МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА, УКРАЇНА

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ, УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ ІРАКУ
AL-RAFIDAIN UNIVERSITY, ІРАК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ПОЛЬЩІ
УНІВЕРСИТЕТ НАЦІОНАЛЬНОЇ КОМІСІЇ З ОСВІТИ В КРАКОВІ, ПОЛЬЩА

V Міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”

«TTSIIT - 2026»

29-30 січня 2026 р.
Україна-Ірак-Польща

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
LUHANSK NATIONAL UNIVERSITY
NAMED AFTER TARAS SHEVCHENKO, UKRAINE

STATE UNIVERSITY OF TRADE AND ECONOMICS, UKRAINE

IRAQ MINISTRY OF EDUCATION
AL-RAFIDAIN UNIVERSITY, IRAQ

POLISH MINISTRY OF EDUCATION AND SCIENCE
UNIVERSITY OF THE NATIONAL COMMISSION ON EDUCATION IN KRAKOW, POLAND

The V International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things

«TTSIIT - 2026»

January 29th - 30th 2026
Ukraine-Iraq-Poland

Рекомендовано рішенням Вченої ради ДЗ „Луганський національний університет імені Тараса Шевченка” протокол №7 від 30.01.2026 р.

Відібрані оргкомітетом доповіді, після допрацювання, можуть бути опубліковані у виданні, яке індексується в наукометричній базі Scopus.

РЕДАКЦІЙНА КОЛЕГІЯ:

Конференція проведена за організаційної, інформаційної та технічної підтримки кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ (завідувачка кафедри доктор філософії, доцент Альона Десятко, технічний супровід – Ярослав Шестак).

Організатор та модератор конференції д.т.н., проф. Юрій Хлапонін

ЗМІСТ

INTRODUCTORY WORD

Olena Karaman

Prof. Dr., rector of Luhansk National University named after Taras Shevchenko

Dear conference participants, dear educators, researchers, students, postgraduate and doctoral candidates, and our valued colleagues and partners from Ukraine, the Republic of Poland, the Republic of Iraq, the United Kingdom, and other countries,

On behalf of Luhansk Taras Shevchenko National University, I am pleased to welcome you to this international scientific and practical conference. I would also like to express our sincere appreciation to our international partners for their strong support of Ukraine, the Ukrainian people, and the Ukrainian academic community in the context of the ongoing war and our struggle for fundamental values — freedom, independence, sovereignty, and democracy.

The world is currently experiencing a new stage of technological transformation, and your research and professional activities play a key role in shaping its future.

The intellectual industry and the Internet of Things are not merely technological concepts; they represent the core of a rapidly evolving global economy.

This conference brings together key directions in the development of the digital society — from fundamental research in computer science to the practical application of information technologies across various domains.

I believe that today's conference is more than an exchange of research findings. It serves as a platform for dialogue and cooperation between science, industry, and public institutions.

I wish all participants engaging discussions, new insights, and meaningful strategic connections.

May your ideas become the basis for real projects that will transform the world and our countries.

We wish you productive work and every success on the path toward building an intellectual future.

Olena Karaman

ВСТУПНЕ СЛОВО

Олена Караман
доктор педагогічних наук, професор,
ректор Луганського національного університету
імені Тараса Шевченка

Шановні учасники науково-практичної конференції, дорогі освітяни, науковці, студенти, аспіранти, докторанти, наші надійні друзі і партнери з України, Республіки Польща, Іракської республіки, Великобританії та інших країн!

Дозвольте привітати всіх від імені Луганського національного університету імені Тараса Шевченка та подякувати іноземним партнерам за величезну підтримку України, українського народу, українських освітян і науковців у кривавій боротьбі з російським агресором за найвищі загальнолюдські й національні цінності – свободу, незалежність, суверенітет, демократію!

Сьогодні світ переживає чергову технологічну революцію, і саме ви є тими, хто формує її архітектуру.

Інтелектуальна індустрія та Інтернет речей – це не просто терміни, це фундамент нової глобальної економіки.

Наша конференція об’єднує найактуальніші вектори розвитку цифрового суспільства: від фундаментальних основ комп’ютерних наук до прикладного впровадження інформаційних технологій у кожну сферу нашого життя.

Я впевнена, що сьогоднішня подія – це не просто обмін доповідями – це майданчик для синергії науки, бізнесу і держави.

Бажаю всім учасникам цікавих дискусій, нових інсайтів та стратегічних знайомств. Нехай ваші ідеї стануть основою для реальних проєктів, що змінять світ і наші країни!

Бажаємо плідної роботи та успіхів на шляху до створення інтелектуального майбутнього!

Олена Караман

PERFORMANCE ANALYSIS OF A PRODUCTION LINE USING COMPUTER MODELLING AND SIMULATION

Kamil KALISZ (Student)[1]
Karina JANISZ (PhD Eng., Assistant Professor)[1]
Kamila KLUCZEWSKA-CHMIELARZ (PhD, Professor at UKEN)[2]

[1]*University of Applied Sciences in Nowy Sącz, Poland, Faculty of Engineering Sciences, Field of study: Mechatronics, email: kalisz.kamil23@gmail.com, kjanisz@ans-ns.edu.pl*
[2]*University of the National Education Commission in Kraków (UKEN), Institute of Technical Sciences Poland, kamila.kluczewska-chmielarz@uken.krakow.pl*

Summary
This paper presents a performance analysis of a production line in a company manufacturing electrical modules. The analysed manufacturing system was modelled and simulated in FlexSim. Based on the simulation results, the main operational issues on the investigated line were identified and practical measures were proposed to remove the bottleneck and increase line throughput in line with customer demand.

Introduction

Modelling and simulation of processes are increasingly used to improve manufacturing systems [5]. Production-line modelling and simulation are key tools for implementing the Industry 4.0 concept, especially in digital twins as well as flexible automation and quality assurance. Companies and academic centres use both commercial and research software, e.g., Tecnomatix Plant Simulation, FlexSim, and AnyLogic. Recent literature documents many applications of modern simulation packages for production-line optimisation in the Industry 4.0 context. Case studies report, among others: identification of process bottlenecks [1, 7], improved productivity [2], analysis of workstation loading [6], and increased machine utilisation [3].

Methodology

The computer model and simulation study were developed in FlexSim based on collected input data. The simulation model was built following a detailed analysis of the investigated production process, carried out within a diploma thesis [4]. The specific objectives were to identify bottlenecks in the production line, to verify whether the customer requirements can be met within the assumed time horizon, and to assess how potential changes influence line performance. A baseline simulation model reflecting the current state was prepared, followed by an improved model aimed at removing the identified bottleneck and achieving the required line throughput.

- collection of input data,
- development of the computer model and its verification,
- model simulation and analysis of simulation outputs.

Application example

The company where the production line was analysed operates in the electrical manufacturing sector. The line produces a large-size power supply module. The manufacturing process starts with collecting the required materials. Each component undergoes incoming inspection, during which key dimensions and conformity with the technical documentation are checked. The inspected parts are transported to the warehouse. The next stage is the main assembly process. After assembly, quality control is performed. In the final step, the product is packed and moved to the finished-goods warehouse. To handle the transport of large and heavy modules, the company uses two forklift trucks. The customer requires 75–80 modules per month. The plant operates in a single-shift system, five days per week, 8 hours per day, including one 30-minute break [4].

In line with the adopted methodology, in the second step of the analysis, data on the processing times of individual operations were collected. Next, a production-line model was created in FlexSim (Fig. 1), taking into account the shop-floor layout. The model reflects material flow from the receiving zone, through successive process stages, to the storage area. The flow item (workpiece carrier) serves as the base on which assembly is performed at each stage. The dimensions of the power supply module were represented in the model accordingly. The incoming inspection workstation is the first process step, supplied with material from the source. The main production line was designed as a cellular (work-cell) layout. It consists of four interconnected assembly stations: bracket assembly, busbar assembly, cable-tray assembly, and cable assembly. After leaving the main line, the product is routed to testing and final inspection, then to packing, and finally to the warehouse. Transport between these stages is carried out by a forklift truck moving along a predefined route. The shipping process to the customer was excluded from the model; placing the pallet in the warehouse was assumed as the end of the production cycle. In the next step, the model logic was verified for correct operation. The production line was then simulated over a full month. The simulation results showed that 57 finished modules were delivered to the warehouse. The analysis indicates that the line is not balanced. Busbar assembly was identified as the critical constraint limiting the throughput of the entire line. Operations upstream of the bottleneck exhibited long blocked states and work-in-process accumulation, while downstream processes did not utilise their available capacity.

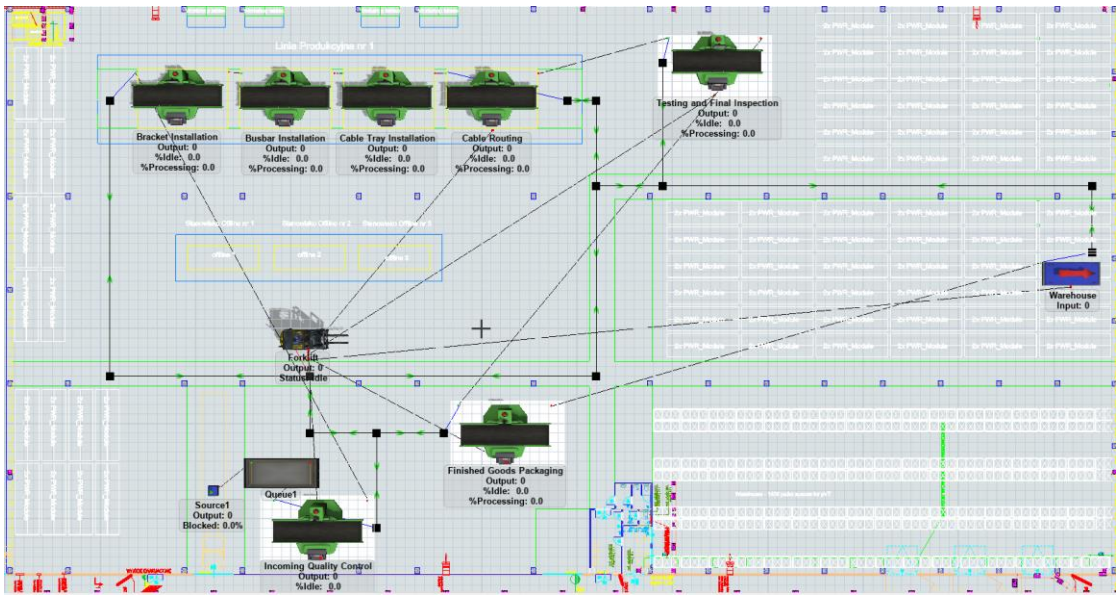


Fig. 1. Production line model [4]

Based on the analysis and the identified bottleneck, simple improvements were proposed for selected operations, together with relocating the packing station and the finished-goods storage area. The improvements were intended to reduce processing times at key stages and to improve flow continuity.

) utilisation before improvements
) utilisation after improvements

Fig. 2. Workstation utilisation analysis [4]

New operation times for individual process stages were defined and implemented in the modified simulation model. The results show that, after introducing the improvements, the output reached 78 units (i.e., 21 products more than in the first simulation). Moreover, by changing the workstation arrangement, internal transport was reduced, which decreased the total forklift travel distance (from 34,4 [km] to 25,66 [km]), resulting in potential savings. A comparison of resource utilisation before and after implementing the improvement concept was also performed (Fig. 2). The blocked state at incoming inspection decreased from 67,18% to 54,43%. At the second stage (bracket assembly), the share of effective working time increased from 62,33% to 94,78%, and the blocked state decreased from 37,67% to 5,22%.

At subsequent stages, a clear increase in productive time was also observed, which indicates better performance of these operations.

Conclusions

By carrying out a computer simulation study that incorporated the proposed line improvements, the bottleneck related to busbar assembly was removed and the possibility of achieving the expected line throughput was demonstrated.
Resource utilisation across individual workstations increased, which translated into smoother flow and higher effective line capacity. In future work, FlexSim can be considered for presentation, simulation, and further optimisation of the analysed line. Process modelling and simulation can therefore support efficient production management. This is possible because simulation experiments can be performed without stopping ongoing manufacturing.

REFERENCES

1. DI-YU L., FENGLIAN J., CHENG-FU Y.Simulation and Optimization of Production Scheduling in Multivariety Small-batch Mixed-flow Assembly Workshops Using IoT. Sensors and Materials, Vol. 37, No. 4, 2025
2. DUBAJ K.: Praktyczne zastosowanie narzędzia Flexsim w modelowaniu symulacyjnym systemów produkcyjnych, Zeszyty Naukowe Akademii Górnośląskiej Nr 6/2023, s. 23 – 31.
3. DUDEK A., STANIEWSKA E. (red.): Potencjał innowacyjny w inżynierii materiałowej i zarządzaniu produkcją. Leśniewski A i in.: Wpływ wybranych czynników na polepszenie wskaźnika OEE na wybranym odcinku procesu produkcyjnego, Wydawnictwo Politechnika Częstochowska, 2023.
4. KALISZ K.: Analiza modelu linii produkcyjnych z zastosowaniem oprogramowania do symulacji komputerowych. Praca dyplomowa na kierunku Mechatronika, Akademia Nauk Stosowanych w Nowym Sączu, 2026
5. KUKLA S.: Symulacja, wizualizacja i racjonalizacja systemów produkcyjnych. Enterprise Management Volume 27. Number 1. June 2024, pp. 24–28.
6. SKIBIŃSKA K., IWAŃKOWICZ R.: System optymalizacji obsady stanowisk dla procesów produkcyjnych. Management and Quality, Vol 6 No 3, 2024
7. WU G., YAO L., YU S.: Simulation and optimization of production line based on FlexSim, DOI: 10.1109/CCDC.2018.8407704

DETECTION OF HIDDEN THREATS IN IOT SYSTEMS BASED ON KLEPTOAUDIT AND FUZZY RISK ASSESSMENT

Yuriy PIDLISNYI (PhD student)
Mykhailo SHELEST (Doctor of Science, Professor)

Chernihiv Polytechnic National University, Ukraine
Yuriy Pidlisnyi (e-mail: ypodlesny@ukr.net)

Abstract

The paper examines an approach to detecting hidden threats in IoT systems, in particular cryptographic anomalies and kleptographic backdoors, based on the combination of cryptographic audit and klepto-audit with subsequent fuzzy risk assessment. Cryptographic audit is understood as a technical verification of cryptographic components of IoT devices (RNG/DRBG, key management, algorithms, protocols) using static, dynamic, and behavioral-statistical analysis methods. Klepto-audit is understood as the verification of trust controllability at the architectural level: the origin and reproducibility of updates, the supply chain, trust anchors, rules for changing truth, and zones of insufficient evidential assurance. The results of both layers are formalized in the form of indicators and integrated into a fuzzy-logic-based risk assessment model. It is shown that such an approach increases sensitivity to "silent" threats in heterogeneous and dynamic IoT environments, where classical signature-based and network methods are ineffective.

Introduction

The Internet of Things (IoT) is being actively deployed in critical and mass application domains, which leads to increased requirements for ensuring the information security of such systems [1,2]. A distinctive feature of IoT environments is the use of resource-constrained devices, simplified protocols, and third-party hardware–software components, which complicates the implementation of full-fledged control mechanisms [3]. A separate category of threats in IoT systems is constituted by hidden controllability threats that may be embedded at the stages of design, manufacturing, or firmware updating of devices [4–5]. This concerns not only "weak cryptography," but situations in which a system formally operates correctly while allowing intentional hidden influence (kleptographic backdoors, parameter manipulation, trigger-based modes, hidden control channels). Such threats often do not manifest as classical network attacks and may remain undetected by traditional intrusion detection systems [6].

In this context, the combination of two complementary approaches is relevant:

1) *cryptographic audit* as a systematic technical verification of the correctness of selection, implementation, and configuration of cryptographic mechanisms in IoT;
2) *klepto-audit* as an assessment of trust controllability and potential hidden control mechanisms in IoT architectures (trust anchors, update and supply provenance,

reproducibility, telemetry/logging, access policies, and rules of "truth"). It addresses not the question of "whether the cryptography is strong," but rather "who and how can covertly control trust."

The results of both layers should be interpreted using methods that account for uncertainty and context, in particular fuzzy logic. Fuzzy assessment makes it possible to combine quantitative indicators (configuration/security metrics) and qualitative expert judgments (signs of controllability, opacity of provenance), transforming them into a unified risk profile with gradations of "low–medium–high" without requiring complete data.

Hidden Threats in IoT Systems

Unlike classical attacks, hidden threats in IoT systems are often implemented through the intentional weakening of cryptographic mechanisms or the introduction of covert control channels. Such threats include the use of random number generators with reduced entropy; embedded mechanisms enabling key predictability; context-dependent or trigger-based modifications of cryptographic algorithms; and hidden parameters within cryptographic exchange protocols. The key distinction of hidden threats lies in the fact that they are *weakly observable*: their effects may manifest rarely, conditionally (trigger-based), or only for a specific actor who possesses a "controllability secret" [6]. Therefore, the detection of such threats requires not only the analysis of code and algorithms, but also an assessment of the *conditions enabling hidden control*: who is able to modify firmware, how updates are delivered, whether the provenance of builds is reproducible, where trust keys are located, which exceptions are permitted, and how they are accounted for.

IoT Device Audit Model Cryptographic Layer and Klepto-Audit

To detect hidden threats, this work employs an audit model (Fig. 1) focused on the analysis of key cryptographic components of an IoT device, in particular random number generators, key management mechanisms, cryptographic algorithms, and protocols.

Cryptographic audit is implemented as a multi-level process and includes:

- *static analysis* aimed at identifying atypical constructs and parameters in the implementation of cryptographic mechanisms.
- *dynamic analysis* that enables the investigation of the behavior of cryptographic components during execution and the detection of trigger-based mechanisms.
- *behavioral-statistical* analysis focused on assessing the entropy, distributions, and correlations of cryptographic parameters.

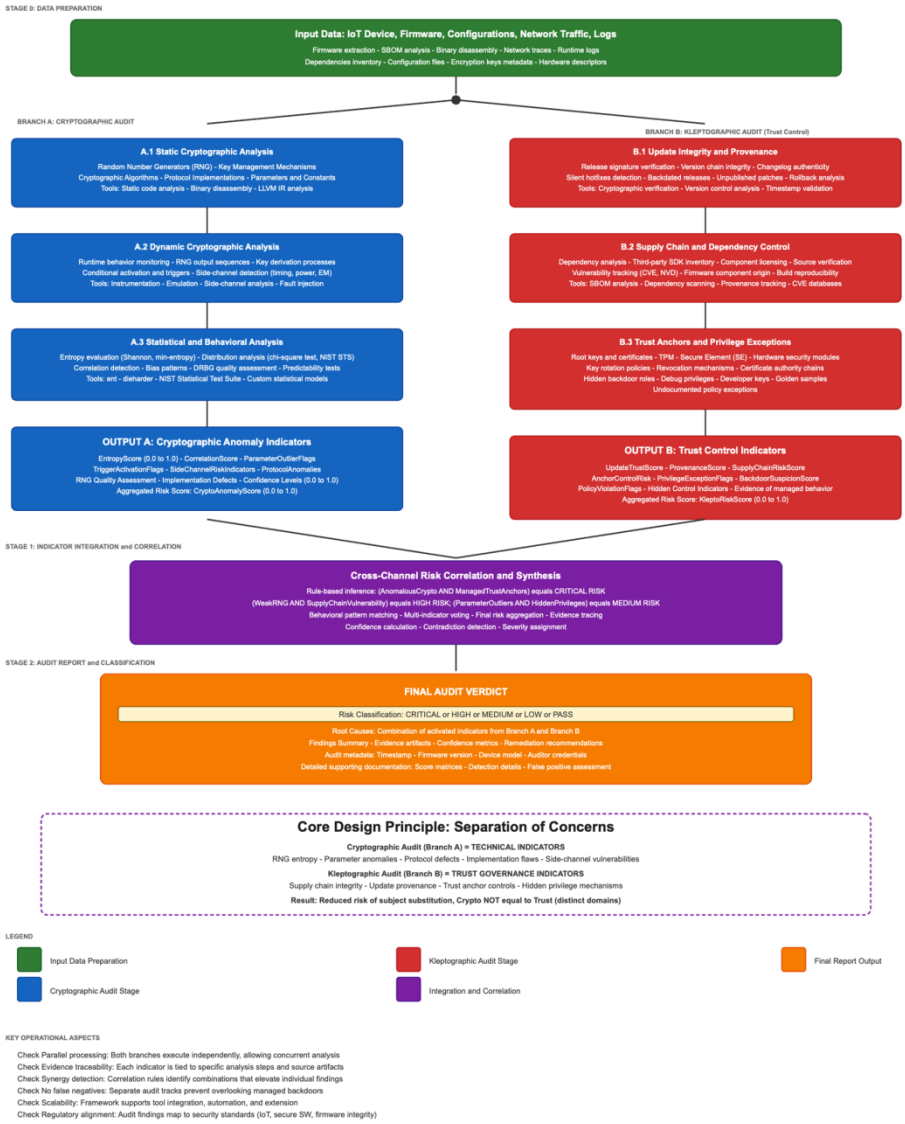


Fig. 1 – Conceptual architecture for detecting hidden threats in IoT systems: integration of cryptographic audit, klepto-audit (trust controllability), and fuzzy risk assessment

At the same time, this is insufficient for IoT environments: even "correct" cryptography may be embedded within a controllable trust loop. Therefore, the model is complemented by klepto-audit—an assessment of architectural conditions enabling hidden control, in particular:

- the provenance and immutability of updates (release signing, provenance, and the possibility of "silent" hotfixes)
- supply chain control (dependencies, components, firmware, third-party SDKs)
- inventory of trust anchors (root keys/certificates/trust modules) and the rules for changing «truth»
- the presence and accounting of exceptions and privileges that effectively allow

The results of cryptographic audit and klepto-audit are formalized in the form of two types of *indicators*:

1) indicators of cryptographic anomaly (entropy, correlations, atypical parameters)

2) indicators of trust controllability (updates, provenance, supply chain, anchors/exceptions). This reduces the risk of subject substitution: “cryptographic audit” addresses technical indicators, while “klepto-audit” addresses the conditions enabling hidden control.

Figure 1 presents the conceptual architecture of the proposed approach. A fundamental aspect is the separation of two levels of analysis. Cryptographic audit performs a technical verification of the implementations of cryptographic mechanisms of an IoT device and is aimed at detecting anomalies in random number generation, key management, and algorithms. Klepto-audit, in turn, focuses on the architectural level and assesses trust controllability: the provenance of updates, supply chain control, trust anchors, and exceptions that may enable hidden influence without formally violating cryptographic protocols. The results of both layers are integrated into a fuzzy inference module, which enables the assessment of risks associated with hidden threats under conditions of uncertainty inherent to IoT environments.

Integration of Audit Results with Fuzzy Risk Assessment

Given the uncertainty and variability of IoT environment parameters, audit results should be interpreted using intelligent methods. In this work, a fuzzy-logic-based risk assessment model is applied for this purpose [7]. The indicators obtained from cryptographic audit and klepto-audit are used as input linguistic variables of the fuzzy model, which makes it possible to account for fuzzy boundaries between normal and anomalous states, as well as ambiguity of interpretation in heterogeneous IoT domains. The fuzzy rule base is constructed on the basis of expert knowledge and reflects typical “silent” threat scenarios: for example, a combination of medium cryptographic anomaly with high controllability of updates may yield a higher integrated risk assessment than “cryptographic noise” without signs of controllability. The outcome of fuzzy inference consists of local and integrated risk estimates, as well as explanatory information regarding dominant risk factors, which enhances the interpretability of audit results and their suitability for practical application (selection of countermeasures, prioritization of inspections, and requirements for provenance assurance) [8].

Conclusions

The theses propose an approach to detecting hidden threats in IoT systems based on the combination of cryptographic audit and klepto-audit with subsequent fuzzy risk assessment. The proposed model makes it possible to integrate the results of technical analysis of cryptographic components and the assessment of trust controllability into a decision-support system for IoT security. It is fundamentally important that cryptographic audit and klepto-audit are not interchangeable: the former identifies

technical anomalies and errors in cryptographic mechanisms, whereas the latter evaluates trust controllability at the architectural level (update provenance, supply chain, trust anchors, exceptions), that is, the structural conditions for hidden control even in the presence of formally correct cryptography. Unlike existing approaches, this work for the first time formalizes klepto-audit as a separate layer for assessing trust controllability in IoT systems and integrates it with cryptographic audit into a unified fuzzy risk assessment model. Further research is planned to focus on experimental validation of the approach using real-world datasets, as well as on expanding the fuzzy rule base to improve the accuracy of hidden threat detection in update, supply chain, and trigger-based behavior scenarios.

