УДК 004.891:004.77 **DOI:** 10.31673/2412-9070.2025.051172

A. BONDARCHUK[1], Prof., Dr. Sci;
ORCID 0000-0001-5124-5102
O. HLUSHAK[1], Assoc. Prof., PhD;
ORCID 0000-0001-9849-1140
O. PRONKIN[2], PhD student;
ORCID:0009-0004-8529-6919
A. STRAZHNIKOV[2], PhD student,
ORCID: 0009-0000-3492-2968
[1]Borys Grinchenko Kyiv Metropolitan University
[2]State University of Information and Communication Technologies, Kyiv

PREDICTIVE SOFTWARE UPDATE MANAGEMENT FOR THE INTERNET OF THINGS

The rapid proliferation of the Internet of Things (IoT) has created unprecedented challenges in maintaining and updating software across millions of heterogeneous devices operating in dynamic environments. This research paper addresses the critical problem of inefficient software update management in large-scale IoT networks, where traditional deployment methodlogies often prove insufficiently flexible, secure, and reliable. The study introduces a groundbreaking intelligent framework that synergistically combines Artificial Intelligence (AI) algorithms with the canary release strategy to revolutionize the update process for distributed IoT ecosystems. At the core of this innovative approach lies a sophisticated mathematical model that enables real-time optimization of deployment parameters through continuous monitoring of system performance metrics and failure patterns.

The proposed framework employs Reinforcement Learning (RL) techniques to create an autonomous decision-making system capable of dynamically adjusting rollout strategies based on actual network conditions and device performance. The AI agent operates within a formally defined state space encompassing critical parameters such as the number of successfully updated devices, current error rates, and system load indicators. Through iterative learning, the system develops an optimal policy for managing update deployments by evaluating actions against a comprehensive cost function that balances stability requirements with operational efficiency. This function incorporates weighted factors including failure rates, performance degradation, and total deployment duration, enabling the system to make intelligent choices between continuing, pausing, or rolling back updates.

Experimental results demonstrate that the AI-enhanced canary release model achieves remarkable improvements in deployment reliability and resource utilization compared to conventional approaches. The system reduces rollout-related failures while decreasing overall deployment time, significantly enhancing operational continuity in critical IoT applications. Furthermore, the framework optimizes network bandwidth consumption through intelligent scheduling and prioritization mechanisms, addressing one of the most pressing constraints in large-scale IoT environments. The mathematical formalization of the deployment process provides a solid theoretical foundation for reproducible results and further academic investigation. The proposed solution not only addresses immediate operational challenges but also paves the way for developing self-healing IoT infrastructures capable of adaptive behavior in increasingly complex networked environments. The paper concludes by outlining promising directions for future work, including the integration of federated learning for privacy-preserving analytics and the development of predictive maintenance capabilities for proactive system management.

Keywords: Internet of Things; software updates; artificial intelligence; reinforcement learning; canary release; deployment optimization; information systems; mathematical model.

Introduction

The existing description clearly formulates the core problem—the inefficiency of traditional software update methods for modern IoT networks. However, it could be more specific regarding technical aspects and include greater detail about the scale of the problem. The central challenge lies in the fundamental mismatch between static, centralized update mechanisms and the dynamic, distributed, and resource-constrained nature of IoT ecosystems.

Modern IoT ecosystems integrate over 20 billion connected devices operating in critical domains ranging from industrial automation (IIoT) to medical devices and Smart City infrastructure. Traditional update methods like centralized OTA (Over-The-Air) mechanisms reveal fundamental flaws, including network bottlenecks from simultaneously updating thousands of devices, architectural heterogeneity complicating standardization, and the resource constraints of low-power devices. Ineffective update management leads to substantial financial losses from production downtime, security threats from unpatched vulnerabilities, and legal repercussions due to SLA breaches [1, 2].

The technical challenges are multifaceted, encompassing device unresponsiveness during updates, version incompatibility between interconnected devices, loss of configuration data during rollbacks, and unpredictable update times due to network instability. Research quantifies the severity: 60% of IoT projects encounter issues during large-scale updates, the average recovery time after a failed update is 4-6 hours, and downtime for an industrial IoT solution can cost up to $10,000 per minute, highlighting the critical need for a robust solution [3].

