decision-making [1]. Against this background, this approach differed in that fuzzy logic was used not to detect an attack as such, but to control the cryptographic profile as an engineering lever for changing the resource intensity of protection. M. Martínez-Rojas *et al.* (2025) substantiated the feasibility of interpreted rules in systems where predictability of behaviour under resource constraints was required and where the price of a control error was high (for example, premature battery depletion or service failure under load), which was consistent with the control logic chosen by the authors of this study [15].

Separately, the role of experimental methodology and reproducibility should be emphasised. M.J. Baucas *et al.* (2023), in studies on building software and hardware stands for network and IoT systems, noted that the combination of a real hardware platform with controlled load scenarios helped to correctly identify inertial effects (queues, load jumps, latent delays) and separate the contribution of management policies and the contribution of implementation details [6]. S. Blanc *et al.* (2022) proposed reproducible approaches to benchmarking in the direction of high-precision performance evaluation of cryptographic implementations for embedded platforms and demonstrated that even within a single class of algorithms, differences in implementations and target platforms could significantly alter the "speed-energy-resilience" practical balance [7]. According to the recommendations, the obtained numerical differences between the scenarios should be interpreted as valid for a given hardware and software configuration and load class, while generalisation of the results should be performed correctly by repeating the technique on other platforms and cryptographic packages.

J. Kaur *et al.* (2023) emphasised that the interpretation of cryptographic "value" in practice should consider the evolution of the attack landscape and cryptanalytic results, since cryptographic stability was determined not only by the choice of algorithm, but also by the mode, parameters, and implementation, which was directly related to resource costs at the edge level [11]. In this context, adaptive profile management should be interpreted as an element of broader cryptographic flexibility and operational stability: the system is able to maintain an acceptable level of protection at critical moments, without wasting resources in modes where the threat is not confirmed or where the resource is critically limited.

The computational energy profile of cryptography is platform-dependent and responsive to implementations, which is confirmed by studies of power consumption on edge devices and benchmarking of various embedded architectures. Battery discharge modelling in applied studies often uses simplification, but studies of attacks focused on energy depletion demonstrate the need to test such models in representative load modes. In networks dominated by radio transmission costs, such as WSN/LPWAN, the cryptographic contribution may be comparable or even less than that of

the physical layer and MAC, which requires the inclusion of additional variables in the control loop, such as transmission frequency, power, and sleep modes. Thus, the results of the study confirm the practical feasibility of regime management of cryptography on a fog node, adapting it to variable threats and limited resources.

Conclusions. As a result of the study, an effective method for increasing the energy survivability of a fog node that functions as a gateway for mobile IoT was identified in conditions of limited power supply and variable threat conditions. An adaptive approach to managing the protective treatment profile based on FLC was proposed, which makes decisions based on charge level values and an integral threat indicator, allowing energy constraints to be effectively reconciled with the need for increased protection during periods of high load. As part of the study, the evaluation criterion was improved, and an integral cost function was introduced, which formalised the trade-off between latency, energy costs, and the level of the processing profile. Experiments conducted on the HIL hardware and software stand based on Raspberry Pi 5 with Docker containerisation confirmed the effectiveness of the method, while using an empirical model for estimating the charge level provided accelerated testing and correct reflection of changes depending on the CPU load.

It has been demonstrated that in normal mode (Adaptive Full Battery), the proposed approach reduced energy consumption by 7% compared to fixed strategies. However, during an attack, the system adapts, moving to an increased level of processing. In critical mode (Adaptive Low Battery), the reduction in power consumption reaches 40% (up to 10.04% of the capacity per session), which provides a significant increase in the battery life of the node under load – up to 1.7 times compared to conventional methods. Sensitivity analysis showed that changes in the weight coefficients in the cost function do not affect the stability of decision-making, and the physical parameters of the system (energy consumption, CPU load) remain within the statistical error. This confirms the stability of the fuzzy rule base and the low sensitivity of the algorithm to setting weight parameters. Further research is aimed at verifying the method on heterogeneous fog/edge-level hardware platforms, adapting the algorithm for resource-limited microcontrollers and expanding the approach for coordinating a group of fog nodes, and automating the development of a threat indicator through integration with intrusion detection systems.

Acknowledgements. None.
Funding. None.
Conflict of Interest. None.