REFERENCES

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. *Computer Networks*. 2010. Vol. 54, No. 15. P. 2787–2805. DOI: 10.1016/j.comnet.2010.05.010.
2. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*. 2015. Vol. 76. P. 146–164. DOI: 10.1016/j.comnet.2014.11.008.
3. Khan R., Khan S. U., Zaheer R., Khan S. Future Internet: The Internet of Things architecture, possible applications and key challenges. *2012 10th International Conference on Frontiers of Information Technology*. IEEE, 2012. P. 257–260. DOI: 10.1109/FIT.2012.53.
4. Young A., Yung M. Kleptography: Using Cryptography Against Cryptography. *Advances in Cryptology — EUROCRYPT'97*. Lecture Notes in Computer Science. Vol. 1233. Springer, Berlin, 1997. P. 62–74.
5. Shamir A. Cryptographic Security of IoT Devices: Threats and Challenges. *IEEE Security & Privacy*. 2018. Vol. 16, No. 3. P. 48–54. DOI: 10.1109/MSP.2018.2701166.
6. Шелест М., Ткач Ю. Клептографія: від бекдору до політики довіри у цифрову епоху : монографія. — Ніжин, ТПК «Орхідея», 2025. - 312 с.
7. Zadeh L. A. Fuzzy sets. *Information and Control*. 1965. Vol. 8, No. 3. P. 338–353. DOI: 10.1016/S0019-9958(65)90241-X.
8. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. Geneva: ISO, 2018.

A LIGHTWEIGHT WIND SIMULATION METHOD FOR TRAINING UAV CONTROL MODELS

Roman TREMBOVETSKYI (Postgraduate, assistant)[1]
Inna ROZLOMII (PhD, associate professor)[2]

[1]*Cherkasy State Technological University, Cherkasy, Ukraine*
roman.tremb@gmail.com, inna-roz@ukr.net

Abstract

Developing robust autonomous UAVs requires overcoming the "sim-to-real" gap, where policies trained in static simulations fail under real-world disturbances. This paper presents a lightweight wind simulation method designed for efficient Deep Reinforcement Learning. By analytically superimposing turbulence, wind shear, thermal flows, and gusts, the model generates complex, non-linear environmental conditions without the computational overhead of fluid dynamics simulations. Experimental validation confirms that agents trained within this framework exhibit exceptional stability and a 97.1% navigation success rate, demonstrating that the proposed method effectively balances physical fidelity with the high-speed processing required for scalable policy optimization.

Introduction

The rapid advancement of Unmanned Aerial Vehicles (UAVs) has led to the increasing adoption of Deep Reinforcement Learning (DRL) for developing robust autonomous control systems. A critical challenge in this domain is the "sim-to-real" gap, where policies trained in idealized simulated environments fail to adapt to the stochastic and non-stationary nature of real-world atmospheric conditions [1]. Wind disturbances represent a primary source of environmental uncertainty, significantly affecting UAV stability and energy efficiency. While high-fidelity Computational Fluid Dynamics (CFD) simulations offer realistic wind modeling [2], their prohibitive computational cost makes them impractical for the data-intensive training loops required by DRL, which often necessitate millions of interaction steps [3]. Conversely, simplified models such as constant wind vectors, fail to capture complex aerodynamic effects like turbulence and gusts, leading to brittle control policies [4]. This paper addresses this trade-off by proposing a lightweight, analytically driven wind simulation method. Our approach models complex wind dynamics through the superposition of distinct physical components – turbulence, wind shear, thermal flows, and gusts – ensuring both high execution speed for assive parallel training and sufficient physical realism to enhance policy robustness.

Methodology

To balance physical fidelity with computational efficiency, a composite wind model was developed that operates analytically rather than relying on computationally intensive fluid dynamics simulations. The total wind velocity vector V_w at any spatial

point *r=(x,y,z)* and time *t* is defined as the superposition of four distinct atmospheric components:

$$V_w(r,t) = V_t + V_s + V_h + V_g(t), \quad (1)$$

where V_t is the turbulence component, V_s is the wind shear, V_h is the thermal flows, and V_g is the wind gusts.

Turbulence (V_t) utilizes a simplified Dryden model [5] to introduce stochastic fluctuations by filtering white noise $\omega(t)$:

$$s_i(t+\Delta t) = s_i(t) + \frac{\Delta t}{\tau_i + \Delta t}(w_i(t) - s_i(t)), \quad (2)$$

where τ_i represents the time constant dependent on the mean wind speed. This approach introduces necessary randomness without the heavy computational cost of complex fluid equations.

Wind shear (V_s) is implemented to replicate the atmospheric boundary layer effect, where wind speed increases with altitude. This spatial dependency is modeled using the power-law equation, where the wind speed at height z is determined relative to a reference height z_r and a roughness parameter α:

$$k(z) = \begin{cases} \left(\frac{z}{z_r}\right)^{\alpha}, z > z_r \\ \frac{z}{z_r}, z \le z_r \end{cases} \quad (3)$$

This component ensures the simulation captures the varying aerodynamic forces a drone experiences during ascent and descent, preventing the policy from overfitting to a uniform wind field.Thermal flows (V_h) simulate convective updrafts arising from uneven surface heating. These are modeled as localized centers with a Gaussian distribution of intensity, generating strong vertical velocity vectors combined with weaker horizontal circulation. This creates zones of instability that are both time- and space-dependent, forcing the agent to adapt to sudden lift forces. Finally, wind gusts (V_g) are modeled as sudden, short-term changes in wind velocity to test the system's reactivity. A multi-frequency harmonic approach was employed, where the gust velocity is calculated as the sum of several sinusoidal functions with randomized amplitudes A_i and phases φ_i:

$$V_g(t) = \sum_i A_i sin\,(\omega_i t + \varphi_i) \quad (4)$$

This superposition results in a non-periodic and unpredictable disturbance pattern that is purely time-dependent, completing a comprehensive environmental model for robust policy training.

Implementation and Validation

The proposed lightweight wind simulation method was implemented within the PyFlyt framework, utilizing the PyBullet physics engine to ensure high-speed processing suitable for large-scale training. To validate the model's efficacy, Deep Reinforcement Learning agents (specifically Proximal Policy Optimization) were

trained in two distinct settings: a static baseline environment and the proposed dynamic environment featuring the composite wind model.

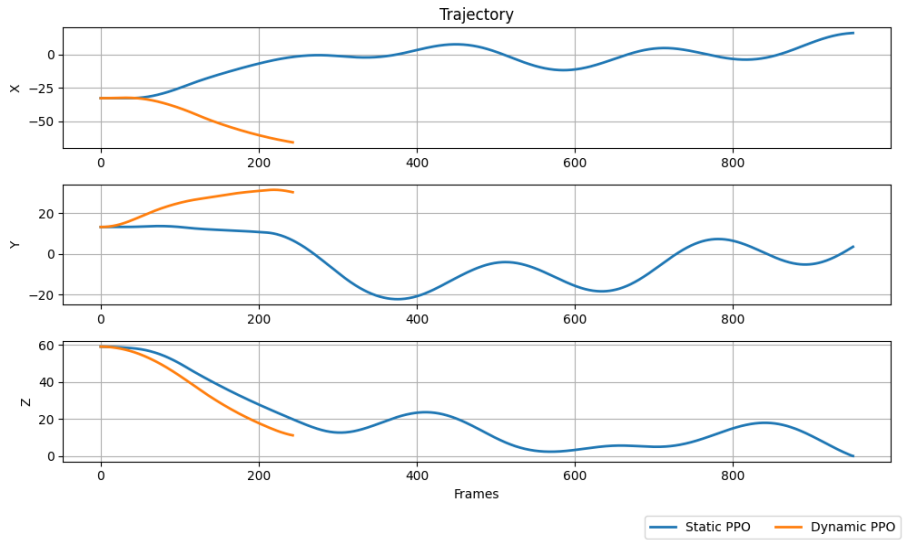


Fig. 1. Validation of the wind model efficacy

Trajectory comparison (Fig. 1) showing the destabilizing effect of modeled wind disturbances on a baseline agent (blue) versus the robust flight of an agent trained within the proposed environment (orange). Experimental results demonstrated a critical disparity in robustness. Agents trained in the static environment failed to adapt to the modeled disturbances, exhibiting unstable oscillatory behavior and a lower success rate in validation tests. Conversely, the agent trained using the proposed wind model achieved a 97.1% success rate, effectively compensating for turbulence and gusts. This confirms that the analytic superposition method provides sufficient physical fidelity to bridge the "sim-to-real" gap without the computational overhead of fluid dynamics simulations.

Conclusions

The study confirms that the proposed analytic wind simulation method effectively bridges the gap between the computational efficiency required for Deep Reinforcement Learning and the physical realism needed for robust control. By modeling complex aerodynamic effects such as turbulence, shear, thermals, and gusts – through mathematical superposition, we achieved a simulation environment capable of high-speed training without compromising the environmental stochasticity essential for policy generalization. Validation results demonstrated that agents trained within this framework exhibited superior stability and a 97.1% success rate, significantly outperforming baselines trained in static conditions. This approach offers a scalable and accessible soluti on for developing robust autonomous UAV systems, facilitating a more reliable transition from simulation to real-world deployment.

REFERENCES

[1] J. Wu, Y. Zhou, H. Yang, Z. Huang, and C. Lv, “Human-guided reinforcement learning with sim-to-real transfer for autonomous navigation,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 12, pp. 14745–14759, 2023.

[2] M. Mani and A. J. Dorgan, “A Perspective on the State of Aerospace Computational Fluid Dynamics Technology,” *Annual Review of Fluid Mechanics*, vol. 55, no. Volume 55, 2023, pp. 431–457, Jan. 2023, doi: 10.1146/annurev-fluid-120720-124800.

[3] B. S. Sarıkaya and Ş. Bahtiyar, “A survey on security of UAV and deep reinforcement learning,” *Ad Hoc Networks*, vol. 164, p. 103642, 2024.

[4] B. Ma *et al.*, “Deep Reinforcement Learning of UAV Tracking Control Under Wind Disturbances Environments,” *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1–13, 2023, doi: 10.1109/TIM.2023.3265741.

[5] R. S. Geronel, R. M. Botez, and D. D. Bueno, “Dynamic responses due to the Dryden gust of an autonomous quadrotor UAV carrying a payload,” *The Aeronautical Journal*, vol. 127, no. 1307, pp. 116–138, 2023, doi: 10.1017/aer.2022.35.

CRYPTOGRAPHIC MECHANISMS FOR PROTECTING IT DEVICES AGAINST UNAUTHORIZED ACCESS

Oksana MARKOVA (PhD in Pedagogical Sciences, Associate Professor)[2]
Iryna VDOVYCHENKO (PhD in Technical Sciences, Associate Professor)[3]

[1]Kryvyi Rih National University, Department of Computer Systems and Networks, markova@knu.edu.ua, vivin2015@knu.edu.ua

Summary

The article is devoted to addressing the problem of protecting IT devices from unauthorized access. The paper highlights the results of an analysis of the theoretical foundations of symmetric and asymmetric encryption as a basis for information security on physical media and in communication channels. The role of hardware security modules (HSM) in the process of generation and secure storage of cryptographic keys is defined. Mechanisms for validating digital certificates and protocols are demonstrated through a security analysis of the knu.edu.ua website.

The study provides a classification of the main threats countered by modern cryptographic standards and defines a threat actor model. Finally, the authors have developed practical recommendations for verifying and strengthening the protection of personal IT devices in everyday and educational activities.

Problem Statement

The relevance of cryptographic protection for IT devices has reached a critical level in 2026. This is no longer merely a matter of data «hygiene» but the very foundation of business survival and personal security.In the modern context of global

digitalization, the security of IT devices has ceased to be an exclusively technical task and has evolved into a strategic necessity. Given the rapid increase in the number of cyber threats–specifically Ransomware attacks and spyware, classified as critical cryptographic failures and system vulnerabilities traditional protection methods, such as password-only authentication, prove insufficient to counter modern methods of unauthorized access.

This necessitates the implementation of multi-layered security systems based on international standards for encryption and key management [11, 4].

The relevance of researching cryptographic mechanisms is driven by the following factors:

Dynamic nature of cyber threats: The continuous advancement of computing power requires a constant review of the robustness of existing algorithms. Utilizing the modern AES-256 standard is critical for ensuring the long-term security of data on physical media [11].

Protection of educational and scientific environments: Within the context of higher education institutions, particularly KNU, where confidential data is processed, the implementation of reliable digital certificates (Sectigo OV) is mandatory to maintain the chain of trust [5].

Transition to modern communication protocols: The use of outdated encryption methods leads to critical vulnerabilities. Implementing the TLS 1.3 protocol allows for the elimination of threats inherent in previous versions and ensures a higher level of user privacy [10].

Standardization of key management: The effectiveness of any security mechanism depends not only on the algorithm itself but also on the procedures for key generation and storage. Compliance with NIST recommendations allows for minimizing the risks of unauthorized access due to key compromise [4].

Thus, the study of modern cryptographic protection methods is essential for building a resilient security model capable of countering both network attacks and threats of physical access to IT infrastructure, aligning with the fundamental principles of constructing secure systems [12].

The aim of the study is to conduct a comprehensive analysis of modern cryptographic mechanisms that ensure the protection of IT devices against unauthorized access, as well as to investigate the practical state of implementation of these technologies using the web resources of educational institutions as a case study.

To achieve this aim, the following objectives must be addressed:

1. To analyze the theoretical foundations of symmetric and asymmetric encryption as a basis for information security on physical media and in communication channels.
2. To investigate the role of hardware security modules (TPM, Secure Enclave) in the process of generating and securely storing cryptographic keys.
3. To examine the mechanisms for validating digital certificates and TLS 1.3 protocols through a security analysis of the knu.edu.ua website..
4. To define the threat actor model and classify the primary threats countered by modern cryptographic standards (AES-256, SHA-256).

5. To develop practical recommendations for verifying and strengthening the protection of personal IT devices in everyday and educational activities.

Object of research: the process of protecting information resources of IT devices against unauthorized actions by threat actors. Subject of research: the set of cryptographic algorithms, authentication protocols, and digital certificate management methods.

1. Theoretical Foundations and Algorithms

1.1. Classification of Encryption Algorithms and Their Role in Data Protection

The security of modern IT devices is fundamentally based on a combination of symmetric and asymmetric encryption methods. For protecting data on physical media (disks), the de facto standard is the AES-256 algorithm [11]. It provides high data processing speeds with zero probability of being compromised by brute-force attacks on modern hardware. At the same time, cryptographic hash functions such as SHA-256 are used to verify information integrity and perform user authentication, which prevents unauthorized modification of system files [13].

Bruce Schneier notes that the security of a system depends not on the secrecy of the algorithm, but on the security of the keys [12]. In modern systems, asymmetric methods (for example, those based on elliptic curves) are used for this purpose, allowing two parties to establish a shared secret without its direct transmission over the network.

2. Hardware Security Modules and Secure Key Storage

To prevent key compromise, which is one of the most common causes of “cryptographic failures”[6], modern IT devices utilize hardware modules (TPM or Secure Enclave). These modules implement key management recommendations developed by NIST [13], ensuring the isolation of cryptographic operations from the main operating system–a feature that is critical when an adversary has physical access to the device.

3. Digital Certificate Validation Mechanisms

3.1. Analysis of the TLS Protocol and Certificate Validation Mechanisms

The primary mechanism for protecting data during transmission is the TLS 1.3 protocol [1]. Unlike previous versions, TLS 1.3 eliminates support for legacy hashing and encryption algorithms, significantly narrowing the attack surface. The connection validation process includes mandatory verification of the digital certificate, which confirms the server's authenticity through a chain of trust to root Certificate Authorities.

3.2. Case Study: Assessing the Security Status of the knu.edu.ua Web Resource

A practical security analysis of the knu.edu.ua website demonstrates the resource's compliance with current security standards. The site utilizes a certificate issued by the Sectigo Certificate Authority [5], employing the robust SHA-256 hashing algorithm. An analysis of technical details confirmed that the current cryptographic protection is valid until March 21, 2026 [5], after which the browser's automatic trust mechanisms will require a cryptographic signature update to prevent Man-in-the-Middle (MitM) attacks. This indicates a systematic approach by the administration toward managing

digital assets and protecting students' personal data within the distance learning process.

4. Defining the Threat Actor Model and Classifying Primary Threats

Developing a threat actor model and classifying threats is the foundation for building any Information Security System (ISS). Without this analysis, protection will be either insufficient or excessively costly and ineffective.

4.1. Defining the Threat Actor Model

A threat actor model (or adversary model) is an abstract or formalized description of an individual (or a group of individuals) who may intentionally or unintentionally cause harm to an information system. When developing the model, the following parameters are taken into account:

- Threat Actor Type;
- Skill Level;
- Motivation;
- Available Resources;
- Access Points.
- Threat Actor Categories by Access Level:
- External;
- Internal (Insiders).

4.2. Classification of Primary Threats

A threat is the potential possibility of violating the three fundamental properties of information: confidentiality, integrity, and availability (the CIA triad).

By Object of Impact: Confidentiality Threats, Integrity Threats, Availability Threats.

By Nature of Origin: Natural, Technological (Man-made), Anthropogenic (The Human Factor).

By Implementation Mechanism: Malware, Social Engineering, Technical Attacks, Physical Threats.

4.3. Specifics of the Threat Actor Model for Kryvyi Rih National University (KNU)

The threat actor model for Kryvyi Rih National University (KNU) is unique, as the institution functions simultaneously as an educational establishment, a research center, and a large-scale organization managing the personal data of thousands of individuals.

The development of this model accounts for the fundamental definitions of the NDTZI (Regulatory Documents on Technical Protection of Information) [3] and the NIST risk analysis methodology [4].

Below is an example of a structured threat actor model adapted to the specific needs of the university:

1. Categories of Internal Threat Actors (Insiders)

According to the classification by O. H. Korchenko [7], internal threat actors possess a distinct advantage in the form of authorized access to resources:

Students:

Objectives: modifying grades in academic records, gaining unauthorized access to examination papers, utilizing university servers for cryptocurrency mining or launching external attacks, and bypassing internet access restrictions in dormitories.
Skill Level: ranges from basic to high (with a particular focus on students from IT-related disciplines) [6].
Staff (Faculty and Administration):
Objectives: unintentional data disclosure (due to low digital literacy), theft of intellectual property (research and development results), and falsification of reporting data.
Skill Level: predominantly medium or low [10].
IT Administrators:
Objectives: abuse of privileges (authority), and concealing their own system configuration errors.
Skill Level: high (possessing full access to databases and servers) [1].
2. Categories of External Threat Actors
External attacks are based on the techniques described in the MITRE ATT&CK knowledge base [5]:
Cybercriminals:
Objectives: infecting the network with Ransomware to demand a ransom, and stealing databases of applicants/staff for sale on the Darknet.
Methods: phishing campaigns targeting corporate emails (@knu.edu.ua), and exploiting vulnerabilities in the university's website.
Competitors (Other Universities or Foreign Intelligence Agencies):
Objectives: espionage targeting scientific research (particularly in the fields of mining, mechanical engineering, and automation, for which KNU is renowned).
Vandals:
Objectives: damaging the university's reputation (website defacement) or deleting information for entertainment purposes [11].
3. Threat Actor Capability Levels
The university typically employs a 4-level classification to assess the technical potential of adversaries:
- Low;
- Medium;
- High;
- Very High.

5. Key Attack Vectors (Scenarios)
- Attack on the «Dean's Office» / «Educational Process» ACS;
- Phishing targeting the Accounting Department;
- Compromising the Wi-Fi Network;
- Physical Access.

6. Recommendations for Threat Mitigation
To neutralize the described threats, it is recommended to implement a Comprehensive Information Security System (CISS) (Ukr: КСЗІ), based on the

provisions of DSTU ISO/IEC 27001 [1] and the risk assessment methodologies of NIST SP 800-30 [4].

Protection Against External Threat Actors (Hackers and Vandals):

- Next-Generation Firewall (NGFW) [6].
- Web Application Firewall (WAF): specialized protection for KNU's web resources, specifically the “Electronic University” system [11], which prevents application-layer attacks such as SQL injections and other similar exploits [1].

DDoS Protection [10].

Protection Against Internal Threat Actors (Students and Staff):

- DLP (Data Loss Prevention) System [8].
- NAC (Network Access Control) System [4].
- Ientity and Access Management (IAM) [1].

Protection Against Malware and Ransomware:

- Endpoint Detection and Response (EDR) [5].
- Backup System [4].

Organizational Measures (Mitigating the “Human Factor”)

- Security Awareness Training [10].
- Physical Access Control System (PACS) [3].

Conclusion

The study underscores the critical necessity for a systematic and continuous evolution of cryptographic protection for IT devices. Achieving this requires not only the implementation of cutting-edge technologies but also persistent threat monitoring, enhancing the security awareness of both users and administrators, and the proactive adaptation of defense mechanisms to a rapidly shifting cyber-threat landscape.

Only such an integrated approach can establish a resilient security model capable of withstanding both network-borne attacks and physical access threats to IT infrastructure in the context of 2026 and beyond.

REFERENCES

1. Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2022, IDT) : DSTU ISO/IEC 27001:2023. [Effective from 2023-12-31]. Kyiv: SE «UkrNDNC», 2023. 38 p.
2. Information technology. Security techniques. Information security risk management (ISO/IEC 27005:2022, IDT): DSTU ISO/IEC 27005:2022. [Effective from 2022-12-31]. Kyiv: SE “UkrNDNC”, 2022. 54 p.
3. Terminology in the field of information protection. Basic concepts : ND TZI 1.1-003-99. Kyiv: Department of STSI of the Security Service of Ukraine, 1999. 42 p.
4. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012. 95 p. URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final (Accessed: 12.01.2026).
5. MITRE ATT&CK®. Knowledge Base of Adversary Tactics and Techniques. URL: https://attack.mitre.org/ (Accessed: 12.01.2026).
6. OWASP Top 10:2021. The Ten Most Critical Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/ (Accessed: 12.01.2026).

7. Korchenko, O. H. (2010). Pobudova system zakhystu informatsii [Construction of information protection systems]: tutorial. Kyiv: NAU. 235 p.
8. CERT-UA. Recommendations and threats. URL: https://cert.gov.ua/ (Accessed: 12.01.2026).
9. The Transport Layer Security (TLS) Protocol Version 1.3: RFC 8446 / E. Rescorla; Internet Engineering Task Force. 2018. URL: https://datatracker.ietf.org/doc/html/rfc8446 (Accessed: 09.01.2026).
10. Advanced Encryption Standard (AES) : FIPS PUB 197 / National Institute of Standards and Technology. 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (Accessed: 09.01.2026).
11. Schneier, B. (2002). Prykladna kryptohrafiia. Protokoly, alhorytmy ta vykhidni teksty na movi C [Applied Cryptography: Protocols, Algorithms, and Source Code in C]. Kharkiv: Fakt. 616 p.
12. Recommendation for Key Management: NIST Special Publication 800-57 Part 1 Revision 5 / Elaine Barker; NIST. 2020. URL: https://doi.org/10.6028/NIST.SP.800-57pt1r5 (Accessed: 09.01.2026).
13. SSL Certificate Report: knu.edu.ua. Sectigo Limited. 2026. URL: https://crt.sh/?q=knu.edu.ua (Accessed: 09.01.2026).
14. OWASP Top 10:2021. Cryptographic Failures. OWASP Foundation. 2021. URL: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ (Accessed: 09.01.2026).

QUALITY ASSESSMENT OF A JOINT PRODUCED BY ROBOTIC WELDING

Patryk SETLAK (Student)[1]
Karina JANISZ (PhD Eng., Assistant Professor)[2]
Marek ALEKSANDER (DSc, Professor University of Applied Sciences in Nowy Sącz)[3]

[1]*University of Applied Sciences in Nowy Sącz, Poland, Faculty of Engineering Sciences,*
e-mail:patryksetlak93@gmail.com, kjanisz@ans-ns.edu.pl, aleksandermarek4@gmail.com

Summary
This paper presents the results of a comprehensive quality assessment of a welded joint produced by robotic welding. The investigation included non-destructive testing: visual testing (VT), magnetic particle testing (MT) and ultrasonic testing (UT), as well as destructive examinations: macro- and microstructural assessment and Vickers hardness measurements. The aim of the study was to evaluate weld quality. The results confirmed good repeatability of weld quality and demonstrated that the selected set of methods is effective in identifying potential welding imperfections.

Introduction

One of the key pillars of Industry 4.0 is the automation of manufacturing processes, including welding. Today, welding remains one of the fundamental joining technologies in structural engineering and industrial production. Robotic welding addresses growing requirements for precision, repeatability, and process efficiency. Modern robotic welding systems typically use multi-axis industrial robots equipped with dedicated welding torches, and rapid progress is also being observed in collaborative robots. Deploying robots reduces human-related variability, improves occupational safety, and increases production rate. Advanced welding technologies also support cost optimisation and reduction of material waste. In practice, MIG/MAG welding is most commonly automated due to its versatility and relatively straightforward integration. TIG welding is also applied, particularly where high weld quality and aesthetics are required. Laser welding is gaining popularity as well, especially in precision manufacturing [1].