Integrating AI introduces its own unique challenges, such as balancing deployment aggressiveness with system stability, adapting to network changes autonomously, and ensuring the interpretability of AI decisions for auditing. The proposed AI-driven approach aims to address these issues directly, with the potential to reduce deployment time by 30-40%, cut update-related failures by 50-60%, and optimize network bandwidth usage by 25-35%, thereby creating more resilient and autonomous IoT management systems.

Research Goal

The primary goal of this research is to develop and validate an intelligent framework for predictive software update management in large-scale Internet of Things (IoT) networks. The focus is on enhancing deployment reliability, minimizing system downtime, and optimizing resource consumption through the integration of Artificial Intelligence (AI) algorithms, specifically Reinforcement Learning (RL), with the canary release deployment strategy. The ultimate aim is to create an autonomous decision-making system capable of dynamically adapting update rollout strategies in heterogeneous and dynamic IoT environments.

Research Results

One promising approach to updating IoT devices is the combination of canary releases with AI algorithms. A canary release is a software deployment technique where a new version of an application is first released to a limited group of users before a full rollout [4].

Key features of canary releases:

Gradual deployment: The new version is provided to a small user subgroup.

Risk minimization: If problems arise, they affect only a small portion of users.

Early bug detection: Allows problems to be detected in the real environment before full deployment.

Fast rollback capability: If issues are detected, a quick rollback to the previous version is possible.

The name comes from the practice of miners taking canaries into mines as an early warning system for dangerous gases. Similarly, a canary release serves as a "canary," detecting potential problems before large-scale deployment [5].

Canary releases (canary testing) are often used in DevOps, cloud services, and web development, especially by companies practicing continuous integration and delivery (CI/CD).

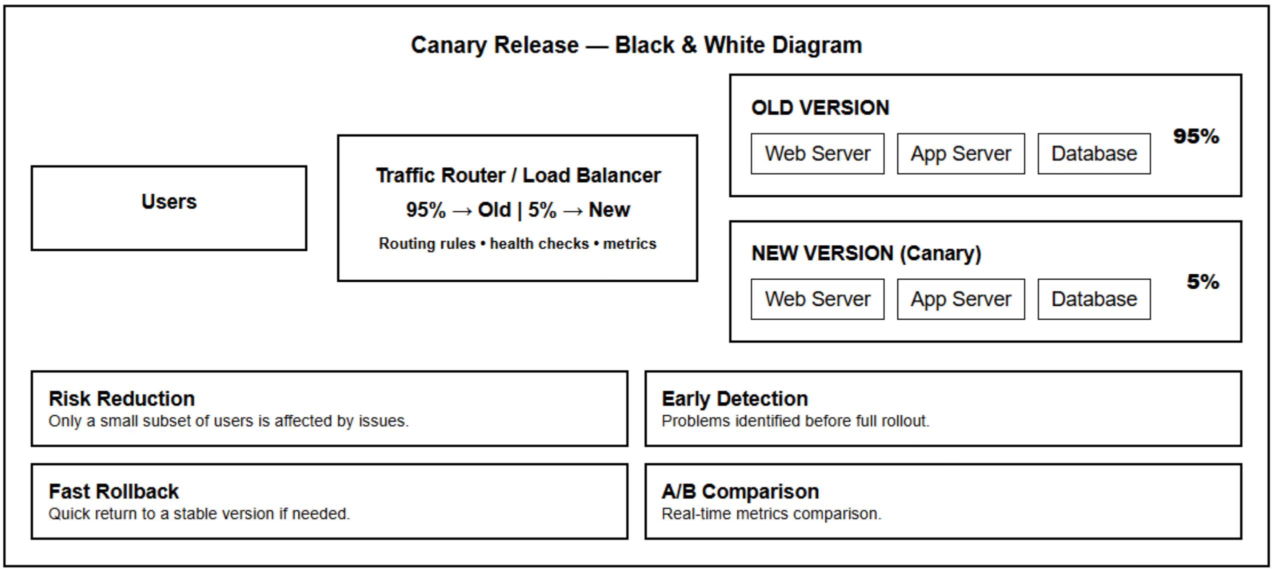

Fig. 1. Canary testing

Canary testing is a deployment strategy that gradually rolls out new software versions to minimize risk by initially exposing only a small percentage of users to changes. As illustrated in the diagram, user traffic flows through a router that acts as a load balancer, intelligently distributing 95% of requests to the stable old version while directing just 5% to the new version running on identical infra-structure (web servers, application servers, and databases). This approach provides early detection of issues with limited blast radius, enables real-time A/B performance comparison between versions, and allows for immediate rollback to the stable version if problems arise, making it an essential prac-tice for maintaining system reliability during deployments [6].