References

1. Akande, H. B., Imoize, A. L., Adeniran, T. C., Lee, C.-C., & Awotunde, J. B. (2025). RF-FLIDS: A novel hybrid intrusion detection model for enhanced anomaly detection in IoT networks. *Security and Privacy*, 8(3), Art. e70041. DOI: https://doi.org/10.1002/SPY2.70041.
2. Alotaibi, A., Aldawghan, H., & Frikha, M. (2025). Lightweight cryptography for energy-conscious authentication in IoT systems. *International Journal of Advanced Computer Science and Applications*, 16(11), 1081–1091. DOI: https://doi.org/10.14569/IJACSA.2025.01611103.
3. Alvi, A.N., Ali, B., Saleh, M.S., Alkhathami, M., Alsadie, D., & Alghamdi, B. (2024). Secure computing for fog-enabled industrial IoT. *Sensors*, 24(7), Art. 2098. DOI: https://doi.org/10.3390/S24072098.

Література

1. Akande H. B., Imoize A. L., Adeniran T. C., Lee C.-C., Awotunde J. B. RF-FLIDS: A novel hybrid intrusion detection model for enhanced anomaly detection in IoT networks. *Security and Privacy*. 2025. No. 8 (3). Art. e70041. DOI: https://doi.org/10.1002/SPY2.70041.
2. Alotaibi A., Aldawghan H., Frikha M. Lightweight cryptography for energy-conscious authentication in IoT systems. *International Journal of Advanced Computer Science and Applications*. 2025. No. 16 (11). P. 1081–1091. DOI: https://doi.org/10.14569/IJACSA.2025.01611103.
3. Alvi A. N., Ali B., Saleh M. S., Alkhathami M., Alsadie D., Alghamdi B. Secure computing for fog-enabled industrial IoT. *Sensors*. 2024. No. 24 (7). Art. 2098. DOI: https://doi.org/10.3390/S24072098.

4. Baek, J., & Kaddoum, G. (2023). FLoadNet: Load balancing in fog networks with cooperative multiagent using actor-critic method. *IEEE Transactions on Network and Service Management*, 20(1), 400–414. DOI: https://doi.org/10.1109/TNSM.2022.3210827.
5. Barari, M., & Saifan, R. (2023). Energy-aware security protocol for IoT devices. *Pervasive and Mobile Computing*, (96), Art. 101847. DOI: https://doi.org/10.1016/J.PMCJ.2023.101847.
6. Baucas, M. J., Spachos, P., & Plataniotis, K. N. (2023). Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, 10(4), 1732–1741. DOI: https://doi.org/10.1109/TCSS.2023.3235950.
7. Blanc, S., Lahmadi, A., Le Gouguec, K., Minier, M., & Sleem, L. (2022). Benchmarking of lightweight cryptographic algorithms for wireless IoT networks. *Wireless Networks*, 28(8), 3453–3476. DOI: https://doi.org/10.1007/S11276-022-03046-1.
8. Gudla, S. P. K., Bhoi, S. K., Nayak, S. R., & Verma, A. (2022). DI-ADS: A deep intelligent distributed denial of service attack detection scheme for fog-based IoT applications. *Mathematical Problems in Engineering*, 2022(1), Art. 3747302. DOI: https://doi.org/10.1155/2022/3747302.
9. He, P., Zhou, Y., Qin, X., He, P., Zhou, Y., & Qin, X. (2024). A survey on energy-aware security mechanisms for the Internet of Things. *Future Internet*, 16(4), Art. 128. DOI: https://doi.org/10.3390/FI16040128.
10. Kalaria, R., Kayes, A. S. M., Rahayu, W., Pardede, E., & Salehi Shahraki, A. (2024). Adaptive context-aware access control for IoT environments leveraging fog computing. *International Journal of Information Security*, 23(4), 3089–3107. DOI: https://doi.org/10.1007/S10207-024-00866-4.
11. Kaur, J., Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2023). A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. *ArXiv*. DOI: https://doi.org/10.48550/arXiv.2304.06222.
12. Kim, C., So-In, C., Kongsorot, Y., & Aimtongkham, P. (2024). FLSec-RPL: A fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks. *Cybersecurity*, 7(1), Art. 27. DOI: https://doi.org/10.1186/S42400-024-00223-X.
13. Krzysztoń, E., Mikołajewski, D., & Prokopowicz, P. (2025). Review of fuzzy methods application in IIoT security – challenges and perspectives.