Automating welding introduces new requirements for quality control. Weld quality is assessed in line with relevant standards, including PN-EN ISO 5817, PN-EN ISO 17637, PN-EN ISO 17638, and PN-EN ISO 17640, which enables an objective verification of compliance with technical requirements and supports process repeatability. A broad set of inspection methods is available, covering non-destructive testing (NDT) such as VT, PT, MT, and UT, as well as destructive testing (DT) such as bend and tensile tests, used to detect and evaluate welding imperfections [2]. A comprehensive overview of more than 20 NDT methods used for alloy welding and WAAM technology, including a table of minimum detectable defect sizes, is provided in [4].

Methodology and test object

The analysed component was a lemniscate connector used as part of a mining roof support. The connector consists of two brackets, two cover plates, two inner and two outer pads, as well as smaller auxiliary parts [3]. Robotic welding was performed in a welding cell based on a Panasonic TL2000 robot with six serially arranged axes. The station was equipped with a Drop Center welding positioner with a maximum payload of 1000 [kg]. The component, the station, and the tests were prepared within an engineering thesis project [3]. The first step was to develop the welding procedure. This started with workstation preparation and fixturing the connector on the positioner. Next, the weld grooves were located. For butt welds, due to limited repeatability of plate bevel geometry, a correction routine was programmed to compensate for deviations in the groove volume. Multipass function libraries were created, containing arc parameters, groove data, angles, torch offsets, and other settings for each pass in all four welds. Finally, the welding sequence was defined and corresponding robot programs were prepared.

The subsequent investigations focused on a welded butt joint. The base material was plate with thicknesses of 25 [mm] and 30 [mm], material S6900QL. The filler material was a 1.2 [mm] electrode wire, grade Mn3Ni1CrMo.

The applied test methods included:

- non-destructive testing: visual testing (VT), magnetic particle testing (MT), ultrasonic testing (UT)
- destructive testing: macro examination, micro examination, and Vickers hardness measurements.

All tests were carried out in an accredited laboratory in accordance with applicable procedures and standards.

Welding process quality analysis

To assess the quality of the robotic welding process, a test specimen was designed and manufactured to reproduce the dimensions, geometry, and weld types of the lemniscate connector (Fig. 1a). Figure 1b shows the 3D model of the specimen. The welds were numbered as follows: weld 14V - No. 1, welds 15IV+5L - Nos. 2-5, and weld 14L - No. 6.

As a first step, non-destructive testing (VT, MT, UT) was used to verify the quality of the welds. All welds were examined visually (VT) and by magnetic particle testing (MT). For weld No. 1 (14V), VT revealed a small interpass groove on the weld face; this resulted from a slightly different groove geometry in the specimen compared with the actual link. MT indicated overlap at the edge of the final cap pass in weld No. 3, caused by insufficient removal of scale after thermal cutting. For weld No. 6 (14L), the inspection showed overly pronounced interpass grooves over a short section of the weld. These features can be readily reduced during parameter tuning and by adjusting program points.

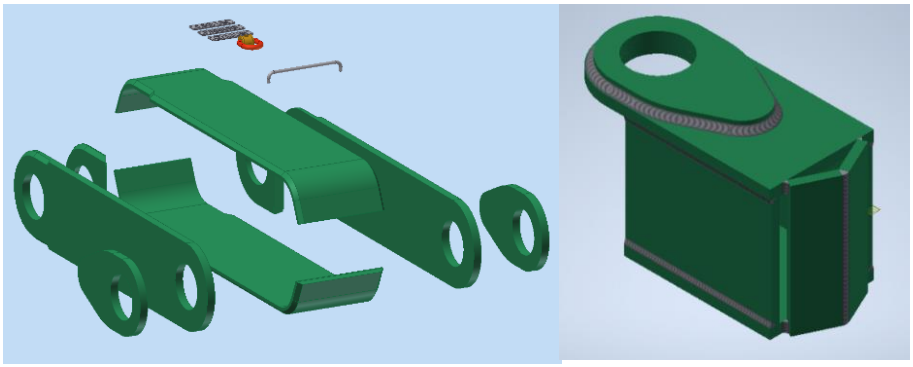


Fig. 1. a) Lemniscate connector b) Specimen model [3]

Ultrasonic testing was performed for welds No. 1-5 and did not reveal any welding defects.

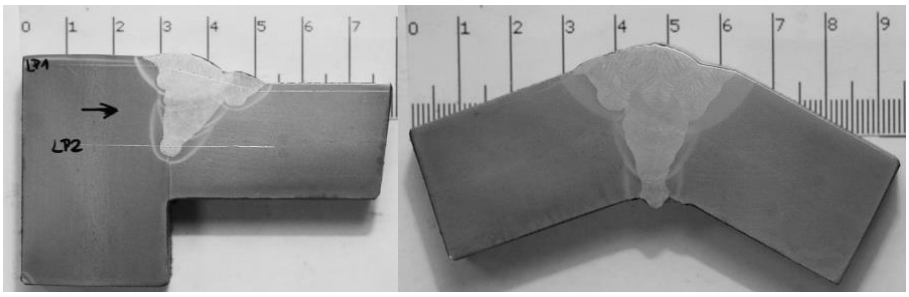


Fig. 2. Weld test results [3]

After the non-destructive examinations, the specimen was transferred to a materials laboratory and cut into smaller pieces to prepare metallographic sections (Fig. 2). Macro- and microstructural examinations confirmed compliance with quality levels B and C in accordance with PN-EN ISO 5817. Vickers hardness profiles were also measured along two traverse lines. The hardness results showed that the heat-affected zone (HAZ) did not exceed the allowable limit of 450 HV 10.

The investigations confirmed that the welds were produced correctly at a satisfactory level. The observed irregularities do not disqualify the welds and can be mitigated by refining the robot program and welding parameters.

Conclusions

The tests did not reveal defects that would exclude the welds from further production. The NDT programme (VT, MT, UT) confirms an acceptable weld quality under the applied acceptance criteria: VT corresponded to quality level C, and both MT and UT returned positive/accepted results for the inspected joints.

Metallographic evaluation identified welding imperfections; however, their severity - assessed according to PN-EN ISO 5817:2023-08—corresponded to quality level C in sample 1 and quality level B in samples 2, 3, 6/1, and 6/2, indicating conformity with the requirements for these levels.

The HV10 hardness profiles showed no exceedance of the specified criterion in the HAZ (maximum about 434 HV10 against the limit of 450 HV10), which indicates

that the thermal cycle did not produce excessive hardening in the measured HAZ regions.

The issues identified in the butt welds were related to insufficient repeatability of weld-groove geometry, to a degree that the Adaptive function could no longer compensate. This can be addressed by equipping the station with a laser vision sensor that scans the entire weld groove and based on this information, updates the parameters stored in the library; as a result, the groove can be filled more accurately. To reduce interpass grooves in the fillet weld, it is sufficient to fine-tune the welding parameters.

Robotic welding provides good joint quality and high repeatability. The applied test set enables a comprehensive assessment of weld quality. Microstructural observations and hardness measurements confirm that the selected welding parameters are appropriate. The presented example shows that welding robotisation is fully justified: robot-made welds can meet the same quality criteria as manual welds. Stable weld quality is essential for maintaining production continuity. Modern robot programming environments, advanced sensing, numerous auxiliary functions, and decreasing system costs mean that welding robots are becoming a practical and economically viable option also for small enterprises.

REFERENCES

1. CIOCHOŃ D.: Robot spawalniczy i spawanie robotem spawalniczym – krótki przewodnik teoretyczny. https://www.astor.com.pl/poradnikautomatyka/robot-spawalniczy-i-spawanie-robotem-spawalniczym-krotki-przewodnik-teoretyczny/ 2023
2. PRAJAPATI V., JAISWAL A., PATIL, Y., PANCHAL H., VOHRA M.A. Detection of Weld Metal Defects using DT and NDT - A Review. International Research Journal of Engineering and Technology Vol./Numer: 7(2), p. 411–415. 2020
3. SETLAK P.: Koncepcja procesu spawania zrobotyzowanego wybranej części. Praca dyplomowa na kierunku Mechatronika, Akademia Nauk Stosowanych w Nowym Sączu, 2026
4. SHALOO M., SCHNALL, M., KLEIN, T., HUBER, N., REITINGER, B.: A Review of Non-Destructive Testing (NDT) Techniques for Defect Detection: Application to Fusion Welding and Future Wire Arc Additive Manufacturing Processes. Materials, Vol. 15(10):3697. 2022.

INTEGRATED SECURITY FRAMEWORK FOR THE SMART HOME IOT ECOSYSTEM

Andrii PETRENKO (PhD, Docent of the Department of Cyber Security)[1,]
Yuriy PEPA (PhD, Associate Professor, Professor)[2]

[1]State University "Kyiv Aviation Institute", Faculty of Computer Science and Technology, Department of Cyber Security: 1pab.05@ukr.net
[2]State University of Information and Communication Technologies, Technical Cyber Defense Systems: yurka14@gmail.com

Summary

The modern smart home has evolved from a set of autonomous devices into a complex hierarchical network of cyber-physical systems; however, according to the OWASP IoT Top 10, fundamental vulnerabilities—such as hard-coded passwords, lack of encryption, and insecure software components—remain present in approximately 70% of commercial devices [1,2]. A key challenge is the widespread reliance on external cloud providers, which introduces critical security risks, including the loss of user privacy due to the transmission of activity metadata to third-party servers and the high scalability of attacks, where a single vulnerability in a manufacturer's cloud infrastructure can enable large-scale compromise of IoT devices. This study aims to address these issues by developing an architecture that relocates decision-making and security mechanisms directly to the user's edge environment.

Main part of the work

This work analyzes the primary threats to IoT systems as described in the OWASP IoT Top 10 methodology and supplemented with contemporary case studies [1–4]:

- Insider threats and social engineering: According to the Unit 42 report, the number of attacks exploiting compromised credentials has increased [6]. In a smart home environment, this often manifests as shared credentials.
- AI-assisted attacks: The use of artificial intelligence for automated discovery of open ports and firmware vulnerabilities.
- Weak authentication mechanisms: The use of static tokens without session binding.

Proposed Framework and Solution Architecture

A three-layer security model is proposed:

1. Hardware Layer

The solution is based on the Raspberry Pi 5, selected for its performance, which enables cryptographic operations without service degradation [7].

- Crypto Acceleration: Utilization of ARMv8 instructions for hardware-accelerated AES and SHA, which is critical for VPN operation and real-time disk encryption.
- Storage Integrity: Replacing SD cards with NVMe SSDs (via the PCIe 2.0 interface). This mitigates issues such as "log poisoning" and sudden system failures, which are commonly exploited in local Denial of Service (DoS) attacks.

- Physical Hardening: Disabling debugging interfaces (UART, JTAG) at the bootloader level (config.txt) to prevent root console access in case of physical access to the board.

2. Network Architecture and Microsegmentation (Network Layer)

The core principle is isolation. The router and Raspberry Pi 5 operate in tandem to create three logical segments (VLANs):

- VLAN 10 (Trusted): Personal devices (PCs, smartphones).
- VLAN 20 (IoT Untrusted): Devices requiring Wi-Fi (e.g., legacy cameras or washing machines). These devices have access only to the Raspberry Pi 5 and no access to the Internet or VLAN 10.
- VLAN 30 (Management): Dedicated exclusively to gateway administration.

Protocol Diversification

For security sensors (locks, motion sensors), the IP stack is completely excluded by using Zigbee 3.0 or Thread [8].

- Mechanism: A coordinator (USB dongle on the Raspberry Pi 5) forms an independent mesh network.
- Effect: Even if an attacker gains access to the Wi-Fi network, Zigbee devices remain invisible, as they operate on a different OSI layer.

3. Software and Logic Layer (Application Layer)

A containerized architecture (based on Home Assistant OS or Docker) is employed to isolate processes from one another.

- Zero Trust Remote Access: Instead of traditional password-based external access, a WireGuard VPN is implemented.
    - Logic: The user first establishes an encrypted tunnel to the Raspberry Pi 5. Only after successful VPN-level authentication (using cryptographic keys rather than passwords) does the smart home web interface become accessible.
- Behavioral Analysis (IDS): Given that the Raspberry Pi 5 is equipped with 4–8 GB of RAM, a lightweight intrusion detection system (e.g., CrowdSec) is deployed. It analyzes login attempt logs and IoT device network requests. If, for example, a smart plug suddenly attempts to connect to a server in Eastern Europe, the system automatically blocks it at the firewall level.

Mathematical Security Model of the Architecture

Let the overall probability of system compromise PsysP_{sys}Psys be defined as the product of the compromise probabilities of each independent layer:

$$P_{sys} = P_{vpn} \times P_{auth} \times P_{seg},$$

where:

P_{vpn} — the probability of compromising a 256-bit WireGuard key (practically zero);
P_{auth} — the probability of bypassing MFA (Multi-Factor Authentication);
P_{seg} — the probability of escaping an isolated VLAN (sandbox escape).

Since all variables are extremely small, the overall system resilience increases exponentially compared to standard cloud-based solutions, where PsysP_{sys}Psys often depends solely on a single user password.

Experimental Section and Results

To validate the proposed model, penetration testing was conducted in accordance with the OWASP FSTM methodology (Table 1).

Table 1— Testing Results

Attack Vector	Standard System (Cloud-based)	Proposed Architecture (Edge + RPi 5)	Result
Brute-force (SSH/Web)	Successful (with weak passwords)	Blocked (Fail2Ban + key-based authentication)ф	Protected
Sniffing (data interception)	Cloud data accessible via API	Local and encrypted traffic	Protected
Physical Tampering	Console access via UART	Disabled at bootloader level	Protected
DDoS on device	Device disruption	Isolation via firewall	Partial protection

The experiment demonstrated that latency in local control via Raspberry Pi 5 was reduced by 40% compared to cloud-based solutions, which further improves the overall system resilience.

Conclusions

The deployment of Raspberry Pi 5 as a central security component enables the transformation of a vulnerable “smart home” into a secure fortress. The proposed architecture minimizes dependence on third-party cloud services, ensures reliable encryption, and enforces the principle of least privilege for each device.

Future research directions: integration of machine learning algorithms (TinyML) directly on the Raspberry Pi for real-time detection of anomalous device behavior without transmitting data to the cloud.

REFERENCES

1. OWASP Foundation. (2024). IoT Security Verification Standard (ISVS).
2. OWASP IoT Project. IoT Top 10 Vulnerabilities, 2025-2026 update.
3. NIST IR 8259. (2020). Foundational Cybersecurity Activities for IoT Device Manufacturers.
4. NIST Special Publication 800-213. IoT Device Cybersecurity Guidance for the Federal Government.
5. Petrenko Andrii. SECURITY OF IOT SYSTEMS USING BLOCKCHAIN / Petrenko Andrii, Pepa Yurii, Teliushchenko Valentyna // IV International Scientific and Practical Conference

"Latest Technological Trends in the Intellectual Industry and the Internet of Things" (TTSIIT-2025), January 30-31, 2025: abstracts, Kyiv: KNUCA. - 2025. – P. 65-70.
6. Palo Alto Networks Unit 42. 2025 Global Incident Response Report: Speed and Insider Threats.
7. Upton, E. (2023). Raspberry Pi 5: Hardware and Architecture Guide.
8. Badea, R. et al. (2025). Zero Trust Architectures in Smart Home Environments. Journal of Cyber Security and Mobility.

AN INTELLIGENT NEURO-ADAPTIVE FRAMEWORK FOR FUNCTIONAL STABILITY OF INFORMATION SYSTEMS

Yuliya OLIMPIYEVA (Postgraduate, Senior Lecturer)[1]
Yuriy PEPA (PhD, Associate Professor, Professor)[2]

[1] State University of Information and Communication Technologies, Higher Mathematics, mathematical modeling and Physics, evanaolimp@ukr.net
[2] State University of Information and Communication Technologies, Technical Cyber Defense Systems, yurka14@gmail.com

Summary

This paper presents an intelligent neuro-adaptive framework for ensuring the functional stability of information systems under uncertainty and destabilizing influences. The proposed approach integrates continuous monitoring, self-diagnosis, probabilistic state estimation, and neuro-adaptive evaluation within a closed-loop control structure. The framework enables early detection of degradation trends, adaptive decision-making, and generation of compensatory control actions, providing preventive maintenance of system operability and adaptability to dynamic operating conditions.

Main part of the work

Ensuring the functional stability of an enterprise information system under the influence of destabilizing factors is effectively achieved through a neuro-adaptive algorithm that integrates the results of monitoring, self-control, and self-diagnosis with intelligent evaluation of the functional state and the generation of control actions [1]. Such an algorithm is designed for the preventive detection of degradation processes and the timely application of compensatory measures in order to preserve or restore the operability of the information system. Unlike existing approaches, the proposed framework jointly considers deterministic diagnostics, probabilistic state dynamics, and adaptive control actions. The proposed framework is applicable to enterprise information systems operating under conditions of uncertainty, high load variability, and structural changes.

The neuro-adaptive functional stability assurance algorithm is based on iterative processing of diagnostic information and implements a closed-loop structure of evaluation–control–adaptation, in which a neuro-adaptive model for functional state assessment, developed in works [1], plays a central role.

Step 1. Collection and updating of diagnostic information

At the first stage, continuous or periodic acquisition of primary diagnostic data is performed to characterize the operation of software and hardware modules as well as the information links of the enterprise information system. This data set includes:

- results of elementary self-control checks;
- telemetry parameters and workload indicators;
- signals indicating deviations from nominal operating modes.

The collected data are organized into time series, which are subsequently used for the construction of aggregated diagnostic features.

Step 2. Formation of the diagnostic feature space

Based on the primary data, aggregated statistical characteristics are computed within sliding time windows, and the diagnostic feature space of the information system is formed as a multidimensional vector that describes the state of the enterprise information system [2-4]:

$$Z = \{z(t)\}, z(t) = \begin{bmatrix} x(t) \\ p(t) \\ \Delta p(t) \end{bmatrix} \in \Re^{d+2(K+1)},$$

where *x(t)* – the vector of deterministic diagnostic features summarizing information about the current and previous states of the system within the observation window, *p(t)* – the vector of estimated probabilities of the enterprise information system being in the corresponding states, $\Delta p(t) = p(t) - p(t - \Delta t)$ – dynamic characteristics of the probability distribution.

This representation enables a compact yet informative description of the system state evolution over time. This vector integrates:

- deterministic aggregated parameters;
- estimates of the probabilities of the information system operating in specific technical states;
- characteristics describing the temporal dynamics of changes in these probabilities.

The resulting vector is consistent with the probabilistic interpretation of system states and is used as input to the neuro-adaptive model.

Step 3. Neuro-adaptive functional state evaluation

The diagnostic feature vector *z(t)* is supplied to the input of the neuro-adaptive evaluation model, which implements a nonlinear mapping $F_S(t) = N_\theta(z(t))$, $F_S(t)$ – estimation of the current value of the integral functional stability indicator of the enterprise information system. The resulting estimate reflects not only the current functional state of the information system but also its degree of proximity to boundary or critical operating conditions [3, 4].

Step 4. Evaluation analysis and decision making

Based on the value of $F_S(t)$, the functional state of the information system is analyzed with respect to predefined threshold or interval-based criteria. The analysis may result in one of the following conditions:

- the system operates within an acceptable functional region and does not require intervention;
- degradation trends are detected, indicating the need for preventive actions;
- the system is in a boundary or critical state and requires immediate compensatory measures.

Step 5. Generation of control actions

When a decrease in functional stability is detected, a control action is generated to compensate for destabilizing factors. Such actions may include:

- redistribution of functional tasks among operational modules;
- adjustment of operating modes of individual components;
- initiation of recovery procedures or isolation of faulty elements.

The control actions are determined with respect to the current functional state of the system and the available system resources.

Step 6. Implementation of control actions and result monitoring

The generated control actions are executed within the information system, followed by repeated acquisition of diagnostic information and evaluation of the updated functional state. This process enables assessment of the effectiveness of the applied measures and their impact on the restoration or maintenance of functional stability.

Step 7. Neuro-adaptive model adaptation

In the presence of systematic discrepancies between the expected and the observed dynamics of the functional stability indicator, neuro-adaptation of the evaluation model parameters is performed. The adaptation process aims to preserve the adequacy of the mapping between the diagnostic feature space and the functional state estimate under changes in the structure of the information system, its operating modes, or the nature of destabilizing factors.

Step 8. Iterative execution of the algorithm

The algorithm operates in an iterative mode, forming a closed-loop neuro-adaptive functional stability assurance process. This organization enables:

- timely identification of hazardous trends;
- preventive mitigation of critical faults and failures;
- sustained operability of the information system under conditions of uncertainty and non-stationarity.

The proposed framework provides improved resilience, adaptability, and early fault prevention compared to conventional rule-based or static diagnostic approaches. The effectiveness of the proposed framework is intended to be validated through simulation and experimental studies on enterprise information system models.

REFERENCES

1. Олімпієва Ю.І.: Забезпечення функціональної стійкості виробничих процесів промислових підприємств на основі нейроадаптивної системи. Системи управління, навігації та зв'язку. 2024. № 3 (77), 44-52.
2. Собчук В.В., Замрій І.В., Олімпієва Ю.І., Лаптєв С.О.: Функціональна стійкість технологічних процесів на основі нелінійної динаміки із застосуванням нейромереж. Сучасні інформаційні системи. 2021. Том 5, № 2, 49-57.
3. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б.: Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології, 2022, №1 (74), 4-14.
4. Zamrii I., Vyshnivskyi V., Sobchuk V.: The method of ensuring the functional stability of the information system based on detection of intrusions and reconfiguration of virtual networks. CEUR Workshop Proceedings. Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2024), Kyiv 2024, 252–264.
5. Khlaponin Y. Improved cryptocurrency market by using Monte Carlo method /Yurii Khlaponin, Mushtaq Talib Al-Sharify, Vadym Kostenko // The 2nd International Conference on Engineering and Advanced Technology 28-29 March 2022, Turkey. AIP Conference Proceedings, 2023, 2787(1).

ALGORITHM FOR SYNTHESIZING BACKGROUND NETWORK TRAFFIC

Vladyslav HERASYMCHUK (Postgraduate student)[1]
Yuriy PEPA (PhD, Associate Professor, Professor)[2]

[1]*State University of Information and Communication Technologies, Department of Telecommunication Systems and Networks: l3urius@gmail.com*
[2]*State University of Information and Communication Technologies, Technical Cyber Defense Systems: yurka14@gmail.com*

Summary

This paper presents a statistical and probabilistic approach to background network traffic synthesis for realistic modeling and testing of information and telecommunication systems. The proposed method integrates multi-stage traffic generation, topology-aware flow formation, probabilistic packet scheduling, and content-level payload synthesis based on Web interaction models [1, p. 7]. Traffic realism is validated using self-similarity analysis through the Hurst exponent, ensuring consistency between synthesized and real network traffic characteristics under controlled experimental conditions.

Main part of the work

The algorithm for synthesizing background network traffic is based on transforming a matrix of statistical traffic characteristics and consists of five stages (Fig. 1).

Stage 1. Selection of the matrix of statistical characteristics of network traffic.

Stage 2. Formation of the topology of the synthesized computer network.

Stage 3. Formation of integral time parameters of network flows.

Stage 4. Synthesis of network packets taking into account the statistical characteristics of network flows and filling the data field of network packets based on the Web server operation model.

Stage 5. Evaluation of the adequacy of the network traffic dump using the Hurst exponent.

At the stage of packet flow synthesis, the existing matrix of network traffic characteristics F (1) is transformed using the corresponding functions, taking into account the duration of testing [2, p. 3]. The generation of a packet sequence for a flow f consists in randomly selecting values in accordance with row f of the matrix with characteristics described by the vector f_c. The value of the index $x \in \{1, \ldots, q_c\}$, where q_c is the maximum value of a given traffic characteristic, is selected randomly according to the specified distribution f_c.

For the purpose of synthesizing the data payload of network packets [3, p. 5], Web traffic is considered as an information exchange between a Web server and a user, carried out by sending requests and processing responses in the form of transmitted Web pages that contain static and dynamic components.The algorithm for synthesizing the data payload of network packets assumes automated formation of requests to the Web server and transmitted data, determined by the required characteristics of information exchange, which allows the structure of the Web server to be dynamically changed during testing.