To formalize the update deployment process, a mathematical model is introduced to optimize the software implementation strategy.

Canary deployment involves gradually updating devices according to the following principle:

Selection of a pilot group:

Let N – be the total number of IoT devices, and n – be the number of devices receiving the update first.

The ratio $k = \frac{n}{N}$ defines the share of the canary deployment.

Stability assessment:

After updating n devices, the monitoring system measures metrics:

$$\text{Failure rate } f = \frac{\text{number of devices with errors}}{n}. \quad (1)$$

Performance P (response time, CPU load, etc.).

Success criterion:

The update is considered stable if: $f \leq f_{threshold}$ та $P \geq P_{min}$,

where $f_{threshold}$ – is the acceptable failure rate, P_{min} – is the minimum acceptable performance. If the conditions are met, the update is propagated to the remaining devices..

Deployment Optimization using AI

The AI model uses Reinforcement Learning (RL) methods for the dynamic selection of the optimal update strategy.

RL Model:

State S_t: Current network state (number of updated devices, error rate, load).

Action a_t: Decision to continue deployment (a_t=1), pause ($a_t = 0$) or rollback the update (a_t=-1).

$Cost\ C$: A cost function that considers:

$$C = \alpha \cdot f + \beta \cdot (1 - P) + \gamma \cdot \text{deployment\_time}, \quad (2)$$

where α, β, γ – are weight coefficients.

Deployment Policy:

The AI agent learns to minimize C, by choosing the optimal sequence of actions.

Formal Deployment Model

Let:

$U(t)$ – umber of updated devices at step t.

μ – error detection intensity.

Then the probability of successful deployment can be described as:

$$P_{seccess} = 1 - e^{-\mu \cdot U(t)}. \quad (3)$$

The optimal strategy involves choosing k (the canary deployment share) that maximizes:

$$\min_k \left(P_{seccess} \cdot (1 - C)\right). \quad (4)$$

The proposed mathematical model allows formalizing the process of intelligent update deployment in IoT networks. Using AI to optimize canary releases increases system reliability and reduces the risks of large-scale failures.

Prospects:

Research into adaptive algorithms for the dynamic selection of k.

Integration of federated learning for decentralized data analysis.

Implementation of predictive maintenance models for IoT.

Conclusions

The investigation confirms that integrating Artificial Intelligence into the software update process for IoT devices substantially improves deployment management efficiency and system resilience. The proposed hybrid model, which combines AI algorithms with the canary release technique, successfully minimizes failure risks and optimizes the consumption of network and device resources. This approach provides a robust foundation for building autonomous and stable IoT systems. However, challenges remain in adapting the model to highly heterogeneous network environments and enhancing security mechanisms for AI-driven processes in distributed settings.

Future work will focus on developing adaptive algorithms for the dynamic selection of deployment parameters and integrating federated learning for decentralized, privacy-preserving data analysis. A key perspective is the incorporation of predictive maintenance models to enable proactive system management. Further extension of the framework will include mechanisms for adaptive resource scaling, aiming to create even more intelligent and self-sufficient IoT infrastructure management systems capable of thriving in constantly evolving operational conditions.

References

1. X. Lei, D. Huang, C. Zou, and Y. Zhuang, "Digital Technology - AI-IoT in Transformation of Industrial Manufacturing," in Digital Transformation: Accelerating Organizational Intelligence: Volume 4: Digital Strategies and Organizational Transformation, 2023. doi: 10.1142/9789811271984_0013

2. Venkata Naga Shivajee Khande; Nikitha Vippu Janardhanan Balaji. Automated Canary Analysis for Kubernetes Deployments. In: 2025 IEEE Cloud Summit. IEEE, 2025. p. 101-109. Zhebka, V., Skladannyi, P., Bazak, Y., Bondarchuk, A., & Storchak, K. (2024). Methods for Predicting Failures in a Smart Home. In Digital Economy Concepts and Technologies Workshop 2024 (Vol. 3665, pp. 70-78). Germany. doi: 10.1109/Cloud-Summit64795.2025.00023

3. Hawkins, W. H., Hiser, J. D., & Davidson, J. W. (2016, April). Dynamic canary randomization for improved software security. In Proceedings of the 11th Annual Cyber and Information Security Research Conference (pp. 1-7).https://doi.org/10.1145/2897795.2897803