4. Baek J., Kaddoum G. FLoadNet: Load balancing in fog networks with cooperative multiagent using actor-critic method. *IEEE Transactions on Network and Service Management*. 2023. No. 20 (1). P. 400–414. DOI: https://doi.org/10.1109/TNSM.2022.3210827.
5. Barari M., Saifan R. Energy-aware security protocol for IoT devices. *Pervasive and Mobile Computing*. 2023. No. 96. Art. 101847. DOI: https://doi.org/10.1016/J.PMCJ.2023.101847.
6. Baucas M. J., Spachos P., Plataniotis K. N. Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*. 2023. No. 10 (4). P. 1732–1741. DOI: https://doi.org/10.1109/TCSS.2023.3235950.
7. Blanc S., Lahmadi A., Le Gouguec K., Minier M., Sleem L. Benchmarking of lightweight cryptographic algorithms for wireless IoT networks. *Wireless Networks*. 2022. No. 28 (8). P. 3453–3476. DOI: https://doi.org/10.1007/S11276-022-03046-1.
8. Gudla S. P. K., Bhoi S. K., Nayak S. R., Verma A. DI-ADS: A deep intelligent distributed denial of service attack detection scheme for fog-based IoT applications. *Mathematical Problems in Engineering*. 2022. No. 2022 (1). Art. 3747302. DOI: https://doi.org/10.1155/2022/3747302.
9. He P., Zhou Y., Qin X., He P., Zhou Y., Qin X. A survey on energy-aware security mechanisms for the Internet of Things. *Future Internet*. 2024. No. 16 (4). Art. 128. DOI: https://doi.org/10.3390/FI16040128.
10. Kalaria R., Kayes A. S. M., Rahayu W., Pardede E., Salehi Shahraki A. Adaptive context-aware access control for IoT environments leveraging fog computing. *International Journal of Information Security*. 2024. No. 23 (4). P. 3089–3107. DOI: https://doi.org/10.1007/S10207-024-00866-4.
11. Kaur J., Canto A. C., Kermani M. M., Azarderakhsh R. A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. *ArXiv*. 2023. DOI: https://doi.org/10.48550/arXiv.2304.06222.
12. Kim C., So-In C., Kongsorot Y., Aimtongkham P. FLSec-RPL: A fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks. *Cybersecurity*. 2024. No. 7 (1). Art. 27. DOI: https://doi.org/10.1186/S42400-024-00223-X.
13. Krzysztoń E., Mikołajewski D., Prokopowicz P. Review of fuzzy methods application in IIoT security

Electronics, 14(17), Art. 3475. DOI: https://doi.org/10.3390/electronics14173475.
14. Kuchuk, H., & Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: A review. *Advanced Information Systems*, 8(2), 65–78. DOI: https://doi.org/10.20998/2522-9052.2024.2.08.
15. Martínez-Rojas, M., Cano, C., Alcalá-Fdez, J., & Soto-Hidalgo, J. M. (2025). Interpretable fuzzy control for energy management in smart buildings using JFML-IoT and IEEE Std 1855-2016. *Applied Sciences*, 15(15), Art. 8208. DOI: https://doi.org/10.3390/APP15158208.
16. Mottola, L., Hameed, A., & Voigt, T. (2024). Energy attacks in the battery-less Internet of Things: Directions for the outure. In *EuroSec'24: Proceedings of the 17th European workshop on systems security* (pp. 29–36). New York: Association for Computing Machinery. DOI: https://doi.org/10.1145/3642974.3652283.
17. Mulesa, O., & Bohdan, Y. (2024). Development of a fuzzy production model for assessing the degree of information security in international cooperation. *Technology Audit and Production Reserves*, 6(2(80)), 6–10. DOI: https://doi.org/10.15587/2706-5448.2024.318446.
18. Oracle (n.d.). Quality of service requirements. URL: https://docs.oracle.com/cd/E19528-01/819-2326/gaxqg/index.html.
19. Pidlisnyi, Y. (2025). Fuzzy logic in IoT security risk assessment: Rule construction and implementation. *Technical Sciences and Technologies*, 3(41), 237–253. DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-237-253.
20. Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*, 24(12), Art. 4008. DOI: https://doi.org/10.3390/S24124008.
21. Ramagundam, S., Karamchandani, H., Patil, G. U., & Subramanium, P. (2025). Context-aware lightweight and post-quantum cryptographic framework for secure wireless communication. *Journal of Discrete Mathematical Sciences and Cryptography*, 28(5-B), 2037–2047. DOI: https://doi.org/10.47974/JDMSC-2421.
22. Sohan Jayram Reddy, K., & Bhargavi, K. (2025). Detection of DDoS attacks in fog computing using interpretable quantum-based 2Q learning approach. In *Proceedings of the 3rd international conference on intelligent and innovative technologies in computing, electrical and electronics* (pp. 1–5). New York: IEEE. DOI: https://doi.org/10.1109/IITCEE64140.2025.10915401.