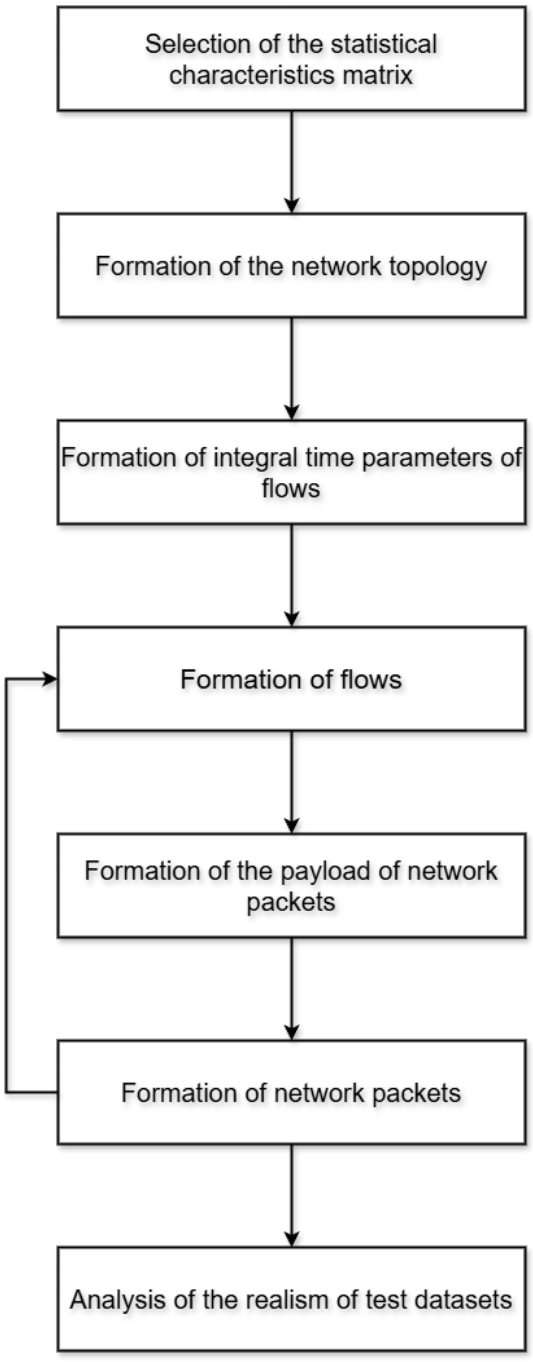


Fig. 1. Diagram of the background network traffic synthesis algorithm

The algorithm for synthesizing the data payload of network packets is implemented using a discrete-time Markov chain. To generate text, a transition matrix is used, where the set of all words, punctuation marks, and HTML tags forms the state space. The formation of the transition matrix is based on a set of HTML pages, according to which the probability of creating (composing) a new phrase is estimated (including hypertext markup constructs) from a sequence of existing phrases. The page formation model on the Web server assigns ranks to the obtained pages, determining the assumed route of a visitor moving through the website and the Web server visit

model. The considered model of interaction with the Web server makes it possible to generate requests to pages depending on the initial conditions, the transition matrix, and the server content.

At the stage of generating packet flows, the following algorithm for packet flow synthesis is applied:

1. Random selection of a pair of nodes: source *s* and destination *d*.
2. Selection of the flow volume *b*:

$$\Phi_{\text{size}}(b) = \max\left\{1, (b_{max} - 1)\left(\frac{x}{q_b}\right)^{\frac{1}{\alpha}}\right\}.$$

3. Selection of packet lengths *l* used in the flow according to the histogram and the selected flow volume *b*.
4. Selection of time intervals between packets Δt taking into account the mean delay value $\bar{z}$:

$$\Phi_t(\Delta t) = \Delta t_{min} + (\Delta t_{max} - \Delta t_{min})\left(\frac{\Delta t}{q_z}\right)^{\frac{1}{\beta}}.$$

5. Computation of the mean packet length $\bar{l}$ and the mean time interval between packets $\overline{\Delta t}$, as well as the mean flow duration $\overline{t_f}$:

$$\overline{t_f} = \frac{b\,\overline{\Delta t}}{\bar{l}}.$$

6. Selection of the start time of the flow τ (the sum $\tau + \overline{t_f}$ is less than or equal to the generation duration):

$$\Phi_{\text{start}}(x) = \tau_{max}\frac{x}{q_\tau}.$$

7. At the selected start time τ, the first packet is transmitted.
8. Selection and transmission of the next network packet.
9. The process continues until the end of the generation time or until the completion time of all flows. The last packet, regardless of the distribution, carries the remaining number of bytes.

At the final stage, the adequacy of the network traffic dump is evaluated using the Hurst exponent, which consists in comparing the values of the Hurst [4, p. 3] exponent for the original and the generated traffic. If the exponent value lies in the interval from 0.5 to 1, the synthesized traffic is considered to correspond to the traffic of real information and telecommunication systems.

Conclusion

The proposed algorithm for synthesizing background network traffic provides a comprehensive and statistically grounded approach to generating realistic traffic patterns for modeling and testing information and telecommunication systems. By combining multi-stage flow formation, probabilistic packet generation, Markov-based

payload synthesis, and validation through the Hurst exponent, the method ensures consistency between synthesized and real traffic. This enables the effective use of the algorithm in simulation studies, performance evaluation, and experimental analysis of network infrastructures under conditions close to real.

REFERENCES

1. Javali C., et al. Network Web Traffic Generator for Cyber Range Exercises. *IEEE LCN*, 2019.
2. Song Y., Keromytis A.D. Behavior-Based Network Traffic Synthesis. Technical paper, 2011.
3. Avallone S., Guadagno S., Emma D., Pescapè A., Ventre G. D-ITG: Distributed Internet Traffic Generator. *Proceedings of ACM Conference* (ACM Digital Library), 2004.
4. Botta A., Dainotti A., Pescapè A. A tool for the generation of realistic network workload. *Computer Networks*, 2012.

ANALYSIS OF CRITERIA FOR MODERN METHODS OF IDENTIFYING ANONYMOUS USERS AT THE OSI MODEL LAYERS

Ivan AZAROV (Master, Assistant)[1]
Anna KORCHENKO (Dr hab., professor)[2]
Illia AZAROV (Student)[3]

[1] *State University of Information and Communication Technologies, Education and Research Institute of Cybersecurity and Information Protection, Department of Cybersecurity and Information Protection Management, Assistant: ORCID: 0000-0002-2732-8861, azarovphone@gmail.com*
[2]*Uniwersytet Komisji Edukacji Narodowej w Krakowie, Instytut Bezpieczeństwa i Informatyki, Katedra Inżynierii Komputerowej i Cyberbezpieczeństwa, Assistant: ORCID: 0000-0003-0016-1966, anna.korchenko@uken.krakow.pl*
[3]*Kyiv Aviation University, faculty of computer science and technologies, department of cybersecurity, specialization cybersecurity : ORCID: 0000-0002-6163-3499, azarovforce@gmail.com*

Summary

This research focuses on the analysis of criteria for modern anonymous user identification methods within the OSI model framework. It examines popular active and passive fingerprinting techniques, outlining their characteristics as well as their key advantages and disadvantages. Additionally, the study identifies critical parameters for user identification at various OSI layers to enhance the protection of information resources in cyberspace.

Keywords

Identification of anonymous users, user de-anonymization within the OSI model, browser fingerprinting

Introduction

The number of digital assets is increasing daily, leading to the emergence of new cyber threats. There is a pressing need to improve methods for detecting anonymous

users, as malicious actors often utilize tools to obfuscate their activities within the digital space across various layers of the OSI model to execute cyberattacks.
Identifying anonymous users enables the prevention of cyber incidents and the mitigation of their consequences, thereby ensuring the protection of server infrastructure through the monitoring and restriction of unauthorized entities' actions.
Thus, the objective is to determine the criticality of anonymous user identification methods by analyzing and classifying them according to the layers of the OSI network model.
The following section reviews modern technologies for extracting unique device and browser characteristics (fingerprints) that remain consistent even in private browsing (incognito) modes.

1. Theoretical foundations for the development of anonymous user identification methods.

Given the continuous evolution of cyberattacks, the use of traditional static user identification methods is insufficient. The generation of a digital fingerprint is based on the principle of variable combinations of unique browser attributes, operating system (OS) settings, and user device characteristics [1, 2]. The user's digital fingerprint itself merely indicates their uniqueness within cyberspace and does not allow for determining the user's level of anonymity.
A comprehensive analysis of modern criteria for collecting user device digital fingerprints allows for a detailed examination, the identification of advantages and disadvantages, as well as the determination of optimal parameters for identifying anonymous users in cyberspace.

2. Active browser fingerprinting methods:

The primary feature of obtaining a user fingerprint via active methods lies in the execution of targeted computations on the user's browser side to derive informative data regarding the individually variable functional characteristics of the software and hardware environment. Active methods can be classified into the following identification categories according to the OSI model:

- The Application Layer (Layer 7), characterized by: ECMAScript objects, Canvas, WebGL, WebGPU, and Emoji fingerprints, font identifiers, Web Audio API, CSS properties, Cookies, LocalStorage, SessionStorage, IndexedDB, Fetch API, WebSockets, Service Workers, browser extensions, and user behavior;
- The Network Layer (Layer 3), which includes: WebRTC with the capability to detect real IPv4 and IPv6 addresses [3,4].

Passive device fingerprinting methods:
The utilization of these device fingerprinting methods enables the passive analysis of information regarding basic configurations, user hardware and software usage patterns, and connection behavior with the server infrastructure, without requiring active client-side computations.

Passive methods can also be classified according to the layers of the OSI model:

- The Application Layer (Layer 7), including: HTTP/2 frame patterns;
- The Presentation Layer (Layer 6), characterized by: TLS/SSL handshake analysis;
- The Transport Layer (Layer 4), based on: TCP header parameters;
- The Network Layer (Layer 3), containing: IP header parameters.

These categories reveal the specific type or version of the user's software and hardware stack. This approach remains effective even when active methods are disabled on the client side, permitting high-accuracy detection of anonymization tools [5,6].

Conclusions

Based on a comprehensive analysis of existing active and passive browser and user device fingerprinting methods for identifying anonymous users, it has been determined that the lower the layer in the OSI model, the higher the criticality of the attributes.

This is due to the fact that the number of such parameters is limited; they are generated directly by the operating system kernel, remain stable and unchanged over long periods, and are significantly more difficult to spoof.

The use of this data allows for the identification not only of mutable browser characteristics but also of fundamental features of the operating system, hardware, and actual network infrastructure.

The most critical attributes are:

At the Network layer: passive detection of IP header parameters and active detection of the user's real IP address via WebRTC. At the Transport layer: passive detection of TCP header parameters. At the Presentation layer: passive detection of TLS/SSL handshake characteristics.

At the Physical and Data Link layers, detection is currently unfeasible, as it requires access to the physical specifications of the device or access to the user's local network.

At the Application layer, the criticality of elements for user identification is the lowest, as it involves many detection techniques that can be easily spoofed.

The application of this research contributes to the prevention of potential threats in cyberspace.

REFERENCES

1. Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. ACM Computing Surveys, 55(14s), 1-41.
2. Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. ACM Transactions on the Web (TWEB), 14(2), 1-33.
3. Laperdrix, P., Rudametkin, W., & Baudry, B. (2016, May). Beauty and the beast: Diverting modern web browsers to build unique browser fingerprints. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 878-894). IEEE.
4. Iqbal, U., Englehardt, S., & Shafiq, Z. (2021, May). Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1143-1161). IEEE.

5. Zhang, D., Zhang, J., Bu, Y., Chen, B., Sun, C., & Wang, T. (2022). A survey of browser fingerprint research and application. Wireless Communications and Mobile Computing, 2022(1), 3363335.
6. Li, S., & Cao, Y. (2020, October). Who touched my browser fingerprint? a large-scale measurement study and classification of fingerprint dynamics. In Proceedings of the ACM Internet Measurement Conference (pp. 370-385).

COMPARATIVE ANALYSIS OF THE EFFICIENCY OF EDGE-CLOUD ARCHITECTURES FOR REAL-TIME NATURAL LANGUAGE PROCESSING TASKS

Ruslan OREL (PhD Student)[1]
Inna ROZLOMII (Ph.D., Associate Professor)[2]

[2]Cherkasy State Technological University, Faculty of Information Technologies and Systems, Department of Information Security and Computer Engineering, Computer Engineering, r.l.orel.asp25@chdtu.edu.ua.
[3]Kyiv Cherkasy State Technological University, Faculty of Information Technologies and Systems, Department of Information Security and Computer Engineering, Computer Engineering

Summary
The paper presents a fundamental study of architectural paradigms for deploying NLP systems, comparing Cloud, Edge, and hybrid models under real-time constraints. It analyzes hardware accelerators (NVIDIA H100 vs. Snapdragon NPU), the impact of quantization, and Split Computing protocols. Results indicate a transition to convergent Edge-Cloud ecosystems where dynamic load balancing is key for next-generation NLP services.

Introduction

The evolution of Natural Language Processing (NLP) algorithms has shifted from statistical methods to Transformer architectures. Marked by the emergence of the GPT and Llama model series, this transition ensured high-quality text generation but created a significant load on infrastructure [1, p. 5998]. While the centralized Cloud AI model offers scalability, latency often exceeds the human perception threshold (100 ms) for real-time interactive applications. The development of System-on-Chip (SoC) mobile systems paved the way for Edge AI—on-device inference—which solves the latency issue but encounters power consumption limitations. This paper deconstructs both approaches and analyzes hybrid architectures (Split Computing).

The effectiveness of architectural and hardware solutions depends on the inference hardware foundation. Cloud data centers utilize graphics accelerators such as the NVIDIA H100. The Hopper architecture provides memory bandwidth of up to 3.35 TB/s and supports the Transformer Engine. This allows for generating token streams measured in thousands per second. However, high throughput is achieved through request batching, which increases latency for the individual user. Node power consumption can exceed 10 kW [2]. Edge devices are optimized for "performance per

watt." Modern chipsets (Snapdragon 8 Gen 3, Apple A17) integrate NPUs capable of running models with up to 10 billion parameters at speeds of 15–20 tokens/sec. However, under intense load, clock speeds decrease due to thermal throttling mechanisms, causing performance degradation. The generation process consists of two phases: Prefill (Compute-Bound, effective in the cloud) and Decode (Memory Bound, latency-sensitive). This dichotomy forms the basis for hybrid architectures. Real-time performance and latency efficiency are determined by the ability to deliver results within the cognitive expectation window. Transmission times (Uplink/Downlink) dominate in cloud architectures. Under unstable connection conditions, RTT can increase to hundreds of milliseconds. Edge AI eliminates network delays, leaving only processing time, which makes the response predictable. Experiments demonstrate that 5G provides more stable latency during mobility compared to Wi-Fi 6, which is prone to interference [3, p. 14]. Radio channel data transmission is energy intensive. Local processing on an NPU consumes about 100 μW per inference, which is significantly more efficient than transmitting large volumes of context. [3, p. 14]. Radio channel data transmission is energy intensive. Local processing on an NPU consumes about 100 μW per inference, which is significantly more efficient than transmitting large volumes of context. Aggressive minimization is applied to optimize performance for Edge AI competitiveness. Quantization allows reducing weight precision to 4 bits (INT4) and fitting a 7B model into 4 GB of memory with less than 1–2% accuracy loss [4, p. 128]. The use of sparse matrices (Wanda++) and knowledge distillation enables the creation of efficient Small Language Models (SLMs), such as Gemini Nano. A promising direction is the integration of Edge and Cloud in the form of hybrid architecture. For example, the Splitwise framework utilizes a phase-splitting concept: heavy context is processed in the cloud (Prefill), while the KV-cache is transferred to the device for local generation (Decode). This allows for a 53–61% reduction in P95 latency [5]. Lyapunov optimization allows for stabilizing request queues by adapting to stochastic changes in network quality. Hybrid models create new threat vectors, notably Model Inversion attacks, which allow text recovery from activations. Differential Privacy and obfuscation are used for protection. A benchmark solution is Apple Private Cloud Compute, which uses a Stateless architecture and hardware code integrity verification, making targeted tracking impossible [6]. Regarding existing implementations, Google made a multi-tiered strategy with Gemini Nano (locally) and Cloud Handoff for complex tasks. Samsung Galaxy AI employs a hybrid approach: Live Translate works On-Device for privacy, while generative editing is performed in the cloud. The analysis indicates a transition to convergent systems. The most effective architecture combines local processing of sensitive data with cloud support via Split Computing mechanisms. Success will depend on NPU specialization and the implementation of security protocols, such as Stateless computing.

REFERENCES

1. Vaswani A. et al. Attention Is All You Need. Advances in Neural Information Processing Systems. 2017. Vol. 30. P. 5998–6008.

2. NVIDIA H100 Tensor Core GPU Architecture: Whitepaper. NVIDIA Corporation, 2022. URL: https://resources.nvidia.com/en-us-tensor-core (accessed: 15.01.2026).
3. Zhang Q. et al. A Survey on Edge Intelligence for Large Language Models. IEEE Internet of Things Journal. 2024. Vol. 11, no. 4. P. 123–145.
4. Dettmers T. et al. QLoRA: Efficient Finetuning of Quantized LLMs. NeurIPS. 2023. P. 120–135.
5. Patel J. et al. Splitwise: Efficient Generative LLM Inference using Phase Splitting. International Symposium on Computer Architecture (ISCA). 2024. P. 1–14.
6. Apple Private Cloud Compute: Security Analysis. Apple Security Research. 2024. URL: https://security.apple.com/blog/private-cloud-compute (accessed: 18.01.2026).

AI-RESILIENT SCIENCE: IN-CONTEXT DEDUCTIVE RECONSTRUCTION AS A NEW EPISTEMIC MODEL

Ihor BUCHENKO (Senior Lecturer)[1]
Andriy LEMESHKO (PhD, Associate professor)[2]

[1]*State University of Information and Communication Technologies, Faculty of Information Technology, Department of Computer Engineering, email i.buchenko@duikt.edu.ua*
[2]*State University of Trade and Economics, Faculty of Information Technology, Department of Software Engineering and Cybersecurity, email a.lemeshko@knute.edu.ua*

Summary

The AI-Resilient Science methodology is substantiated, utilizing AI as a computational engine for deductive reconstruction of theoretical systems. The approach relies on axiomatic context filters and executable documents to ensure theoretical reproducibility. Rooted in Augustinian epistemology, the method transforms AI hallucinations into diagnostic signals for verifying axiom rigidity. Adversarial deduction is employed to verify logical coherence, strictly distinguishing it from empirical correspondence. This framework positions AI as a logic-driven opponent while maintaining human-centric interpretative control.

Introduction

Epistemological and methodological foundations of AI-resilient science

The current state of Large Language Model (LLM) development necessitates a fundamental reappraisal of their role within the architecture of scientific inquiry [3]. Within the scientific community, two methodologically limited approaches predominate: viewing LLMs either as universal "oracles" or as mere statistical imitators of knowledge, unsuitable for basic research [6]. In contrast, this paper proposes considering LLMs as robust computational engines of deduction, capable of unfolding complex logical structures provided that axiomatic boundaries are clearly defined [3, 5].

The central object of analysis is AI-Resilient Science – a concept of scientific activity characterized by resilience to artificial intelligence and the potential for reconstruction through its use [5]. A theory is categorized as "AI-Resilient" if an independent language model, granted access only to its axiomatic specification, can deductively reconstruct the system of conclusions without referencing the original

text [5]. This introduces a new criterion for scientific reproducibility, where the object of restoration is the structure of thought rather than the textual form [1]. The methodological foundation for such an approach is identified as Augustinian epistemology [1]. According to the principles of Augustine of Hippo, the mind does not create truth ex nihilo (from nothing) but merely actualizes, arranges, and organizes elements provided to it from external sources [1]. Within this model, AI acts as an ontologically "blind" logician: lacking direct access to empirical reality, it ensures the internal coherence (consistency) of a theory within a given world model [6].

The Deductive Reconstruction Method serves as the core tool of this epistemic model [5]. It involves restoring the system of logical consequences based on specified inference rules, where AI is employed as an adversarial agent to verify the completeness of theoretical constructs [6]. This approach allows for the transformation of AI "hallucinations" from a technical defect into a diagnostic signal, indicating logical gaps or insufficient rigor in the initial axiomatics [6].

Consequently, the proposed epistemic model shifts the emphasis from text generation to the design of intellectual structures [1]. The practical implementation of this method requires a transition to creating dynamic systems subject to machine interpretation [3]. This necessitates an examination of the technical toolkit – specifically the use of "filters" and executable documents, which will be detailed in the following section [5].

Section 2.

Technical implementation: in-context ontology and executable documents

The technical implementation of the AI-Resilient Science method is based on an extended form of In-Context Learning, which allows the model to utilize provided information without updating its internal weights [3]. The preparation of an In-Context Ontology is identified as a key instrument, implemented through a system of "filters" that act as operational specifications of thinking [5]. The deductive reconstruction process is executed according to a strictly defined step-by-step protocol that encompasses axiomatization through the formation of executable documents with ontology, formalism, and interpretation of the subject domain, context loading by transferring formulated axioms directly into the AI working session, deductive generation to unfold logical consequences using independent models, as well as iterative refinement to correct the original axiomatics based on identified discrepancies with a subsequent repetition of the cycle [5].

The efficiency of the method critically depends on the technical parameter of the Context Window, which determines the limit of tokens the model can consider simultaneously, thereby restricting the complexity of the ontology that can be deployed as an "executable theory" [3]. To ensure transparency and output quality, the Chain-of-Thought (CoT) Prompting technique is employed, encouraging the model to generate intermediate reasoning chains and allowing the researcher to verify each link in the deductive process [4]. Loading executable documents into the context activates the Attention Mechanism, providing conditions for emergent deduction—

the model's ability to derive consequences implicitly contained within the axiomatics but not present in its training data [3].

Section 3.

Cross-validation and hallucinations as a diagnostic tool

A vital component of the method is the cross-validation of theoretical conclusions between independent language models, defined as AI-based Peer Review [6]. Within this approach, the statistical diversity of models is taken into account, as each Large Language Model (LLM) is a probabilistic approximator with its own statistical priorities and architectural features, making their discrepancies methodologically significant [6]. According to the concept of Adversarial Deduction, several AI agents are employed to generate and mutually verify logical chains, where model consensus serves as an indicator of conclusion coherence, and discrepancies act as markers of weak points in the axiomatics [6].

Particular emphasis is placed on the phenomenon of AI hallucinations, which are transformed from a defect into a diagnostic tool acting as an indicator of axiom rigidity [6]. A hallucination is viewed as a signal of insufficient theory definition or the presence of hidden assumptions, as differences in the "visions" of various models point to logical gaps in the axiomatic base [6]. Furthermore, the methodology strictly distinguishes between the concepts of coherence and correspondence: AI can guarantee the internal logical consistency (coherence) of a theory within a given world model but cannot confirm its alignment (correspondence) with empirical reality, which remains the prerogative of the experimental method [2, 6]. Thus, AI is utilized as an ideal logical engine, lacking access to truth but capable of rigorous verification of the structural integrity of knowledge [1, 2].

Conclusion

The research identifies that transforming AI from a text generator to a deductive analysis tool establishes a new epistemic infrastructure. AI-Resilient Science ensures scientific theory reproducibility at the logical structure level. Executable documents function effectively as operational specifications of thought. Adversarial deduction among independent models identifies axiomatic weaknesses, converting statistical errors into validation instruments. Future research involves developing tools for automated In-Context ontology creation and integrating the method into theoretical physics.

REFERENCES

1. Augustine of Hippo. Confessions. Oxford University Press, 2008. 384 p.
2. Popper K. The Logic of Scientific Discovery. Routledge, 2002. 544 p.
3. Vaswani A. et al. Attention Is All You Need. NeurIPS. 2017.
4. Wei J. et al. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models. NeurIPS. 2022.
5. Lemeshko A. Temporal Theory of the Universe. Zenodo / ResearchGate.
6. Ji Z. et al. Survey of Hallucination in Natural Language Generation. ACM Computing Surveys. 2023.
7. Floridi L. The Philosophy of Information. Oxford University Press, 2011. 416 p.

OUTBOUND TRAFFIC ANOMALY DETECTION ALGORITHM FOR IOT DEVICES

Nataliia PETLIAK (PhD, Senior Lecturer of Cybersecurity Department at Khmelnytskyi national university)[1]
Yurii KLOTS (candidate of technical sciences, associate professor, head of cybersecurity department at Khmelnytskyi national university)[1]

[1]*Khmelnytskyi national university, faculty of information technologies, cybersecurity department, npetlyak@khmnu.edu.ua*
[1]*Khmelnytskyi national university, faculty of information technologies, cybersecurity department, klots@khmnu.edu.ua*

Summary

This study presents an algorithm for detecting anomalies in outbound IoT traffic using fuzzy clustering and Sugeno-type inference. By automating rule generation through the Fuzzy C-Means and Wang–Mendel algorithms, the proposed approach eliminates expert dependency and reduces computational overhead. Validated using the CSE-CIC-IDS2018 dataset, the model effectively identifies botnet activity and network scanning. The results demonstrate an adaptive and interpretable solution suitable for securing resource-constrained IoT devices in real-world infrastructures.