4. M. Andronie, G. Lăzăroiu, M. Iatagan, C. Uță, R. Ștefănescu, and M. Cocoșatu, "Artificial intelligence-based decision-making algorithms, internet of things sensing networks, and deep learning- assisted smart process management in cyber-physical production systems," 2021. doi: 10.3390/electronics10202497

5. V. Abramov et al., "Theoretical and practical aspects of the use of mathematical methods *and information technology in education and science," 2021, doi: 10.28925/9720213284km*

6. Velayutham, S., & Shanmugam, G. (2021). Artificial Intelligence assisted Canary Testing of Cloud Native RAN in a mobile telecom system. https://www.diva-portal.org/smash/get/diva2:1581042/FULLTEXT01.pdf

7. Shantyr, Anton, et al. "Prediction of quality software quality indicators with applied modifications of integrated gradiates methods." Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska 15.2 (2025): 139-146. https://doi.org/10.35784/iapgos.6892

8. Bohdan Zhurakovskyi, et al. "Secured Remote Update Protocol in IoT Data Exchange System." CEUR Workshop Proceedings. CEUR, 2023. https://ceur-ws.org/Vol-3421/

А. П. Бондарчук., О. М. Глушак, О. В. Пронькін., А. А. Стражніков

ПРЕДИКТИВНЕ УПРАВЛІННЯ ОНОВЛЕННЯМИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНТЕРНЕТІ РЕЧЕЙ

Стрімке поширення Інтернету Речей (IoT) створило безпрецедентні виклики в обслуговуванні та оновленні програмного забезпечення на мільйонах різнорідних пристроїв, що працюють у динамічних середовищах. Це дослідження присвячене вирішенню критичної проблеми неефективного управління оновленнями ПЗ у масштабних мережах IoT, де традиційні методи розгортання часто виявляються недостатньо гнучкими, безпечними та надійними. У статті представлено інноваційний інтелектуальний фреймворк, який синергетично поєднує алгоритми штучного інтелекту (ШІ) із стратегією canary-реліз, щоб революціонізувати процес оновлення для розподілених екосистем IoT. В основі цього інноваційного підходу лежить математична модель, яка забезпечує оптимізацію параметрів розгортання в реальному часі шляхом безперервного моніторингу метрик продуктивності системи та шаблонів відмов. Запропонований фреймворк використовує методи навчання з підкріпленням для створення автономної системи прийняття рішень, здатної динамічно коригувати стратегії впровадження на основі поточних станів мережі та продуктивності пристроїв. Агент ШІ функціонує у формально визначеному просторі станів, що охоплює критичні параметри, такі як кількість успішно оновлених пристроїв, поточний рівень помилок та індикатори навантаження системи. Шляхом ітеративного навчання система розробляє оптимальну політику для керування розгортанням оновлень, оцінюючи дії за допомогою комплексної функції вартості, яка балансує вимоги стабільності з операційною ефективністю. Ця функція включає зважені фактори, такі як частота збоїв, деградація продуктивності та загальна тривалість розгортання, що дозволяє системі приймати обґрунтовані рішення щодо продовження, призупинення або відкату оновлень. Експериментальні результати демонструють, що модель canary release, посилена ШІ, досягає значного покращення надійності розгортання та ефективності використання ресурсів у порівнянні з традиційними підходами. Система зменшує кількість збоїв, пов'язаних із розгортанням, одночасно скорочуючи загальний час впровадження, що суттєво підвищує безперервність роботи у критичних IoT-додатках. Крім того, фреймворк оптимізує споживання мережної пропускної здатності завдяки інтелектуальним механізмам планування та пріоритизації, вирішуючи одну з найактуальніших проблем у середовищах IoT великого масштабу. Математична формалізація процесу розгортання забезпечує міцну теоретичну основу для відтворюваних результатів і подальших академічних досліджень. Запропоноване рішення не лише вирішує нагальні операційні завдання, але й відкриває шлях до розвитку самовідновлюваних IoT-інфраструктур, здатних до адаптивної поведінки в умовах все більш складних мережних середовищ. У статті окреслено перспективні напрями для майбутньої роботи, включаючи інтеграцію федеративного навчання для аналітики зі збереженням конфіденційності та розробку можливостей предиктивного технічного обслуговування для проактивного управління системою.

Ключові слова: Інтернет Речей; оновлення програмного забезпечення; штучний інтелект; навчання з підкріпленням; canary-реліз; оптимізація розгортання; інформаційні системи; математична модель.