– challenges and perspectives. *Electronics*. 2025. No. 14 (17). Art. 3475. DOI: https://doi.org/10.3390/electronics14173475.
14. Kuchuk H., Malokhvii E. Integration of IoT with cloud, fog, and edge computing: A review. *Advanced Information Systems*. 2024. No. 8 (2). P. 65–78. DOI: https://doi.org/10.20998/2522-9052.2024.2.08.
15. Martínez-Rojas M., Cano C., Alcalá-Fdez J., Soto-Hidalgo J. M. Interpretable fuzzy control for energy management in smart buildings using JFML-IoT and IEEE Std 1855-2016. *Applied Sciences*. 2025. No. 15 (15). Art. 8208. DOI: https://doi.org/10.3390/APP15158208.
16. Mottola L., Hameed A., Voigt T. Energy attacks in the battery-less Internet of Things: Directions for the outure. In *EuroSec'24: Proceedings of the 17th European workshop on systems security* (pp. 29–36). New York: Association for Computing Machinery, 2024. DOI: https://doi.org/10.1145/3642974.3652283.
17. Mulesa O., Bohdan Y. Development of a fuzzy production model for assessing the degree of information security in international cooperation. *Technology Audit and Production Reserves*. 2024. Vol. 6, No. 2 (80). P. 6–10. DOI: https://doi.org/10.15587/2706-5448.2024.318446.
18. Quality of service requirements. *Oracle*. URL: https://docs.oracle.com/cd/E19528-01/819-2326/gaxqg/index.html.
19. Pidlisnyi Y. Fuzzy logic in IoT security risk assessment: Rule construction and implementation. *Technical Sciences and Technologies*. 2025. No. 3 (41). P. 237–253. DOI: https://doi.org/10.25140/2411-5363-2025-3(41)-237-253.
20. Radhakrishnan I., Jadon S., Honnavalli P. B. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*. 2024. No. 24 (12). Art. 4008. DOI: https://doi.org/10.3390/S24124008.
21. Ramagundam S., Karamchandani H., Patil G. U., Subramanium P. Context-aware lightweight and post-quantum cryptographic framework for secure wireless communication. *Journal of Discrete Mathematical Sciences and Cryptography*. 2025. No. 28(5-B). P. 2037–2047. DOI: https://doi.org/10.47974/JDMSC-2421.
22. Sohan Jayram Reddy K., Bhargavi K. Detection of DDoS attacks in fog computing using interpretable quantum-based 2Q learning approach. In *Proceedings of the 3rd international conference on intelligent and innovative technologies in computing, electrical and electronics* (pp. 1–5). New York: IEEE, 2025. DOI:

23. Sönmez Turan, M., McKay, K., Chang, D., Bassham, L. E., Kang, J., Waller, N. D., Kelsey, J. M., & Hong, D. (2023). Status report on the final round of the NIST lightweight cryptography standardization process. Gaithersburg: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.IR.8454.
24. Sönmez Turan, M., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2025). Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions. Gaithersburg: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-232.
25. Upadhiyay, A., & Jain, A. (2025). Cyber resilient framework with energy efficient swarm routing and ensemble threat detection in fog assisted wireless sensor networks. *Scientific Reports*, 15(1), Art. 36461. DOI: https://doi.org/10.1038/s41598-025-21368-w.

https://doi.org/10.1109/IITCEE64140.2025.10915401.
23. Sönmez Turan M., McKay K., Chang D., Bassham L. E., Kang J., Waller N. D., Kelsey J. M., Hong D. Status report on the final round of the NIST lightweight cryptography standardization process. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: https://doi.org/10.6028/NIST.IR.8454.
24. Sönmez Turan M., McKay K. A., Chang D., Kang J., Kelsey J. Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions. Gaithersburg: National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-232.
25. Upadhiyay A., Jain A. Cyber resilient framework with energy efficient swarm routing and ensemble threat detection in fog assisted wireless sensor networks. *Scientific Reports*. 2025. No. 15 (1). Art. 36461. DOI: https://doi.org/10.1038/s41598-025-21368-w.