Introduction

The rapid expansion of the Internet of Things has resulted in the widespread deployment of network-connected devices with limited computational resources and simplified security mechanisms, which increases their exposure to network-based threats and complicates the application of conventional protection solutions. A characteristic feature of IoT infrastructures is the predominance of outbound network traffic related to telemetry, control signaling, and communication with external services, where anomalies often indicate early stages of device compromise or unauthorized activity. At the same time, existing IoT traffic monitoring solutions face challenges in terms of computational overhead, adaptability, and interpretability, which motivates the development of lightweight and transparent approaches for detecting abnormal behavior in outbound network traffic of IoT devices.

Modern Internet of Things (IoT) and cyber-physical systems often feature end devices with limited computing resources and minimal built-in security, making them highly vulnerable to network attacks. A key characteristic of IoT infrastructures is the dominance of outbound network traffic generated by telemetry transmission, service messages, and interactions with remote services. Analyzing this outbound traffic enables the timely detection of device compromise, botnet activity, or stealthy network scanning, making it a promising focus for the development of anomaly detection systems. However, most modern approaches to IoT traffic analysis rely on classical machine learning methods [1], which require significant computational resources, lengthy training phases, and complex parameter tuning. Alternative approaches based on fuzzy logic [2] offer interpretability but, in their traditional

form, heavily depend on expert assessments for defining term sets, membership functions, and rule bases. This dependence complicates system scalability and increases deployment time.

In this context, the study focuses on developing an anomaly detection algorithm for outbound network traffic of IoT devices. The proposed algorithm combines the advantages of fuzzy logic with automated knowledge acquisition methods, thereby minimizing the influence of subjective expert assessments, reducing model configuration time, and lowering computational overhead compared to classical machine learning approaches.

The study proposes an algorithm for analyzing outbound network traffic of IoT devices (Fig. 1), based on fuzzy logic with the use of fuzzy clustering and Sugeno-type inference. The scientific novelty of the proposed approach lies in the automated generation of term sets and fuzzy rules derived from the statistical properties of network traffic without expert involvement. In particular, Fuzzy C-Means clustering is employed not only for preliminary data analysis but also as a core mechanism for constructing linguistic variables and membership function parameters, ensuring consistency of the fuzzy model with real-world characteristics of IoT traffic.

The input data for the algorithm consists of IoT device outbound network traffic parameters. The model is trained and evaluated using the CSE-CIC-IDS2018 dataset, which is widely used for modeling IoT device behavior in heterogeneous networks due to its diverse network activity scenarios, including reconnaissance, scanning, and botnet interactions. The structure of this dataset accurately reflects outbound traffic flows typical of IoT environments, making it suitable for both training and validation of the proposed algorithm.

At the initial stage, the algorithm performs network data collection and preprocessing, including outlier removal, feature normalization, and formation of the training dataset. Particular emphasis is placed on parameters that most informatively characterize IoT outbound activity, such as flow duration and forward packet count. These features enable effective detection of deviations associated with atypical transmission intensity or prolonged sessions uncharacteristic of normal IoT device operation.

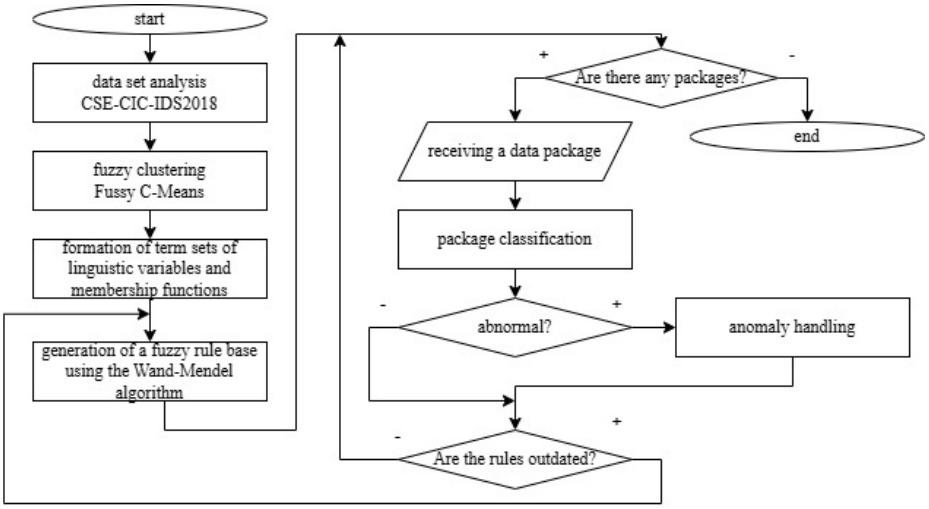


Fig. 1 – Algorithm for Analyzing Outbound Network Traffic of IoT Devices

Further analysis of the training dataset is conducted using the Fuzzy C-Means clustering algorithm, which is applied for the automated formation of linguistic terms for input variables. The fuzzy nature of the clustering enables the representation of gradual transitions between normal and anomalous network traffic states, which is characteristic of IoT systems where anomalies tend to accumulate over time rather than manifest instantaneously. The clustering results are interpreted as term sets of linguistic variables describing different levels of abnormality in outbound traffic of IoT devices.

Based on the obtained clusters, trapezoidal membership functions are constructed, with parameters automatically determined without expert involvement. This ensures the objectivity of the model and enhances its consistency with the real-world statistical properties of IoT traffic. System adaptability to changes in the network environment is achieved through periodic updates of membership function parameters during operation.

The Wang–Mendel algorithm is employed to construct the knowledge base, enabling the automatic generation of fuzzy IF–THEN rules from the training data. The implementation of rule weighting and normalization ensures conflict resolution and reduces redundancy in the knowledge base, which is crucial for resource-constrained IoT traffic analysis systems.

The final stage of the algorithm is implemented as a Sugeno-type fuzzy inference system, which provides high processing speed and enables direct computation of a numerical anomaly index. The resulting index is used to classify outbound network traffic of IoT devices as normal or anomalous and can serve as a basis for developing early attack detection systems.

In this study, the authors propose an algorithm for detecting anomalies in outbound network traffic of IoT devices, designed to operate under conditions of limited computational resources and dynamic network environments. The proposed approach ensures automated formation of decision-making rules based on the statistical characteristics of traffic, which reduces dependence on subjective configuration and simplifies deployment in heterogeneous IoT infrastructures. The algorithm focuses on the analysis of outbound connections, which represent an informative source for the early detection of device compromise and atypical network activity. The proposed algorithm is characterized by low computational complexity and stable performance under varying traffic loads, making it suitable for real-time network security monitoring systems. A key feature of the approach is the transparency of the decision-making process, which enables interpretability of analysis results and supports their practical use in incident response procedures. This property is particularly important for critical and industrial IoT environments, where explainability of security decisions is essential. Experimental evaluation confirms the effectiveness of the algorithm in detecting anomalous activity in outbound traffic of IoT devices and its robustness to variations in network conditions. The obtained results indicate the feasibility of applying the proposed approach as a component of comprehensive IoT security systems and demonstrate its potential for the further

development of automated solutions for network behavior analysis with minimal computational overhead.

REFERENCES

7. Yu. Klots, N. Petliak, S. Martsenko, V. Tymoshchuk, I. Bondarenko. Machine learning system for detecting malicious traffic generated by IoT devices. CEUR Workshop Proceedings, 2nd International Workshop on Computer Information Technologies in Industry 4.0 (CITI 2024). Ternopil, Ukraine, June 12-14, 2024. Vol. 3742. P. 97-110
8. V. Titova, Yu. Klots, V. Cheshun, N. Petliak, A.-B.M. Salem. Detection of network attacks in cyber-physical systems using a rule-based logical neural network. CEUR Workshop Proceedings, 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS 2024). Khmelnytskyi, Ukraine, June 28, 2024. Vol. 3736. P. 255-268

INTELLIGENT MODEL OF THE EDUCATIONAL PLATFORM FOR DISTANCE LEARNING

Oleksii SAVON (Postgraduate student)[1]

[1]*State University of Trade and Economics, Faculty of Information Technologies, Department of Software Engineering and Cybersecurity, Kyiv, Ukraine*
[1] o.savon@knute.edu.ua

Abstract

The paper develops an intelligent neural network model based on a recurrent neural network (RNN) that provides personalized support for the learning process. The use of RNN in distance learning platforms makes it possible not only to predict learning success and identify difficult topics, but also to create adaptive learning paths that increase motivation and effectiveness.

Keywords

Distance learning, educational process, educational platform, intellectual analysis of the educational process, recurrent neural network, artificial neural network.

Introduction

Thanks to rapid advances in digital technology, distance learning platforms have become an important part of modern education, providing convenient access, flexibility, and the possibility of an individualized approach. At the same time, despite their widespread use, there is now a need to create models that can process large amounts of data on user behavior over time, predict learning outcomes, and provide recommendations for content personalization.Recurrent neural networks (RNN), thanks to their feedback mechanism and internal memory, allow you to process sequences of any length, accumulate context, and generate predictions and recommendations based on the student's previous actions. The aim of the work is to develop an intelligent neural network model based on a recurrent neural network (RNN) that analyzes student activity and thus provides personalized support for the learning process.

Research results

One of the key tasks in developing an educational platform for distance learning is to build a neural network model that allows for intelligent analysis of the learning process, forecasting, and adaptation of content to student needs.To implement forecasting and recommendation tasks in the distance learning system, RNN was chosen as the main architecture [1, 2, 3]. It provides a balance between complexity, functionality, and quality of adaptation to the user's learning behavior. Let each user have a sequence of actions in time:

$$X = \{x_1, x_2, ..., xT\}$$

where $x_t \in R^n$ is the vector of user parameters at step t. Each vector includes: ratings (g_t), activity time (a_t), viewing materials (m_t), completing tests (t_t), and lesson topic (s_t).

It is necessary to build a model f that implements:

- regression forecasting assessment: $\hat{y}_T = f(X)$;
- classification of the probability of successful completion of the course: $\hat{y}_T = P(\text{success} \mid X)$.

Model requirements: ability to process sequences of variable length actions; context awareness: time, topic, level of understanding; high prediction accuracy and adaptability; recommendation module support; ability to integrate with gamification mechanisms.

A recurrent neural network (RNN) is an artificial neural network designed to process data sequences by using an internal state (memory) that is updated at each time step. Let us consider the mathematical description of an RNN [1, 4, 5].

The state is updated as follows: at each time step t, the hidden state h_t is updated using the input vector x_t and the previous state h_{t-1}:

$$h_t = \sigma_h(W_{xh} * x_t + W_{hh} * h_{t-1} + b_h) \quad (1)$$

where σ_h is a nonlinear activation function, W_{xh} is a weight matrix from the input to the hidden layer, W_{hh} is a weight matrix between hidden states, and b_h is the bias terms. The output of the y_t network is calculated as:

$$y_t = \sigma_y(W_{hy} * h_t + b_y) \quad (2)$$

where σ_y is the output activation function, W_{hy} is the weight matrix from the hidden state to the output, and b_y is the bias terms. When training on a sequence of length T, the total loss function is as follows:

$$\mathcal{L} = \sum_{t=1}^{T} \mathcal{L}_t(\hat{y}_t, y_t) \quad (3)$$

where $\hat{y}_t$ is the actual (reference) value of the output at step t. RNN training is performed using the Backpropagation Through Time (BPTT) algorithm, which takes into account the dependencies between all-time steps:

$$\frac{\partial \mathcal{L}}{\partial W} = \sum_{t=1}^{T} \frac{\partial \mathcal{L}_t}{\partial \hat{y}_t} \cdot \frac{\partial \hat{y}_t}{\partial h_t} \cdot \frac{\partial h_t}{\partial W} \quad (4)$$

Each student forms a sequence of events $\{x_1, x_2, ..., x_T\}$, where each x_t is a vector of features, for example: practical work assessment (g_t), time of activity in the system (a_t), time spent working with theoretical material (v_t), test completion (t_t, 0 or 1), lesson topic (s_t, in the form of one-hot encoding). The network processes the sequence $\{x_1, x_2, ..., x_T\}$, updating the hidden state h_t and generating a prediction y_t – for example, the probability of successful completion of the module or the expected final grade.
The state of the hidden layer is updated at each time step:

$$h_t = \tanh(W_{xh} * x_t + W_{hh} * h_{t-1} + b_h) \quad (5)$$

Projected output is:

$$\hat{y}_t = \sigma(W_{hy} * h_t + b_y), \quad (6)$$

where W_{xh} is the input weights; W_{hh} is the recurrent weights; W_{hy} is the output weights; σ is the sigmoid.
Forecasting tasks are:

– Assessment forecast:

$$\hat{y}_T = \text{expected grade} \in [0,100] \quad (7)$$

– Probability of completing the course:

$$\hat{y}_T = P(\text{successful completion of the course} \mid x_1, x_2, ..., x_T) \quad (8)$$

The loss function for the entire sequence is as follows:

$$\mathcal{L} = \sum_{t=1}^{T} \mathcal{L}_t(\hat{y}_t, y_t)$$

Backward propagation of error (BPTT) allows updating the weights W_{xh}, W_{hh}, W_{hy}.
LSTM can be used to overcome fading gradient problems:

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f)$$
$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i)$$

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o)$$
$$\check{c}_t = tanh(W_c x_t + U_c h_{t-1} + b_c)$$
$$c_t = f_t \odot c_{t-1} + i_t \odot \check{c}_t$$
$$h_t = o_t \odot tanh(c_t)$$

The architecture of the recurrent neural network is shown in Fig. 1.

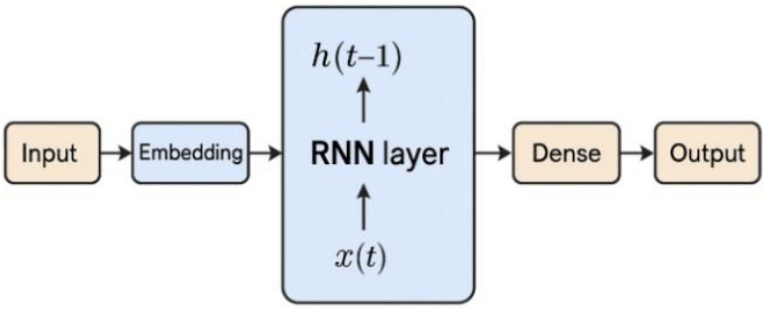


Fig. 1. Recurrent Neural Network (RNN) Architecture

Input is vectors that describe the user's state at each time step. Such features may include the number of materials viewed, activity time, ratings, test completion status, and lesson topic (in the form of one-hot vectors).
Embedding (Vector representation) – this layer (optional) is mainly used for categorical features or for smoothing the dimension of input vectors. It converts one-hot representations into dense vector representations, helping to reduce dimension and redundancy.
The RNN layer is the central component of the architecture. At each step, a new hidden state *h(t)* is calculated, which takes into account the current input *x(t)* and the previous state *h(t−1)* according to the formula:

$$h(t)_t = \tanh(W_{xh} * x_t + W_{hh} * h_{t-1} + b_h)$$

Here, context accumulation takes place – the RNN “remembers” what the student did in the previous steps.
Dense (Output layer) is a fully connected layer that converts the hidden state into a predicted variable.
Output – the final prediction for a given step or sequence as a whole.
The arrow from $h_{(t-1)}$ back into the RNN indicates recursion: the network uses the previous state at each step.

Conclusions

This paper defines and describes a recurrent neural network (RNN) model, a type of artificial neural network designed to analyze data sequences. It uses internal memory that stores information from previous steps to improve data processing in each

subsequent step. In the planned distance learning system, RNN, unlike other models for distance learning educational platforms, allows for intelligent analysis of the learning process, adaptation of content to the needs of each student, etc., and has broad prospects and potential for development.

REFERENCES

[1] Zadachyn V. M., Konjushenko I. G., «Systems modeling: lecture notes» (in Ukrainian), Kharkiv, HNEU, 2010. 268 p.

[2] Soloviov V. M., «Modeling of complex systems» (in Ukrainian), Cherkasy, 2015. 353 p. DOI: *https://doi.org/10.31812/0564/1147*.

[3] Fekri M. N., Patel H., Grolinger K., Sharma V., «Deep Learning for Load Forecasting with Smart Meter Data: Online Adaptive Recurrent Neural Network. Applied Energy», 2021, vol 282, Part A, article no. 116177. DOI: *https://doi.org/10.1016/j.apenergy.2020.116177*.

[4] Ritter H., Martinetz T., Schulten, K., «Neural Computation and Self-Organizing Maps; An Introduction», Addison-Wesley Longman Publishing Co. Inc., 1992. 306 p.

[5] Salem F. M., «Recurrent Neural Networks: From Simple to Gated Architectures», Springer, Accessed: 2022. [Online]. Available: *https://www.scribd.com/document/566571215/Recurrent-Neural-Networks-From-Simple-to-Gated-Architectures-by-Fathi-M-Salem-z-lib-org*.

MIDDLEWARE-BASED INTERCEPTORS FOR SECURING IOT-DRIVEN FEDERATED LLM AGENTS

Volodymyr MATIIEVSKYI (Senior lecturer)[1]

[1]*National University of Life and Environmental Sciences of Ukraine, Faculty of Information Technologies, Department of Computer systems, networks and cybersecurity, cybersecurity, m_vv@outlook.com*

Abstract

The integration of IoT and Generative AI has led to Federated Agents, autonomous systems that use Federated Learning (FL) to fine-tune LLMs on distributed edge data. Although FL enhances privacy by retaining data locally, it is susceptible to semantic attacks such as prompt injection and knowledge poisoning. Existing server-side defenses fail to detect these linguistic threats. This paper introduces Federated Guardrails, shift-left security approach using middleware-based interceptors at the IoT edge to sanitize inputs, monitor outputs, and reduce attack success rates while preserving low-latency performance

Keywords

Federated Learning, Internet of Things (IoT), Large Language Models (LLMs), Middleware Security, Prompt Injection, Federated Guardrails, Shift Left Security

Introduction

By 2026 forecasts estimate more than 64 billion IoT devices online. The rapid proliferation of IoT devices has evolved beyond simple data collection to encompass complex decision-making via Federated Learning (FL). “In FL, the algorithm training is performed in a decentralized manner by different nodes, or clients, that use local data. In this scenario, each decentralized node trains an individual model using its

own data and shares the model parameters (instead of the data) with the rest." [5]. We are witnessing the emergence of Federated Agents, where IoT nodes (e.g., smart home hubs, industrial controllers) collaboratively train LLMs to reason and act within their environments. However, this decentralization introduces severe security risks [4, 138510]. Federated learning aims to train machine learning models on distributed datasets across multiple devices while preventing data leakage. In this approach, a global model is shared with IoT devices, where it is locally updated using on-device data, and only the resulting model updates are transmitted back, rather than the raw data itself [3]. Standard FL defenses focus on Model Poisoning—preventing malicious gradient updates from corrupting the global model. Yet, LLM-based agents face unique semantic threats: Prompt Injection: Adversaries manipulate input data with hidden instructions (e.g., "Ignore safety rules") to override the agent's alignment. If a federated client trains on such data, the global model may generalize this vulnerability. RAG Poisoning: In Retrieval-Augmented Generation (RAG) systems, attackers inject malicious documents into the local knowledge base, causing the agent to hallucinate or execute harmful commands. These attacks bypass traditional weight-based defenses because the "poison" is not a statistical outlier in the gradient space but a semantic pattern in the data space. To address this, we argue for a "Shift Left" approach. Security must move from the central server to the Client Input Stage, implementing Federated Guardrails—middleware that intercepts and sanitizes data streams at the edge.

Materials & methods

Authors propose different approaches for FL example [1],[2],[6], but we can improve them by using the "Shift Left" principle, borrowed from DevSecOps, dictates that security checks should occur as early as possible in the data lifecycle. In the context of Federated IoT, this means validating data before it enters the local training loop. This is implemented via the Interceptor Pattern, a middleware layer wrapping the FL client. We propose a middleware architecture that sits between the raw IoT data stream and the local LLM. This middleware functions as a bi-directional filter: Input Interceptors: Sanitize incoming prompts and training data. We utilize lightweight, edge-compatible classifiers (regex-based rules) to detect prompt injection signatures. Output Interceptors: Monitor the agent's actions during the evaluation phase. If the agent generates toxic content or hallucinates (detected via uncertainty quantification), the update is suppressed locally.

Algorithm and Pseudocode

The following algorithm describes the SecuredFlowerClient, which integrates guardrail middleware using the Flower framework and LangChain callbacks (Fig. 1).

Require: Local Data $D = \{(x_i, y_i)\}$, Global Model W_t
Require: Guardrail Policy $\mathcal{G}_{in}(\cdot), \mathcal{G}_{out}(\cdot)$
Receive W_t from Server
$D_{safe} \leftarrow \emptyset$
for $(x_i, y_i) \in D$ **do**
  if $\mathcal{G}_{in}(x_i) ==$ Safe **then** ▷ Input Interceptor (e.g., Injection Check)
    $\hat{y} \leftarrow \text{Model}(W_t, x_i)$
    if $\mathcal{G}_{out}(\hat{y}) ==$ Safe **then** ▷ Output Interceptor (e.g., Toxicity Check)
      $D_{safe} \leftarrow D_{safe} \cup \{(x_i, y_i)\}$
    else
      LogThreat($\hat{y}$); **continue**
  else
    LogThreat(x_i); **continue**
end for
$\Delta W \leftarrow \text{Train}(W_t, D_{safe})$
return $\Delta W, |D_{safe}|$

Fig.1 Pseudocode of proposed algorithm

Results

For evaluation test we created guardrail policies (regex-based rules) for known injections and create dataset, and make comparation with using local LLM-as-a-judge. Comparing our client-side filtering against traditional server-side robust Implementing the "Shift Left" interceptor reduced the ASR to <15%, outperforming server-side defenses which often struggle to distinguish semantically poisoned updates from legitimate data drift. The middleware introduces a negligible overhead. Benchmarks indicate that optimized guardrails are 1.5x faster than "LLM-as-a-judge" evaluation methods, making them suitable for real-time edge processing. By filtering malicious data before training (Shift Left), we avoid the computational cost of backpropagation on poisoned samples. This resulted in an 2x reduction in wasted compute resources compared to post-training filtering.

Discussion

The results confirm that moving security controls to the edge—"Shifting Left"—is not only a security imperative but an efficiency one for IoT. In bandwidth-constrained networks, preventing "garbage in" (poisoned data) prevents "garbage out" (poisoned models) and saves vital energy resources. A limitation of this approach is the need to update the guardrail policies themselves. If the guardrail model (e.g., the toxicity classifier) is static, it may become obsolete against new jailbreak techniques. Future work will explore Federated Policy Sync, where clients collaboratively train the guardrail model itself, ensuring the defense evolves alongside the threats. Also, the model's performance was evaluated on an artificial data set and the results may

differ significantly on other data sets for example Bot_IoT, Iot network intrusion [5]. Also of the limitations in the experimentation has been the low numbers of clients.

Conclusion

"Federated Guardrails" represent a critical advancement in securing IoT-driven Federated Agents. By implementing middleware interceptors that sanitize inputs and monitor outputs at the edge, we effectively neutralize semantic threats like prompt injection and RAG poisoning before they can corrupt the global model. This "Shift Left" architecture offers a scalable, low-latency, and privacy-preserving solution that bridges the gap between IoT constraints and the security demands of Generative AI.

REFERENCES

1. Alahmari S., Alkharashi A. Privacy-Aware Federated Learning Framework for IoT Security Using Chameleon Swarm Optimization and Self-Attentive Variational Autoencoder. *Computer Modeling in Engineering & Sciences*. 2025. P. 1–10. URL: https://doi.org/10.32604/cmes.2025.062549
2. Anupriya, Malik A. Clustering in iot based wireless sensor network using swarm intelligence and machine learning approaches: review and future directions. *Procedia computer science*. 2025. Vol. 259. P. 1024–1033. URL: https://doi.org/10.1016/j.procs.2025.04.056
3. A Survey on Federated Learning for Resource-Constrained IoT Devices / A. Imteaj et al. *IEEE Internet of Things Journal*. 2021. P. 1. URL: https://doi.org/10.1109/jiot.2021.3095077 .
4. Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis / M. A. Ferrag et al. *IEEE Access*. 2021. Vol. 9. P. 138509–138542. URL: https://doi.org/10.1109/access.2021.3118642.
5. Federated learning for malware detection in IoT devices / V. Rey et al. *Computer Networks*. 2022. Vol. 204. P. 108693. URL: https://doi.org/10.1016/j.comnet.2021.108693.
6. Federated Learning Meets Swarm Intelligence: A Privacy-Centric Framework for Big Data Processing / P. Gadiraju et al. *2025 Global Conference in Emerging Technology (GINOTECH)*. 2025. P. 1–9. URL: https://doi.org/10.1109/GINOTECH63460.2025.11076871.

ПІДХІД ДО ПЕРСОНАЛІЗАЦІЇ СЕРВІСІВ В IoT-ОРІЄНТОВАНОМУ SMART-СЕРЕДОВИЩІ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ

Andriy HOLYNSKYI (Postgraduate)[1]
Tetiana ZHYROVA (PhD, Associate Professor)[2]

[1,2] State University Trade and Economic, Kyiv, Ukraine
[1,2] Department of Software Engineering and Cybersecurity
[1] a.holynskyy@knute.edu.ua, [2] zhyrova@knute.edu.ua

Abstract

This paper addresses the problem of service personalization in IoT-oriented smart environments characterized by dynamic context and heterogeneous devices. The aim of the study is to develop a multi-criteria model for service personalization based on user characteristics, contextual parameters, and IoT data. The proposed approach enables coordinated decision-making and improves adaptability of smart services. The results can be applied in the design of IoT-based smart systems.

Keywords

Internet of Things; smart services; personalization; multi-criteria model.

Вступ

Розвиток Інтернету речей сприяє формуванню IoT-орієнтованих smart-середовищ, у межах яких інтегрується гетерогенні пристрої, сервіси та користувачі. Інтернет речей розглядається як глобальна інфраструктура взаємодії фізичних об'єктів та інформаційних систем, що створює основу для навчання інтелектуальних сервісів у режимі реального часу [1, с. 1-3]. IoT-орієнтовані smart-середовища характеризуються динамічністю контексту, розподіленою архітектурою та різноманіттям користувацьких потреб. За таких умов застосування статичних підходів до надання сервісів є неефективним і не забезпечує належного рівня адаптації до змін середовища та індивідуальних вимог користувачів [3, с. 22-26; 4, с. 1-5]. Персоналізація сервісів дозволяє підвищити ефективність функціонування smart-систем шляхом адаптації їх параметрів до контексту використання та характеристик користувачів. Водночас реалізація персоналізованих сервісів потребує одночасного врахування множини критеріїв, що зумовлює доцільність застосування багатокритеріальних моделей прийняття рішень в IoT-орієнтованих smart-середовищах [6, с. 83-86; 8, с. 13051-13055].

Актуальність дослідження зумовлена зростанням складності IoT-орієнтованих smart-середовищ і необхідністю адаптації сервісів до динамічних умов та індивідуальних потреб користувачів.

Метою роботи є обґрунтування доцільності використання багатокритеріального підходу при персоналізації сервісів в IoT-орієнтованому smart-середовищі.

Постановка задачі та методи дослідження

IoT-орієнтовані smart-середовища функціонують у умовах постійної зміни контексту, що зумовлено динамікою параметрів середовища, стану пристроїв та поведінки користувачів. За таких умов виникає задача забезпечення адаптивного надання сервісів з урахуванням індивідуальних потреб користувачів і технічних обмежень IoT-інфраструктури. Аналіз архітектури IoT-систем свідчить про доцільність використання моделей прийняття рішень, які дозволять обробляти різнорідні вхідні дані та підтримувати гнучку адаптацію сервісів [2]. З огляду на багатофакторний характер процесу персоналізації сервісів, зазначена задача не можу бути ефективно розв'язана із застосування однокритеріальних підходів. Персоналізація в IoT-орієнтованих smart-середовищах потребує одночасного врахування характеристик користувача, параметрів контексту використання, а також технічних і ресурсних обмежень системи, що зумовлює необхідність застосування багатокритеріальних моделей прийняття рішень [6, с. 83-98; 8, с. 13051-13069]. Для досягнення поставленої мети у роботі визначено такі завдання:

- формування множини критеріїв персоналізації сервісів в IoT орієнтованому smart-середовищі;
- розроблення узагальненої багатокритеріальної моделі персоналізації сервісів.

У дослідженні використано методи системного аналізу, що дозволяють формалізувати структуру IoT-орієнтованого smart-середовища та взаємозв'язки між його компонентами, а також методи багатокритеріального прийняття рішень, зокрема підходи, орієнтовані на оцінювання альтернатив за сукупністю кількісних і якісних критеріїв [6, с. 83-98; 7, с. 15-18]. Для узагальнення сучасних підходів до багатокритеріального аналізу та підтвердження можливості їх застосування у smart-системах використано результати оглядових досліджень [8, с. 13051-13069]. Сформульовані положення та обрані методи визначать підхід до побудови багатокритеріальної моделі персоналізації сервісів в IoT-орієнтованому smart-середовищі, що дозволяє перейти до її безпосереднього опису та аналізу.

Багатокритеріальна модель персоналізації сервісів в iot-орієнтованому smart-середовищі

У IoT-орієнтованому smart-середовищі персоналізація сервісів здійснюється в умовах багатофакторності та динамічної зміни параметрів функціонування. Користувачі відрізняються за індивідуальними потребами, пріоритетами та контекстами використання сервісів, тоді як IoT інфраструктура характеризується обмеженими ресурсами, гетерогенністю пристроїв і розподіленою архітектурою. За таких умов доцільним є використання багатокритеріальної моделі, яка дозволяє формалізувати процес персоналізації сервісів з урахуванням сукупності різнорідних факторів [6, с. 83-98; 8, с. 13051-13069]. Запропонована модель персоналізації ґрунтується на поєднанні даних,

отриманих від IoT-пристроїв, характеристик користувача та параметрів контексту smart-середовища. У межах моделі процес персоналізації розглядається як задача виору або адаптації сервісу, доступні ресурси системи та пріоритети функціонування smart-середовища [7, с. 15-18]. На відміну від статичних і контекстно-орієнтованих підходів багатокритеріальна модель забезпечує узгоджене врахування кількісних і якісних показників, що дозволяє підвищити гнучкість і адаптивність процесу персоналізації сервісів. Такий підхід створює умови для прийняття обґрунтоваих рішень у ситуаціях, коли окремі критерії можуть мати суперечливий характер або різний рівень проритетності [8, с. 13051-13069; 9]. При формуванні багатокритеріальної моделі персоналізації також враховуються вимоги до безпеки та надійності IoT-пристроїв, визначені у сучасних нормативних документах і рекомендаціях, зокрема NIST IR 8259A та ETSI EN 303 645 [10, 11]. З метою наочного порівняння підходів до персоналізації сервісів у smart-системах у роботі узагальнено їх ключові характеристики, що наведено в таблиці 1.

Таблиця 1. Порівняльна характеристика підходів до персоналізації сервісів у IoT-орієнтованих smart-середовищах (розроблена автором)

Підхід	Користувач	Контекст середо-вища	IoT-дані	Багатокрите-ріальний аналіз
Статичний	так	ні	ні	ні
Контекстно-орієнтований	так	так	частково	ні
Багатокритеріа-льний	так	так	так	так

Узагальнення демонструє, що багатокритеріальний підхід дозволяє інтегрувати індивідуальні характеристики користувачів, контексті параметри та дані IoT-інфраструктури в єдину модель персоналізації, що є важливим для підвищення ефективності функціонування smart-сервісів.

Висновки

У роботі розглянуто проблему персоналізації сервісів в IoT-орієнтованих smart-середовищах, що функціонують в умовах динамічної зміни контексту та гетерогенності пристроїв. Обґрунтована доцільність застосування багатокритеріального підходу для підвищення адаптивності процесу персоналізації сервісів. Запропонована багатокритеріальна модель персоналізації сервісів, яка забезпечує узгоджене врахування характеристик користувача, параметрів smart-середовища та даних IoT-інфраструктури. Отримані результати можуть бути використані при проєктуванні IoT-

орієнтованих smart-систем і слугувати основою для подальших досліджень у напрямі розвитку адаптивних персоналізованих сервісів.

REFERENCES

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey // *Computer Networks*. – 2010. – Vol. 54, No. 15. – P. 2787–2805.
2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions // *Future Generation Computer Systems*. – 2013. – Vol. 29, No. 7. – P. 1645–1660.
3. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // *IEEE Internet of Things Journal*. – 2014. – Vol. 1, No. 1. – P. 22–32.
4. de Matos E., Tavares E. J., Tiburski R. T., Amaral L. A., Hessel F. Context information sharing for the Internet of Things: A survey // *Computer Networks*. – 2020. – Vol. 166. – Article 106988.
5. Gulzar B., Ullah I., Kim D. H., Lee J. W. Exploring Personalized Internet of Things: A survey on personalization approaches, challenges and future directions // *Internet of Things*. – 2024. – Vol. 25. – Article 100923.
6. Saaty T. L. Decision Making with the Analytic Hierarchy Process // *International Journal of Services Sciences*. – 2008. – Vol. 1, No. 1. – P. 83–98.
7. Hwang C. L., Yoon K. *Multiple Attribute Decision Making: Methods and Applications*. – Berlin : Springer, 1981. – 259 p.
8. Behzadian M., Otaghsara S. K., Yazdani M., Ignatius J. A state-of-the-art survey of TOPSIS applications // *Expert Systems with Applications*. – 2012. – Vol. 39, No. 17. – P. 13051–13069.
9. Brusilovsky P. Adaptive hypermedia // *User Modeling and User-Adapted Interaction*. – 2001. – Vol. 11. – P. 87–110.
10. Fagan M. J., Megas K. N., Scarfone K., Smith M. *Foundational Cybersecurity Activities for IoT Device Manufacturers (NIST IR 8259A)*. – Gaithersburg : National Institute of Standards and Technology, 2020. – 44 p.
11. ETSI EN 303 645 V2.1.1. Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI, 2020.

ADAPTIVE DATA PROCESSING MODEL AT EDGE AND FOG LEVELS OF INDUSTRIAL IoT SYSTEMS UNDER DEVICE COMPROMISE CONDITIONS

Valerii KOZLOVSKYI (D.Sc. in Engineering, Professor)[1]
Stanislava KUDRENKO (PhD in Engineering, Associate Professor)[2]
Ihor MAKIEIEV (PhD student)[3]

[1,2,3]State University "Kyiv Aviation Institute", 1 Liubomyra Huzara ave., Kyiv, 03058, Ukraine,
[1]valerii.kozlovskyi@npp.kai.edu.ua, [2]stanislava.kudrenko@npp.kai.edu.ua,
[3]8390988@stud.kai.edu.ua

Abstract
This paper investigates an approach to improving the resilience of Industrial Internet of Things systems through adaptive data processing at the edge- and fog-levels. The problem of edge-device compromise, which leads to data distortion and reduced reliability of decision-making processes, is considered. An adaptive model is proposed that combines local anomaly detection at the edge-level with neural network–based trust evaluation at the fog-level. A recurrent neural network is employed to estimate device trust by analyzing the temporal dynamics of behavioral, statistical, and network features. The proposed approach enables adaptive data weighting and reduces the impact of compromised devices without abrupt disconnection, thereby enhancing the reliability and robustness of industrial IoT systems.

Keywords
Industrial Internet of Things, edge computing, fog computing, neural networks, trust evaluation, anomaly detection.

Introduction
Industrial Internet of Things (IIoT) systems have found wide application in manufacturing, energy, transportation, and other critical sectors where reliability, responsiveness, and continuous data processing are key requirements. Such systems are characterized by a large number of distributed edge devices that collect primary information directly from physical objects and the operating environment. As the scale of IIoT systems grows, so does the level of cyber threats, particularly the risk of edge device compromise. These devices often have limited computational resources and simplified security mechanisms. Compromise of such devices can lead to data distortion, disruption of control algorithms, and erroneous decision-making, which is especially critical for industrial applications. Traditional approaches to centralized data processing in cloud environments do not always provide the required level of resilience and responsiveness under conditions of anomalous behavior of individual nodes. In this regard, the use of multi-level data processing architectures, particularly those combining edge- and fog-levels, becomes relevant. These architectures enable preliminary data analysis, reduce latency, and localize the impact of potentially compromised devices. The purpose of this work is to develop a model of adaptive data processing at the edge and fog-levels of industrial IoT systems, which ensures

dynamic assessment of the trust level of edge devices using machine learning methods and enhances the system's resilience to the compromise of individual components.

Research results

The proposed model is aimed at increasing the resilience of industrial IoT systems to such situations through adaptive data processing and dynamic assessment of the level of trust in edge-devices. The key feature of the model is the combination of local analysis at the edge-level with an intelligent mechanism for assessing trust at the fog-level, implemented using machine learning methods.

General structure of the model

The model is based on a multi-level architecture that includes edge- and fog- levels. The edge-level performs primary data processing and local anomaly detection, while the fog-level provides a generalized analysis of device behavior, trust level assessment, and customization of processing parameters. The cloud level within this model is considered as an environment for long-term storage and strategic analysis and does not participate in operational decision-making. The general process of data transfer and processing between levels can be formalized in the form of transformation (1):

$$D_{fog}(t) = \Phi(D_{edge}(t), M_{edge}(t)), \quad (1)$$

where $D_{edge}(t)$is the data collected by edge-devices at a point in time$t$, $M_{edge}(t)$ is the metadata of local analysis (signs, anomaly estimates), and is a $\Phi(\cdot)$ function of aggregation and generalization at the fog-level.

At the edge-level, each device performs primary data processing, which includes normalization, noise filtering, and aggregation of measurements in time windows. In addition, local anomaly detection is implemented at this level using lightweight machine learning methods suitable for limited computing resources. Such methods may include small-dimensional autoencoders, isolation forest, or online statistical models of normal behavior. For each edge device, an estimate of the abnormality of the data flow is generated:

$$a_i(t) = f_{edge}(x_i(t)), \quad (2)$$

where $x_i(t)$— the measurement vector of the i-th device at time t, $f_{edge}(\cdot)$ is the local ML model, $a_i(t)$ is a numerical estimate of the anomaly.

The edge- level does not make final decisions about compromise, but only transmits aggregated data to the fog-level along with anomaly scores (2) and basic statistical characteristics. The fog-lavel acts as an intelligent coordinator that has access to data

streams from multiple edge-devices. At this level, an extended feature vector is formed for each device, including:

- anomaly assessments from the edge-level;
- statistical characteristics of the signal (dispersion, stability);
- behavioral signs (frequency of errors, data omissions);
- network parameters (latency, packet loss, traffic volume);
- contextual parameters of the system operating mode.

The generalized vector of features has the form (3):

$$z_i(t) = [a_i(t), \Delta x_i(t), \sigma_i(W), loss_i(W), delay_i(W), traffic_i(W), \dots], \quad (3)$$

where W is the observation time window.

To assess the level of trust in edge devices, the model proposes a neural network module *Trust Neural Network (TNN)*, which operates at the fog-level. In order to take into account the temporal dynamics of device behavior, it is advisable to use a recurrent architecture, in particular GRU (Gated Recurrent Unit).

The process of assessing trust is formalized by equations:

$$h_i(t) = GRU(z_i(t), h_i(t-1)), \quad (4)$$

$$T_i(t) = \sigma(W h_i(t) + b), \quad (5)$$

Expression (4) is the hidden state of the model, $T_i(t) \in [0,1]$is a continuous indicator of the level of trust in the i-th device, $\sigma(\cdot)$ is a sigmoid activation function.

The obtained value (5) is used to adaptively control the impact of edge device data on the overall processing process. In particular, the model provides for data weighting according to the confidence level:

$$x_i^*(t) = T_i(t) \cdot x_i(t), \quad (6)$$

Equation (6) is weighted data used for further analysis and decision-making. In addition, depending on the value (5), the device can be switched to one of the modes of operation: normal, degraded or quarantine. This approach avoids abrupt shutdown of devices and ensures smooth adaptation of the system to changes in their behavior.

In case of compromise of the edge device, the model does not rely on a one-time solution, but analyzes the change in the level of trust over time. A gradual decrease $T_i(t)$indicates the accumulation of anomalous signs and allows you to localize the impact of the compromised node without disrupting the operation of the entire system. The fog-level can also initiate adaptive retraining of local ML models at the edge-level by updating their parameters. Thus, the proposed model combines local detection of anomalies at the edge-level with neural network trust assessment at the fog-level, which provides an adaptive response of the system to device compromise. The scientific novelty lies in the use of a continuous trust score formed on the basis of behavioral and network features using a recurrent neural network, as well as in the mechanism of adaptive data weighting in a multi-level edge–fog architecture.

Conclusions

The paper proposes a model of adaptive data processing at the edge and fog-levels of industrial IoT systems, focused on functioning in conditions of compromise of individual devices. The model combines local detection of anomalies at the edge-level with neural network assessment of the level of trust in devices at the fog-level, which allows you to dynamically limit the impact of inaccurate data without abruptly shutting down nodes. The use of a continuous trust score provides adaptive data weighting and increases the system's resilience to abnormal device behavior. The proposed approach can be applied in industrial IoT systems with increased requirements for reliability, security and efficiency of information processing.

REFERENCES

[1] R. C. Sofia, J. Soldatos**, «**Shaping the Future of IoT with Edge Intelligence», *Future Internet*, vol. 16, no. 3, Mar. 2024, Article 85.

[2] A. Abbas, S. U. Khan, A. Y. Zomaya**,** «Fog Computing: Theory and Practice», *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 6, Nov. 2020, Article e1352.

[3] R. Rezapour, M. A. Pourmina, A. Ghasemi**,** «Security in fog computing: A systematic review on issues and solutions», *Future Generation Computer Systems*, vol. 118, May 2021, pp. 197–217.

[4] A. K. Jumani, M. M. Qureshi, A. Raza**,** «Fog computing security: A review», *Security and Privacy*, vol. 6, no. 1, Jan. 2023, Article e173.

[5] A. M. Sheikh, M. H. Rehman, A. H. Khan**,** «A survey on edge computing security challenges», *Future Internet*, vol. 17, no. 4, Apr. 2025, Article 175.

[6**]** T. Zhukabayeva, A. O. Abid, S. Khan**,** «Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions», *Sensors*, vol. 25, no. 1, Jan. 2025, Article 213.

[7] A. Alwarafy, K. Al-Thelaya, M. Abdallah**,** «Security and privacy issues in edge computing-assisted internet of things», *IEEE Access*, vol. 8, Aug. 2020, pp. 40000–40020.

[8] L. Kong, Y. Wang, G. Chen, «Edge-computing-driven internet of things: A survey», *ACM Computing Surveys*, vol. 55, no. 4, Apr. 2022, Article 78.

A FUZZY–PERCEPTUAL APPROACH TO CANDIDATE RANKING IN A MULTICRITERIA DECISION SPACE

Volodymyr TEMNIKOV (Doctor of Science (Engineering), Professor)[1]
Andrii TEMNIKOV (Senior Lecturer)[2]
Tetiana SHCHERBAK (Candidate of Sciences (Engineering), Associate Professor)[3]

[1,2,3]*State University «Kyiv Aviation Institute»*
[1]*temnikov_v@ukr.net,* [2]*temnikoff@ukr.net,* [3]*tetiana.shcherbak@npp.kai.edu.ua*

Summary

This paper presents a fuzzy–perceptual approach to candidate ranking for high-risk, high-responsibility tasks. The method integrates quantitative measurements and qualitative expert assessments using interval type-2 fuzzy sets and perceptual computing. Expert inputs are aggregated via a linguistic weighted average operator within weighted graph structures, and candidates are ranked by centroid-based comparison of the resulting fuzzy evaluations. The approach supports transparent, well-founded decisions under uncertainty and incomplete information.

Reducing the impact of the human factor on the safety of safety-critical technological processes requires effective monitoring of personnel functional state (FS), particularly at the stage of professional selection. The complexity of such assessment is driven by multiple interacting factors, a large number of monitored indicators, and the need to engage experts from multiple domains. Of particular relevance is the control of psychophysiological state, which encompasses sensorimotor reactions, attention allocation and switching, visual and auditory memory, stress resilience, decision-making speed, and the ability to act under extreme conditions. At present, a contradiction persists between the demand for comprehensive FS assessment and the lack of a universal information toolkit capable of providing well- founded support to managerial decision-makers [1]. Addressing this challenge requires the development of information technologies and mathematical models that enable multidimensional analysis and forecasting of changes in personnel psychophysiological characteristics.

Effective managerial decision-making in professional selection and monitoring of personnel engaged in high-responsibility, high-risk activities requires integrated information support. The proposed approach to intelligent decision support is based on a generalized scheme of information links among the monitored subjects, expert assessments, and decision-makers. An information system developed on these principles can enable well-founded comparison of candidates using a set of FS indicators that includes not only psychophysiological characteristics but also health status measures and professional competence indicators (knowledge, skills, and abilities). Expert-driven assessment involving specialists in medicine, engineering, and related domains makes it possible to formalize personnel selection procedures and reduce the subjectivity of managerial decisions.

To ensure the objectivity and completeness of evaluation, a multilevel model of FS indicators is employed, integrating psychophysiological characteristics, health-related measures, and professional preparedness. Expert assessments are provided in both numerical and linguistic forms, thereby enabling the incorporation of information that cannot be adequately formalized on a purely quantitative scale.

The proposed approach is based on weighted graph models with linguistic input nodes [2], enabling aggregation of assessments while accounting for the relative importance of each factor (1). Assigning weights in a linguistic form, followed by numerical processing, improves usability for experts and reduces subjectivity in interpretation. The resulting mathematical model supports candidate ranking based on integral scores obtained through hierarchical fusion of assessments provided by multiple experts, each operating within their respective domain of specialization.

$$F = \sum_{i=1}^{n} \mu(w_i) \cdot \mu(l_i), \quad (1)$$

$\mu(w_i)$ is transformation function of the weight of the i-th criterion; $\mu(l_i)$ is numerical representation of the linguistic assessment of the i-th indicator. For effective pre-employment selection of personnel whose work involves elevated levels of strain and responsibility, a multilevel evaluation framework is advisable. Assessment is performed using both aggregated and physiological indicators, including the Baevsky Stress Index, which reflects the state of the cardiovascular regulatory system, as well as parameters of speech signals. Aggregated assessments may be represented as fuzzy intervals or linguistic variables. Because qualitative FS indicators are not directly formalizable, fuzzy set theory and perceptual computing are essential for integrating human expertise into the decision-making process.

The perceptual model comprises three principal processing stages. Experts' linguistic assessments are encoded as fuzzy sets. Subsequent computation is performed using Computing With Words (CWW), i.e., word-to-word transformations. Finally, the output is decoded into an aggregated assessment suitable for practical use (2).

$$f: \widetilde{W}_1 \times \widetilde{W}_2 \times \cdots \times \widetilde{W}_n \to \widetilde{W}_{out}, \quad (2)$$

$\widetilde{W}_i$ are fuzzy sets corresponding to the linguistic evaluations of the input variables; $\widetilde{W}_{out}$ is the resulting (overall) linguistic evaluation.

To support the development of an information system capable of effective personnel selection, a dataset is constructed that includes indicators of physiological state, psychophysiological characteristics, and professional readiness. Each assessment session is formalized as a column vector of indicator values, while temporal dynamics are captured via a matrix representation in which rows correspond to parameters and columns correspond to observation time points. Information is then generalized through linear aggregation using a vector of weighting coefficients.

To represent the fuzziness and subjectivity inherent in expert assessments, interval type-2 fuzzy sets (IT2FS) are employed; each set is characterized by upper and lower membership functions that define the uncertainty bounds. Linguistic assessments are modeled as trapezoidal IT2FS, enabling computational manipulation of linguistic terms within a computational framework [3]. Linguistic aggregation is performed through a CWW transformation using the Linguistic Weighted Average (LWA)

operator, which combines expert judgments while accounting for the relative importance of each parameter (3).

$$\tilde{A} = LWA(\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_k; w_1, w_2, \dots, w_k) = \bigoplus_{j=1}^{k} (w_j \otimes \tilde{p}_j), \quad (3)$$

$\tilde{p}_j$ is interval type-2 fuzzy set (IT2FS) representing the indicator assessment, w_j is corresponding weight. The results of the CWW transformation are subsequently used for candidate ranking. Specifically, ranking is based on computing the centroids of each IT2FS (4) and comparing the resulting values. This procedure enables transparent and well-justified evaluation of candidates for duties characterized by high neuro-emotional workload.

$$A_i = \frac{\sum_{j=1}^{k} \left(w_j \cdot Centroid(\tilde{p}_{ij}) \right)}{\sum_{j=1}^{k} w_j}, \quad (4)$$

$\tilde{p}_{ij}$ is IT2FS-based assessment of the j-th indicator for the i-th candidate; w_j is indicator weight. Based on this approach, a mathematically founded method for aggregating expert assessments is proposed, enabling the integration of quantitative and qualitative indicators while accounting for their relative importance. The proposed solutions provide flexibility in processing multidimensional information, robustness to incomplete data, and suitability for further automation of managerial decision-making. In the longer term, these results may serve as a basis for developing an intelligent decision support system for professional selection. The deployment of such a system would contribute to improved reliability, stability, and safety in organizations performing safety-critical tasks.