Maksym SAVKA
Postgraduate Student,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0003-2049-9438
E-mail: maximsavka@gmail.com

Volodymyr PILINSKY
PhD in Technical Sciences, Professor,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-2569-9503
Scopus Author ID: 35867898100
ResearcherID: J-6418-2017
E-mail: pww@ukr.net

Максим САВКА, Володимир ПІЛІНСЬКИЙ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

АДАПТИВНА ЕНЕРГООРІЄНТОВАНА АПАРАТНО-ПРОГРАМНА СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ FOG-ВУЗЛА ІНТЕРНЕТУ РЕЧЕЙ ЗА НЕЧІТКОЮ ЛОГІКОЮ

Мета. *Метою дослідження є розроблення та експериментальна перевірка енергоорієнтованого апаратно-програмного методу адаптивного управління захистом периферійних електронних пристроїв (fog-вузлів) Інтернету речей. Метод має базуватися на нечіткій логіці та здійснювати вибір конфігурації апаратно-програмних засобів захисту залежно від поточного рівня заряду батареї та змінного рівня загрози. Це дозволить забезпечити енергетичну стійкість вбудованих систем у критичній інфраструктурі за одночасного збереження конфіденційності та цілісності даних.*

Методика. *Дослідження проводилося з використанням спеціалізованого програмно-апаратного стенда, реалізованого у форматі Hardware-in-the-Loop на базі одноплатного комп'ютера Raspberry Pi 5, який виконував роль автономної апаратної платформи IoT. Програмну архітектуру розгорнуто у вигляді взаємодіючих Docker-контейнерів: сервісу обробки запитів (API), агента адаптивного управління (ASM) та модуля моніторингу. Для прийняття рішень застосовано контролер на базі нечіткої логіки типу Takagi-Sugeno нульового порядку. Вхідними лінгвістичними*

змінними слугували оцінка стану заряду підсистеми живлення та поточний рівень загрози, а вихідною – один із чотирьох визначених режимів безпеки. Для оцінювання витрат розроблено скалярну цільову функцію, що враховує затримку обробки, енергоспоживання електронного вузла та рівень безпеки. Динаміка роботи підсистеми живлення відтворювалася за допомогою емпіричної моделі логічного розряду, що пов'язує навантаження процесора зі швидкістю споживання енергії.

Результати. *Експериментальне тестування, проведене у чотирьох сценаріях тривалістю 120 с, підтвердило переваги адаптивного підходу порівняно зі статичними політиками безпеки. Встановлено, що фіксовані політики є нераціональними: застосування сильних алгоритмів (наприклад, AES-256) призводить до прискореного розряду підсистеми живлення під час інтенсивного трафіку, тоді як постійне використання спрощених режимів підвищує ризики вразливості пристроїв. Результати засвідчили, що у штатному режимі адаптивний підхід зменшує енергоспоживання електронного вузла приблизно на 7% порівняно з фіксованим максимальним захистом, гарантуючи при цьому перехід до найвищого рівня безпеки під час атаки. У критичному режимі низького заряду система реалізує стратегію виживання, утримуючи найменш енерговитратну конфігурацію апаратно-програмних засобів захисту. Це дозволяє знизити енергоспоживання на 40% та подовжити час автономної роботи апаратної платформи під навантаженням у 1,7 раз. Аналіз чутливості довів стабільність фізичних показників системи незалежно від зміни вагових коефіцієнтів цільової функції.*

Наукова новизна. *Удосконалено критерій оцінювання ефективності функціонування апаратних платформ IoT шляхом введення інтегральної цільової функції, яка формалізує компроміс між затримкою обробки, енерговитратами та конфігурацією захисту. Вперше запропоновано та експериментально обґрунтовано модель управління апаратно-програмними засобами захисту на базі нечіткої логіки, яка реалізує концепцію graceful degradation для вбудованих систем Інтернету речей. На відміну від існуючих рішень, ця модель динамічно узгоджує обмеження підсистеми живлення з потребою у підвищеному захисті, забезпечуючи пріоритет енергозбереження при критично низькому заряді та максимальний захист за наявності достатнього ресурсу.*

Практична значимість. *Практичне застосування запропонованого рішення дозволяє суттєво підвищити надійність та енергетичну живучість вбудованих систем та апаратних платформ IoT в умовах нестабільного електропостачання. Збільшення часу автономної роботи у критичних ситуаціях надає вікно можливостей, необхідне для передачі важливих тривожних сповіщень або очікування відновлення живлення. Розроблена архітектура дозволяє гнучко модифікувати сценарії управління та може бути легко імплементована на реальних електронних периферійних пристроях.*

Ключові слова: *вбудовані системи; апаратні платформи IoT; енергоспоживання електронних вузлів; підсистема живлення; апаратно-програмні засоби захисту.*