REFERENCES

1. P. Pavlenko, D. Tavrov, V. Temnikov, S. Zavgorodniy, and A. Temnikov, “The method of expert evaluation of airports aviation security using perceptual calculations”, in Proc. 2018 IEEE 9th Int. Conf. on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 2018, pp. 406–410. [Online]. Available: https://doi.org/10.1109/DESSERT.2018.8409168

2. G. Castellano, R. Scaringi, G. Vessio, and G. Zaza, “Integrating Graph Neural Networks and Fuzzy Logic to Enhance Deep Learning Interpretability,” in Proceedings of the EXPLIMED Workshop at ECAI 2024, 2024. [Online]. Available: https://ceur-ws.org/Vol-3831/paper1.pdf

3. K. Wiktorowicz, “T2RFIS: Type-2 Regression-Based Fuzzy Inference System,” Neural Computing and Applications, vol. 35, pp. 20299–20317, 2023. [Online]. Available: https://doi.org/10.1007/s00521-023-08811-7

CRDT-BASED DATA SYNCHRONIZATION IN AUTONOMOUS DISTRIBUTED IoT SYSTEMS

Andrii ALEKSANDROV (Postgraduate Student of the Department of Software Engineering and Cybersecurity, Python Developer)[1]
Nataliia KOTENKO (PhD in Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Software Engineering and Cybersecurity)[1]

[1]State University of Trade and Economics, Faculty of Information Technology, Department of Software Engineering and Cybersecurity, specialization: Software Engineering, a.aleksandrov@knute.edu.ua
[1]State University of Trade and Economics, Faculty of Information Technology, Department of Software Engineering and Cybersecurity, specialization: Software Engineering, kotenkono@knute.edu.ua

Summary

Data consistency in distributed IoT systems is examined under CAP and PACELC constraints. Traditional locking and Operational Transformation mechanisms prove limited for offline-first scenarios due to centralization dependencies. Conflict-free Replicated Data Types (CRDTs) are identified as a superior alternative, ensuring strong eventual consistency through commutative operations without central coordination. Despite increased metadata overhead, CRDT-based synchronization offers the essential fault tolerance and node autonomy required for resilient decentralized architectures.

Theoretical foundations of data consistency in distributed IoT systems

Ensuring data integrity and consistency is one of the fundamental problems of distributed computing systems. The relevance of this problem significantly increases in Internet of Things environments, where a large number of autonomous nodes exchange data under unreliable network conditions, variable latency, and possible communication failures. In such systems, devices often operate in partial isolation, which makes continuous centralized coordination infeasible. In distributed IoT architectures, synchronization is considered as a set of protocols that maintain consistency among replicated data stored at independent nodes. The core difficulty arises from the uncertainty of remote system states and the impossibility of guaranteeing instantaneous message delivery. Existing strategies are traditionally divided into pessimistic approaches, based on locking mechanisms, and optimistic approaches, which allow temporary divergence followed by asynchronous reconciliation [5]. The theoretical limits of such systems are formalized by the CAP theorem, which states that it is impossible to simultaneously guarantee consistency, availability, and partition tolerance [1]. Since network partitions and message loss cannot be excluded in real IoT deployments, the construction of CA-class systems is technically infeasible. In practice, system designers must choose a compromise between strong consistency and high availability. This concept is further refined by the PACELC theorem, which states that even in the absence of network partitions, a trade-off exists between latency and consistency [2]. This aspect is especially critical

for IoT systems, where network delays directly affect the correctness of decision-making in real-time applications such as smart homes, industrial sensor networks, and edge computing platforms. A practical implementation of availability-oriented architectures is provided by the BASE model, which assumes flexible system state and eventual consistency [3]. In such systems, temporary divergence of replicas is permitted as long as convergence is guaranteed in the absence of new updates. A key challenge in this context is maintaining correct event ordering and preserving causal dependencies between operations. Preserving causality in distributed environments requires specialized logical time mechanisms, since physical clocks cannot reliably reflect event precedence due to clock drift and variable network delays. Logical and vector clocks allow reconstruction of causal order and detection of concurrent operations, which is a necessary prerequisite for building correct synchronization algorithms in autonomous IoT nodes [4]. Thus, architectural constraints of distributed IoT systems necessitate abandoning strong consistency models and adopting eventual consistency with explicit causality support.

Data synchronization mechanisms for distributed IoT systems

Historically, the first approach to ensuring consistency relied on mutual exclusion mechanisms. Under this model, only one node is allowed to modify a shared resource at any given time, while others remain blocked. This approach guarantees linearizability and eliminates conflicts but is poorly suited for IoT systems due to high sensitivity to network latency and the lack of support for autonomous operation [5]. Subsequently, asynchronous approaches based on local updates and later merging were introduced. Three-way merge algorithms, widely used in version control systems, are effective for batch processing but unsuitable for real-time scenarios typical of sensor-based and control-oriented IoT applications. To eliminate blocking in real-time collaborative environments, the Operational Transformation method was proposed [6]. Its core idea is to transmit individual operations rather than full object states and to transform concurrent operations before application. The correctness of such algorithms relies on convergence and intention preservation properties [7]. However, full support of these properties has proven algorithmically complex in practice. In most real-world implementations, Operational Transformation requires a centralized server to linearize the operation order. This creates a single point of failure and prevents efficient deployment in peer-to-peer architectures and offline-first environments. For IoT systems with large numbers of autonomous nodes, such reliance on centralized coordination represents a fundamental limitation [6, 10].

An alternative approach is provided by Conflict-free Replicated Data Types. Unlike previous methods, CRDTs shift the responsibility for consistency from synchronization algorithms to the mathematical properties of data structures. For such types, either a merge function or a set of commutative operations is defined to guarantee convergence regardless of message delivery order [8, 9]. CRDTs are classified into state-based and operation-based types. In the former case, the merge

function must be associative, commutative, and idempotent, while in the latter all concurrent operations must be commutative. These properties ensure strong eventual consistency: all replicas that receive the same set of updates are guaranteed to converge to an identical state without centralized coordination [8]. The main drawback of classical CRDTs is the overhead in memory and network bandwidth consumption. Since data structures are monotonic, deletions are implemented logically using special markers, which leads to continuous growth of metadata. However, in IoT environments these costs are often acceptable in exchange for autonomy, fault tolerance, and resilience to intermittent connectivity.

Conclusions

The conducted analysis demonstrates that synchronization in autonomous distributed IoT systems is fundamentally constrained by CAP and PACELC trade-offs. Traditional pessimistic locking and operational transformation mechanisms provide limited scalability and autonomy due to their reliance on centralized coordination. conflict-free replicated data types enable strong eventual consistency while naturally supporting decentralized and offline-first architectures. These properties make CRDT-based synchronization a promising foundation for resilient large-scale IoT systems. Further research should focus on optimizing metadata management and designing hybrid synchronization mechanisms for resource-constrained devices.

REFERENCES

1. Gilbert S., Lynch N. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News. 2002. Vol. 33, no. 2. P. 51–59. URL: https://doi.org/10.1145/564585.564601 (date of access: 24.01.2026).
2. Abadi D. Consistency tradeoffs in modern distributed database system design: CAP is only part of the story. Computer. 2012. Vol. 45, no. 2. P. 37–42. URL: https://doi.org/10.1109/mc.2012.33 (date of access: 24.01.2026).
3. Kleppmann M. Designing data-intensive applications: the big ideas behind reliable, scalable, and maintainable systems. O'Reilly Media, Incorporated, 2017. 616 p.
4. Lamport L. Time, clocks, and the ordering of events in a distributed system. Communications of the ACM. 1978. Vol. 21, no. 7. P. 558–565. URL: https://doi.org/10.1145/359545.359563 (date of access: 24.01.2026).
5. Attiya H., Welch J. L. Sequential consistency versus linearizability. ACM transactions on computer systems. 1994. Vol. 12, no. 2. P. 91–122. URL: https://doi.org/10.1145/176575.176576 (date of access: 24.01.2026).
6. Ellis C. A., Gibbs S. J. Concurrency control in groupware systems. The 1989 ACM SIGMOD international conference, Portland, Oregon, United States. New York, New York, USA, 1989. URL: https://doi.org/10.1145/67544.66963 (date of access: 24.01.2026).
7. Ressel M., Nitsche-Ruhland D., Gunzenhäuser R. An integrating, transformation-oriented approach to concurrency control and undo in group editors. The 1996 ACM conference, Boston, Massachusetts, United States, 16–20 November 1996. New York, New York, USA, 1996. URL: https://doi.org/10.1145/240080.240305 (date of access: 24.01.2026).
8. Conflict-Free replicated data types / M. Shapiro et al. Lecture notes in computer science. Berlin, Heidelberg, 2011. P. 386–400. URL: https://doi.org/10.1007/978-3-642-24550-3_29 (date of access: 24.01.2026).

9. CRDT-based knowledge synchronization in an internet of robotics things ecosystem for ambient assisted living / J. Galeas et al. Computer vision and image understanding. 2025. P. 104437. URL: https://doi.org/10.1016/j.cviu.2025.104437 (date of access: 24.01.2026).
10. Gentle J., Kleppmann M. Collaborative text editing with eg-walker: better, faster, smaller. EuroSys '25: twentieth european conference on computer systems, Rotterdam Netherlands. New York, NY, USA, 2025. P. 311–328. URL: https://doi.org/10.1145/3689031.3696076 (date of access: 24.01.2026).

DECISION-MAKING UNDER UNCERTAINTY WITH COGNITIVE LOAD IN HUMAN-CENTERED DECISION SUPPORT SYSTEMS

Олександр ЛОЗКО (Магістр прикладної математики (ФПМ, КПІ), студент спеціальності “Психологія” (МАУП))
e-mail: alexanderlozko21@gmail.com

Abstract

This paper explores a human-centered approach to decision-making under uncertainty in decision support systems (DSS). It is shown that uncertainty in such systems arises not only from external data and environmental variability but also from latent human cognitive states. Cognitive load is considered a dynamic latent factor influencing the effectiveness of decision-making. A human-centered DSS architecture is proposed that adapts recommendations to both environmental uncertainty and users’ cognitive limitations.

Вступ

Сучасні системи підтримки прийняття рішень (Decision Support Systems, DSS) широко застосовуються в інтелектуальних та smart-системах для аналізу складних процесів і формування рекомендацій в умовах невизначеності. Такі системи активно використовують методи математичного моделювання, аналізу даних та штучного інтелекту з метою підвищення якості рішень у динамічних середовищах. У людиноцентричних системах підтримки прийняття рішень невизначеність має багатовимірний характер і може виникати на різних рівнях, зокрема на рівні зовнішнього середовища, внутрішнього стану користувача та інтерпретації рекомендацій системи. Проте більшість класичних підходів до побудови DSS зосереджуються переважно на моделюванні невизначеності даних або середовища, припускаючи, що людина здатна раціонально обробляти отриману інформацію без суттєвих когнітивних обмежень [1; 2].

Прийняття рішень в умовах невизначеності

Класичні DSS базуються на ймовірнісних моделях, баєсівському висновку та методах стохастичної оптимізації, де невизначеність розглядається як властивість зовнішнього середовища або даних [2]. Однак ефективність таких

систем у реальних умовах залежить не лише від точності моделей, але й від здатності користувача інтерпретувати та застосовувати рекомендації. Рішення в людиноцентричних DSS приймаються за наявності кількох джерел невизначеності, включаючи невизначеність середовища, людського стану та взаємодії користувача з системою. У межах даної роботи основна увага приділяється невизначеності зовнішнього середовища та латентному когнітивному стану користувача.

Когнітивне навантаження як латентний стан

Когнітивне навантаження розглядається як латентний динамічний стан користувача, що впливає на здатність обробляти інформацію та приймати рішення [1]. У межах DSS цей стан не вимірюється безпосередньо, а оцінюється на основі поведінкових індикаторів, таких як час реакції, частота помилок та патерни взаємодії з системою. Інтеграція когнітивного навантаження як системного параметра дозволяє враховувати обмеження людської когнітивної обробки інформації поряд із класичними моделями невизначеності.

Людиноцентрична архітектура DSS

Запропонована людиноцентрична архітектура DSS передбачає замкнений контур взаємодії, у якому система оцінює стан середовища та когнітивний стан користувача, формує адаптивні рекомендації та коригує свою поведінку на основі зворотного зв’язку [4]. Ефективність рекомендацій DSS значною мірою залежить від рівня ситуаційної обізнаності користувача та коректності інтерпретації інформації [3]. Залежно від рівня когнітивного навантаження система може змінювати кількість альтернатив, рівень деталізації пояснень або ступінь автоматизації рішень.

Висновки

У роботі запропоновано людиноцентричний підхід до прийняття рішень в умовах невизначеності, у межах якого когнітивне навантаження інтегрується як латентний динамічний стан користувача. Такий підхід дозволяє розширити класичні DSS та підвищити ефективність взаємодії людини з інтелектуальними системами. Подальші дослідження можуть бути спрямовані на розширення моделі людського стану та урахування додаткових джерел невизначеності.

REFERENCES

1. Kahneman D. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.
2. Simon H. A. *Models of Bounded Rationality*. Cambridge: MIT Press, 1982.
3. Endsley M. R. Toward a theory of situation awareness. *Human Factors*, 1995, Vol. 37, No. 1, pp. 32–64.
4. ISO 9241-210. *Human-centred design for interactive systems*. International Organization for Standardization, 2019.

MICROSERVICES ARCHITECTURE DESIGN OF WEB APPLICATION FOR BIOMETRIC DATA PROCESSING

Serhii BULBA (PhD, associate professor)[1]

[1]*State University of Trade and Economics, Faculty of information technologies, Department of Software Engineering and Cybersecurity, Kioto 19, Kyiv, 02156, Ukraine*
[1]*serhii.bulba@gmail.com*

Abstract

The article explores approaches to designing a microservice architecture for a web application for processing biometric data. Relevance of the work stems from the need to create scalable, flexible, and fault-tolerant biometric verification systems. Main focus is on the software architecture and the principles of decomposing functionality into independent services. The features of the integration interaction between system components within the microservice approach are considered.

Keywords

Microservice architecture, biometric data, biometric verification, web application, cloud-native design.

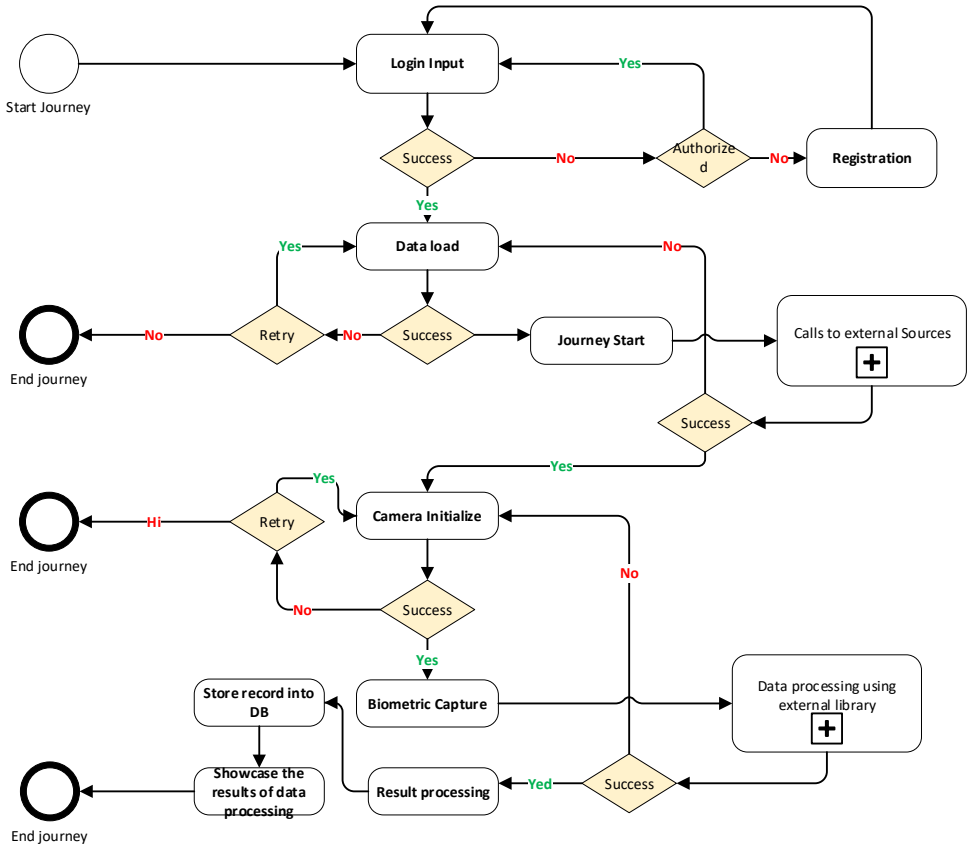
Introduction

Working with biometric data is in the field of view of a number of scientists and practitioners, and is always relevant from the point of view of applied application. Issues related to improving the architecture of solutions that process biometric information are becoming particularly relevant. Such solutions require high-accuracy results and the ability to flexibly scale and handle high loads. In particular, we are talking about processing large datasets containing images of people, converted to various formats. Increasing the efficiency of such solutions is achieved by applying the principles of microservice architecture, including leveraging multiple resources and technological stacks offered by cloud providers. The purpose of the research is to develop an architectural design of a microservice architecture for biometric data processing solutions.

Summary of the main material

Biometric verification in the modern world has become an integral part of many solutions and processes that help ensure privacy and control access to relevant data or locations. An important technology in the verification of biometric data is deep learning models of neural networks (deep learning). Gaiduchok M. A. [1], Chernyak O. I. [1], and Nazarkevych M. A. [2] investigated the basic principles of working with biometric data in the context of substantiating the mathematical apparatus and business logic of implementing the corresponding software solutions. Tymoshin Yu. A. [4] and Orlenko S. P. [4] note

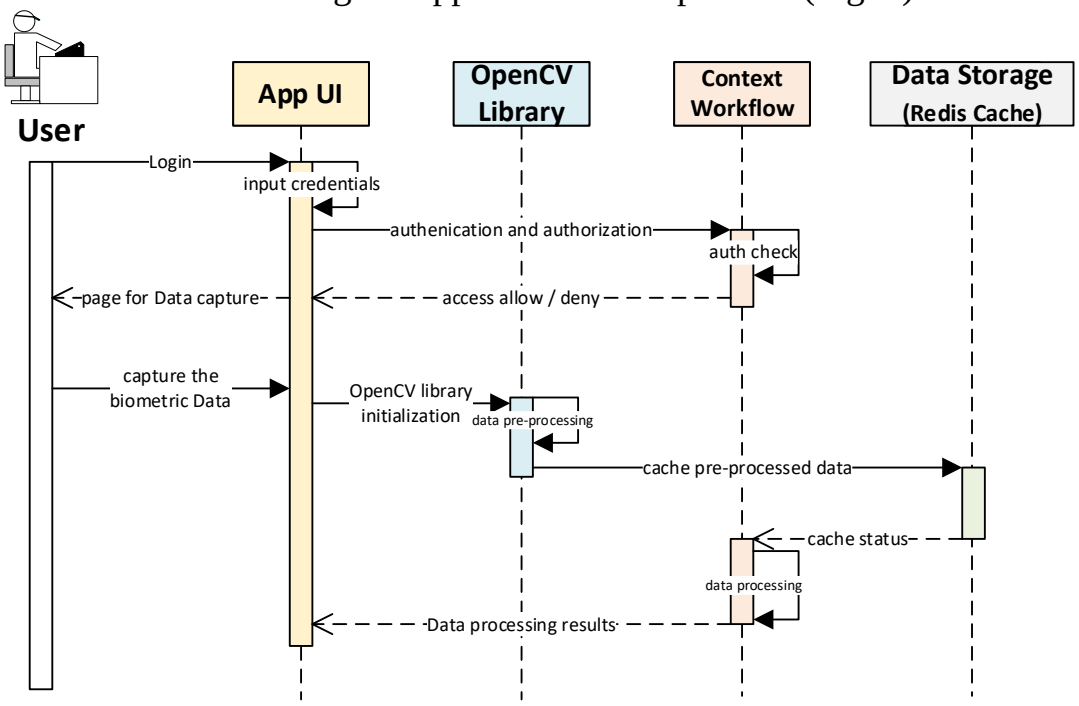
that the main algorithms for solving problems with biometric data are AdaBoost and RealBoost. Additionally, the authors proposed using HaarCascade and LBPCascade to implement the algorithms described above. Kumar K., Kasivisvandaham I., Priyanka P., Bharkav V. [6] in their work, rather briefly and meaningfully, described the algorithm for processing biometric data using multi-cascade neural networks (MTCNN). According to the authors, the use of multi-cascade models allows for achieving classification accuracy of biometric data (e.g., facial images) sufficiently high [6]. A team of authors, consisting of Kumar G., Venu K., Srinevasi R., and Sai A. [7], attempted to develop a face recognition model using the Haar Cascade Classifier, based on the open-source OpenCV (literally, Open Computer Vision Library) [9]. The modeling the scope of functional requirements is creating a cross-functional diagram. In our case, a sample of such a diagram was developed for a business user who will verify their data. The diagram was created in Microsoft Visio (Fig. 1). It depicts three main entities: the user, the system, external libraries, and providers.



Pic. 1. Workflow of Biometric verification for the App on microservices architecture based on cloud-centric design

The user must start the flow by opening a link to the Application. Then he must enter his login and password, and after successful authorization, he can enter his personal data and verify it.

A sequence diagram was constructed to provide a high-level representation of the integration interactions among the application's components (Fig. 2).



Pic. 2. Sequence diagram for Biometric Data processing App

For simplicity, we have only built a basic Positive flow (Happy path). However, during the application development process, it is worth considering possible alternative scenarios - incorrect data was entered, an error was received from an application component, an error was received from the provider, the connection was lost, etc

Conclusions

It was shown that biometric verification is a complex multi-level process that combines requirements for accuracy, scalability, and economic feasibility. Modern image processing methods were analyzed, in particular, deep learning models and classical filtering and classification algorithms. The feasibility of using the Gabor filter to extract key features of biometric images was substantiated. Using standard, non-customized libraries is suitable for solutions that do not require very high data processing accuracy. Otherwise, in our opinion, it is better to use customized models that require prior training. Any solution that includes customized models, in addition to the software components (Run Time), must include a well-defined structure and logic for deploying the solution (Build Time). At the same time, the deployment environment must contain the appropriate components for building a machine learning model with subsequent testing and deployment of these models in the production environment (Production Environment). In our opinion, such an approach to solving the problem may not always be optimal from the perspective of software

architectural design. The fact is that deep learning models, particularly multi-cascade models, require an iterative training process (the number of iterations can be significant and depends on the quality of the training data). This requires significant computing resources, leading to solutions that may conflict with stakeholders' economic interests. For example, stakeholders may need a simple application for image classification that does not require complex machine learning models. And the formation of solutions with complex models increases the costs of both software development and support.

REFERENCES

1. Gaiduchok M. A., Chernyak O. I. (2018). Development of a software module for visualization of filtering and spectral analysis of biometric network data. Youth in science: research, problems, prospects (MN-2018), January 2-June 6, 2018: collection of materials. Vinnytsia: VNTU, URL: https://conferences.vntu.edu.ua/index.php/mn/mn2018/paper/viewFile/3575./3033
2. Nazarkevych M. A. Development of biometric identification methods based on Ateb-Gabor filtering. Ukrainian Journal of Information Technologies. 2021. No. 3. P. 106-113. URL: https://www.researchgate.net/publication/352714792_ROZROBLENNA_BIOMETRICNIH_METODIV_IDENTIFIKACII_NA_PIDSTAVI_FILTRACII_ATEB-GABOROM
3. On approval of the Regulation on the national system of biometric verification and identification of citizens of Ukraine, foreigners and stateless persons: Resolution of the Cabinet of Ministers of Ukraine; Regulation dated 27.12.2017 No. 1073. URL: https://zakon.rada.gov.ua/laws/show/1073-2017-%D0%BF#Text
4. Tymoshin Yu. A., Orlenko S. P. (2018). An algorithm for recognizing people's faces based on a convolutional neural network. Adaptive automatic control systems. № 1. P. 166-173.
5. Dwijayanti, Suci & Ramadhan, Muhammad & Yudho, Bhakti (2023). Facial recognition and body temperature measurements based on thermal images using a deep-learning algorithm. IAES International Journal of Artificial Intelligence (IJ-AI). Volume 12. DOI: 10.11591/ijai.v12.i4.pp1654-1665.
6. Kranthi Kumar K., Kasiviswanadham Y., Priyanka P., Bhargavi V. Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN). Science Direct. 2023. Volume 80, Part 3. pp. 2406-2410. URL: https://www.sciencedirect.com/science/article/abs/pii/S2214785321047672
7. Kumar, Meriga G, Venu K, Kishore Bolla, Sreenivasulu Ram, Sai Ramakrishna, Aravinda (2024). A Hybrid Model for Face Detection Using HAAR Cascade Classifier and Single Shot Multi-Box Detectors Based on Open CV. International Research Journal of Multidisciplinary Scope. Volume 5, pp. 650-661. DOI: 10.47857/irjms.2024.v05i01.0304
8. Najibi Alex (2020). Racial Discrimination in Face Recognition Technology. Blog, science policy, special edition: science policy and social justice. Volume 10. URL: https://sciencepolicy.hsites.harvard.edu/blog/racial-discrimination-face-recognition-technology
9. OpenCV library portal. URL: https://opencv.org/
10. Remone, Roweida & Dash, Sushree (2023). Face Recognition and Face Detection Benefits and Challenges Section A-Research paper 2561 Eur. European Chemical Bulletin. Volume 12. pp. 2561-2566. DOI: 10.31838/ecb/2023.12.si6.226
11. Wang Sai (2021). The Application of Face Recognition System. Advances in Social Science, Education and Humanities Research. Volume 631. pp. 242-247. DOI: 10.2991/assehr.k.220105.04

SCIENTIFIC FOUNDATIONS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN OCCUPATIONAL HEALTH AND SAFETY BASED ON THE LEGISLATIVE FRAMEWORK OF UKRAINE

Mykhailo PRYGARA (Candidate of Technical Sciences, Associate Professor)[1]
Olena VYSOTSKA (Candidate of Technical Sciences, Associate Professor)[2]
Anatolii DAVYDENKO (Doctor of Technical Sciences, Professor, Leader Researcher)[3]

[1]*Uzhhorod National University, Uzhhorod, Ukraine, Department of Machine Industry Technology, mykhailo.prygara@uzhnu.edu.ua*
[2]*State University "Kyiv Aviation Institute", Kyiv, Ukraine, Department of Cybersecurity, Lek_Vys@ukr.net*
[3]*G.E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine, Kyiv, Ukraine, Department of Mathematical and Econometric Modeling, davidenkoan@gmail.com*

Abstract
The article examines the scientific foundations and practical aspects of implementing artificial intelligence (AI) in the field of occupational safety (OS) in Ukraine in the context of digitalization for 2024–2026. The author identifies and analyzes four key areas of technology development: computer vision for monitoring personal protective equipment, predictive risk analytics, intelligent wearable devices (exoskeletons, fatigue sensors), and the automation of administrative processes through VR/AR training. Based on a comparative analysis, the study demonstrates the advantages of an AI-oriented approach over the classical one, particularly through the shift from a reactive to a predictive management model, which allows incidents to be forecasted 24–48 hours in advance with 85–90% accuracy.

Keywords
Artificial intelligence, occupational safety, predictive analytics, computer vision, industrial safety, digitalization, wearable devices.

Introduction
The implementation of Artificial Intelligence (AI) has experienced rapid growth across numerous industries. By 2026, AI has transitioned from a futuristic concept to a fundamental tool in the field of Occupational Health and Safety (OHS). Today, over 90% of the world's large industrial companies utilize AI to automate safety protocols and reduce the frequency of incidents.
Strategic and Legislative Vector (2025–2026) Ukraine is actively integrating AI into public administration and industry, which is enshrined at the regulatory level: State AI Development Strategy until 2030: Identifies labor safety as one of the priority areas to minimize the human factor in hazardous industries; Digitalization through the 'Obriy' system: In 2025–2026, the government launched a large-scale digitalization of labor relations (CMU Resolution on the pilot project 'Obriy'). This creates a 'digital foundation' — data arrays on qualifications, training, and health

status, which AI can analyze in real time; Harmonization with the EU AI Act: Since AI systems in labor protection are classified as high-risk systems, the relevance lies in creating transparent and ethical algorithms that comply with EU requirements.
The traditional occupational safety system in Ukraine has operated for years on the principle of analyzing accidents that have already occurred. AI fundamentally changes this approach: Risk prediction: Instead of recording injuries, AI analyzes 'near misses' and behavioral factors, warning of danger before it occurs; Big Data processing: Modern enterprises generate thousands of signals from sensors, cameras, and logs. Humans are unable to process such a volume of data, whereas AI identifies hidden correlations (for example, the connection between shift time, workshop temperature, and the increase in minor injuries).
The relevance of AI in Ukraine today has a unique context: Remote control and monitoring: At critical infrastructure sites that are under threat of shelling or in de-occupied territories, AI allows minimizing human presence in dangerous areas through the use of robotics and drones with AI analytics; Staff shortage: Due to migration processes and mobilization, many new employees are working in enterprises. AI assistants help with training and monitor the safety of newcomers, automatically guiding them on the correctness of their actions.
The use of AI in occupational safety is not only about humanitarian benefits but also about profitability: Reducing payouts: According to statistics from 2024-2025, company expenses on compensation, fines, and accident investigations remain high. Implementing AI reduces these costs by 20-30% within the first two years; Electronic document management (EDM): Order of the Ministry of Economy No. 839-21 allowed the transition to EDM in occupational safety. AI automates the verification of these documents, eliminating a formal approach ('signing for the sake of signing').
The purpose of the research is a scientific rationale and the development of a conceptual model for integrating artificial intelligence (AI) systems into the field of occupational safety (OS) in Ukraine. The research is aimed at transforming the safety management system from reactive to predictive (proactive) based on the analysis of modern technological solutions and the adaptation of domestic legislation to EU standards (EU AI Act).

Research results

There are four primary directions in OHS where AI is currently most active:
The first direction is computer vision technologies Computer Vision. This technology is based on the use of AI-equipped surveillance cameras that analyze video streams in real-time to:

– Monitor PPE: The system automatically records instances where a worker enters a danger zone without a helmet, vest, or goggles.

– Detect Dangerous Behavior: AI recognizes falls, physical altercations, or the presence of personnel in the operating zones of cranes and loaders.

– Monitor Access Zones: It warns of unauthorized or unidentified persons entering critical areas.

The second direction is predictive analytics (risk forecasting). Instead of reacting to an accident that has already occurred, AI analyzes large datasets (incident history, weather conditions, equipment status) to provide forecasts:

– Injury Prediction: The system can indicate a high risk of injury in a specific area during the next shift due to personnel fatigue or technical malfunctions.

– Smart Maintenance: AI notifies of the need for equipment repair before it becomes hazardous to the operator.

The third direction is smart devices and wearables. Workers utilize wearable devices that monitor physical conditions:

– Fatigue Sensors: These measure pulse and micro-movements to warn drivers or operators of the risk of falling asleep or overexertion.

– AI Exoskeletons: These assist in correctly distributing loads on the back and legs, preventing occupational diseases.

– Gas and Noise Detectors: Smart sensors immediately transmit data to a central console if toxic substance levels exceed safety norms.

The fourth direction is the automation of paperwork. AI has significantly simplified the administrative workload for OHS specialists:

– Voice Reporting: An inspector can dictate a violation report into a smartphone, which AI instantly converts into a structured document, attaches photos, and assigns responsible parties for remediation.

– Training (VR/AR): AI-based virtual reality simulators create accident scenarios where workers can practice skills without real-life risks.

Let's compare classical approaches to occupational safety with the use of AI based on four parameters. Reaction: Classical - reactive (after an event), manual (tables, papers); AI - proactive (prevention); Inspections: Classical - selective (inspector raids), AI - continuous (24/7 monitoring); Data analysis: Classical - manual (tables, papers), AI - instant (Big Data); Human factor: Classical - high risk of error, AI - minimizes errors due to fatigue.

The use of AI in OHS is currently undergoing a stage of deep scientific validation. Research from 2024–2026 focuses not only on the "possibility" of technology application but also on its specific quantifiable efficiency.

We will provide an overview of key scientific directions and references to current works:

1. Predictive Analytics: According to recent reports (e.g., ILO 2025 [1]), machine learning systems have achieved 85–90% accuracy in predicting dangerous industrial situations. Studies show that analyzing "weak signals" (minor violations) allows for the prevention of major accidents 24–48 hours before they occur.

2. Computer Vision: Modern Deep Learning algorithms are now capable of not only seeing a helmet but also determining if it is correctly fastened or if gloves meet the specific requirements for handling certain chemicals.

3. Biometric Sensors: A 2025 study (MDPI [2]) confirms that using "smart" exoskeletons and posture sensors reduces dangerous movements by 84%, which is critical for preventing musculoskeletal disorders.

Despite high efficiency (incident reduction by 25–60%), scientists emphasize that AI should be a supplement to, rather than a replacement for, human oversight to avoid "digital stress" among employees.

As of early 2026, Ukraine's legislation regarding Artificial Intelligence is in a state of active "Euro-integration transformation." While there is no standalone law titled "On AI in Occupational Health and Safety," the field is regulated by a complex of regulatory acts adapting to EU AI Act standards (EU Regulation 2024/1689).

Here's how it looks in practice:

1. Harmonization with the EU AI Act Ukraine is officially implementing the provisions of European AI legislation. According to these provisions, AI systems used in workplaces (including for monitoring health and safety) are classified as High-Risk AI Systems.
2. Law of Ukraine "On Labor Protection" The main law (in particular Article 13) places the obligation on the employer to implement "modern technical means and scientific developments" to prevent injuries.
3. Digitalization and State Labor (2025–2026) In January 2026, Cabinet of Ministers Resolution No. 41 came into effect, launching the 'Obriy' system for electronic personnel record management.
4. Personal Data Protection This is the main 'stumbling block.' The use of AI video analytics (facial recognition, biometrics) falls under the Law of Ukraine 'On Personal Data Protection'.

Conclusions

In summary, the use of AI in OHS depends heavily on the specific industry and remains a non-trivial, highly relevant scientific task. In this work, the following was done: Classify the key areas of AI usage (Computer Vision, predictive analytics, IoT, automation) and assess their technical efficiency; Analyze the scientific reliability of predictive models and biometric sensors in the context of reducing industrial injuries; Determine the compliance of innovative safety monitoring tools with current Ukrainian legislation and personal data protection requirements. Compare the effectiveness of traditional control methods with AI-oriented approaches based on reaction speed, continuity, and human factor influence. The relevance of AI in occupational safety in Ukraine today is a challenge of our time. It is the only way to ensure European-level safety amid high risks, limited human resources, and the need for rapid industrial recovery.

REFERENCES

1. Global report revolutionizing health and safety: The role of AI and digitalization at work. 2025. https://www.ilo.org/sites/default/files/2025-04/ILO_Safeday25_Report_EN_r8%2B%281%29.pdf_r8+(1).pdf.

2. Naranjo J.E., Mora C.A., Bustamante Villagómez D.F., Mancheno Falconi M.G., Garcia M.V.: Wearable Sensors in Industrial Ergonomics: Enhancing Safety and Productivity in Industry 4.0. *Sensors*, 2025, 25, 1526. https://doi.org/10.3390/s25051526.

АНАЛІТИКА ТА A/B ТЕСТУВАННЯ У ВИСОКОНАВАНТАЖЕНИХ ПЛАТФОРМАХ

Вікторія ТРОФИМЧУК (Магістр, IT бізнес аналітик)[1]

[1]*Apomedical LTD*
[1]*trofymchukviktoria@gmail.com*

Анотація

У роботі представлено дослідження багатокритеріальної оптимізації хмарних обчислювальних систем у режимі реального часу. Запропонований підхід ґрунтується на побудові адаптивної функції витрат, що враховує латентність, споживання обчислювальних ресурсів та пропускну здатність мережі. У межах дослідження застосовано гібридну модель Lagrange–Pareto, яка поєднує метод множників Лагранжа з принципами Парето-оптимальності для пошуку компромісних рішень.

Ключові слова: хмарні обчислення, багатокритеріальна оптимізація, адаптивна функція витрат.

Abstract

This paper presents a study of multi-criteria optimization of cloud computing systems operating in real time. The proposed approach is based on the construction of an adaptive cost function that accounts for latency, computational resource consumption, and network throughput. Within the scope of the study, a hybrid Lagrange–Pareto model is applied, combining the classical Lagrange multiplier method with the principles of Pareto optimality to identify compromise solutions.

Keywords:

Cloud computing, multi-criteria optimization, adaptive cost function.

Вступ

Хмарні обчислювальні системи стали основою сучасних цифрових сервісів, починаючи від потокового відео та онлайн-платежів і завершуючи корпоративними інформаційними платформами. Зростання кількості користувачів, збільшення обсягів даних і вимоги до роботи в режимі реального часу призводять до того, що навантаження на хмарні середовища стає нерівномірним і важко прогнозованим. У таких умовах традиційні методи управління ресурсами, які базуються на фіксованих правилах або локальній оптимізації, не завжди забезпечують стабільну якість сервісу [1].

Особливу складність становить необхідність одночасного врахування кількох критеріїв ефективності: мінімізації затримки, оптимального використання обчислювальних ресурсів та підтримання достатньої пропускної здатності мережі. Оптимізація лише одного з цих параметрів часто призводить до погіршення інших, що робить задачу управління хмарною інфраструктурою багатокритеріальною за своєю природою. Тому виникає потреба у підходах, які

дозволяють знаходити компромісні рішення, адаптовані до реальних умов експлуатації [2].
У даній роботі запропоновано метод багатокритеріальної оптимізації хмарних обчислювальних систем, який поєднує математичне моделювання та гібридний підхід Lagrange–Pareto. Запропонована модель орієнтована на роботу в квазіреальному часі та дозволяє адаптувати розподіл ресурсів залежно від типу навантаження і пріоритетів сервісу, що робить її придатною для використання у високонавантажених хмарних платформах.
Метою дослідження є розробка методу багатокритеріальної оптимізації хмарних обчислювальних систем у режимі реального часу.

Результати дослідження
У межах дослідження запропоновано математичну модель оптимізації хмарної обчислювальної системи, яка дозволяє оцінювати її стан у режимі реального часу з урахуванням ключових показників продуктивності. На відміну від традиційних підходів, де оптимізація виконується за одним параметром [3,4], у даній роботі система розглядається як багатокритеріальний об'єкт, у якому затримка, використання ресурсів та пропускна здатність мережі взаємопов'язані між собою.
Для формалізації задачі введено узагальнену функцію витрат $C(t)$, яка дозволяє описати поточний стан системи одним інтегральним показником:

$$C(t) = \alpha L(t) + \beta R(t) + \gamma \frac{1}{\beta(t)} \quad (1)$$

де *L(t)* — затримка обробки запитів,
R(t) — використання обчислювальних ресурсів,
B(t) — пропускна здатність мережі,
α, β, γ — вагові коефіцієнти, що визначають пріоритети оптимізації.

Використання вагових коефіцієнтів дозволяє адаптувати модель до різних сценаріїв роботи хмарної платформи. Наприклад, для відеострімінгових сервісів критичною є мінімізація затримки, тоді як для аналітичних або фінансових систем важливішим є контроль використання ресурсів. Таким чином, зміна значень *α, β, γ* не потребує зміни структури моделі, а лише коригує її поведінку відповідно до вимог сервісу. Оптимізація функції витрат виконується з урахуванням системних обмежень на допустимі значення параметрів:

$$L(t) \leq L_{max}, R(t) \leq R_{max}, B(t) \geq B_{min} \quad (2)$$

Для пошуку оптимального рішення використано гібридний метод Lagrange–Pareto [5,6], який поєднує метод множників Лагранжа з принципами Парето-оптимальності. Такий підхід дозволяє сформувати множину допустимих рішень, серед яких можна обрати найбільш збалансоване залежно від поточного типу навантаження.

Аналіз чутливості моделі

Для оцінки впливу вагових коефіцієнтів на поведінку системи проведено аналіз чутливості функції витрат до зміни параметра α, що відповідає за затримку. Результати цього аналізу наведено на рис. 1.

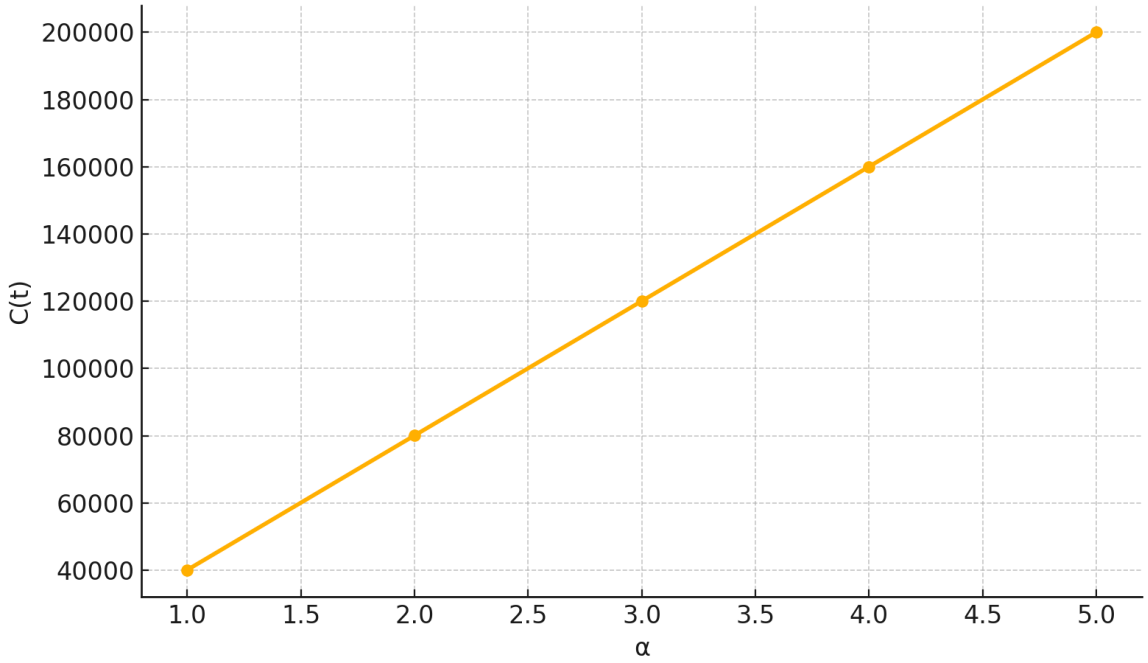


Рис. 1. Залежність функції витрат *C* від вагового коефіцієнта *α* при фіксованих значеннях *β= 1*та *γ=3*

З рисунка видно, що зі збільшенням значення α функція витрат зростає майже лінійно, що підтверджує чутливість моделі до пріоритетів оптимізації. Це означає, що підвищення ваги латентності змінює поведінку системи у бік мінімізації затримки, навіть якщо це призводить до менш ефективного використання ресурсів або зниження пропускної здатності.

Таким чином, запропонована модель дозволяє гнучко керувати балансом між продуктивністю та витратами, що є критично важливим для високонавантажених хмарних платформ з різними типами сервісів.

Висновки

У роботі було досліджено задачу багатокритеріальної оптимізації хмарних обчислювальних систем у режимі реального часу та запропоновано підхід на

основі гібридної моделі Lagrange–Pareto. Розроблена математична модель дозволяє одночасно враховувати затримку обробки запитів, використання обчислювальних ресурсів та пропускну здатність мережі, що є критичним для високонавантажених платформ.

Результати чисельного моделювання показали, що запропонований метод забезпечує більш ефективне використання ресурсів і зниження затримки порівняно з традиційними підходами, особливо в умовах імпульсного навантаження. Проведений аналіз чутливості підтвердив можливість гнучкого налаштування моделі відповідно до вимог конкретного сервісу.

Незважаючи на отримані позитивні результати, подальші дослідження можуть бути спрямовані на розширення моделі з урахуванням додаткових параметрів та її апробацію в реальних хмарних середовищах.

REFERENCES

1. Buyya R., Calheiros R. N., Dastjerdi A. V. Cloud Computing: Principles and Paradigms. New York: Wiley, 2011. 637 p.
2. Zhang Q., Chen M., Li L. Dynamic resource allocation for cloud computing using multi-objective optimization. IEEE Transactions on Cloud Computing. 2020. Vol. 8, No. 2. P. 345–357. doi:10.1109/TCC.2018.2871849
3. Deb K. Multi-Objective Optimization Using Evolutionary Algorithms. Chichester: Wiley, 2001. 518 p.
4. Miettinen K. Nonlinear Multiobjective Optimization. Boston: Springer, 1999. 298 p.
5. Bertsekas D. P. Nonlinear Programming. 3rd ed. Belmont: Athena Scientific, 2016. 843 p.
6. Mao M., Humphrey M. A performance study on the VM startup time in the cloud. Proceedings of the IEEE International Conference on Cloud Computing. 2019. P. 423–430.

TEMPORAL INTERPRETATION OF QUANTUM DECOHERENCE IN INFORMATION SYSTEMS

Andriy LEMESHKO (PhD, Associate Professor)[1]
Yurii KOZUB (D.Sc., Professor)[2]

[1]*State University of Trade and Economics, Faculty of Information Technology, Department of Software Engineering and Cybersecurity, e-mail: a.lemeshko@knute.edu.ua*
[2]*Luhansk Taras Shevchenko University, Lubny, Ukraine e-mail: kosub.yg@gmail.com*

Abstract

This paper proposes a temporal interpretation of quantum decoherence, in which the loss of coherence is treated as a consequence of disrupted temporal synchronization rather than as an intrinsic stochastic process. Within this framework, phase coherence corresponds to a state of global temporal alignment, whereas decoherence emerges from local temporal fluctuations and correlations. It is shown that the proposed interpretation is formally consistent with the density matrix formalism and standard models of phase damping. Furthermore, non-Markovian effects, slow drift, and 1/f noise are interpreted as manifestations of temporally correlated dynamics. The presented approach provides a unified conceptual basis for analyzing decoherence, noise, and memory effects in quantum and information systems, without modifying the standard quantum mechanical formalism.

Keywords

Quantum decoherence; temporal interpretation; phase synchronization; non-Markovian dynamics; 1/f noise; information systems.

Introduction

Quantum decoherence represents one of the fundamental limitations in the development of quantum technologies and high-precision information systems. It determines the time scales over which quantum superposition and phase coherence can be preserved, thereby constraining quantum computation, communication, sensing, and synchronization. Beyond strictly quantum platforms, decoherence-like phenomena also manifest in complex information systems, where phase instability, correlated noise, and memory effects limit performance and reliability.

In standard quantum theory, decoherence is described within the framework of open quantum systems [1-5]. The interaction between a system and its environment leads to the suppression of off-diagonal elements of the density matrix, effectively destroying interference effects. This description has proven highly successful from an operational perspective and is widely employed in both theoretical and experimental studies. However, the parameters governing decoherence rates are typically introduced phenomenologically and depend on simplified assumptions about the environment.

A particularly challenging aspect arises in systems exhibiting non-Markovian behavior, where memory effects, temporal correlations, and slow fluctuations dominate the dynamics [6]. Such regimes are common in solid-state quantum devices, distributed information architectures, and systems affected by low-frequency

noise. While advanced mathematical tools exist to describe these effects, their physical interpretation often remains fragmented and system-specific.
This work is motivated by the need for a coherent interpretative framework that can account for decoherence, noise, and memory effects in a unified manner. Instead of attributing decoherence solely to environmental randomness, we explore an alternative viewpoint in which temporal structure and synchronization play a central role. The proposed temporal interpretation does not introduce new dynamical laws but offers a physically meaningful perspective on the origin of phase instability in quantum and information systems.
The purpose of the research is to develop and present a temporal interpretation of quantum decoherence, in which phase damping is understood as a consequence of disrupted temporal synchronization. The objective is to demonstrate that this interpretation is formally consistent with standard quantum mechanical descriptions while providing additional insight into non-Markovian effects, correlated noise, and stability issues in complex information systems.

Research results

In the conventional framework of quantum mechanics, decoherence is described using the density matrix formalism [7]. For an isolated system, the evolution of the density matrix is unitary and governed by the von Neumann equation, ensuring the preservation of quantum coherence. In realistic conditions, however, quantum systems are inevitably coupled to external degrees of freedom, which leads to the necessity of describing them as open systems.
Within this formalism, decoherence manifests as the suppression of off-diagonal elements of the density matrix in a particular basis. This process, often referred to as phase damping, results in the gradual disappearance of interference effects while leaving the diagonal elements—associated with classical probabilities—largely unaffected. Such behavior provides an effective explanation for the emergence of classical-like properties without invoking an explicit collapse of the wave function.
A widely used approach to modelling decoherence is based on Markovian master equations, particularly those of the Lindblad type [8]. These equations assume that environmental correlations decay rapidly compared to the characteristic time scales of the system, leading to memoryless dynamics. Under this assumption, decoherence rates are described by phenomenological coefficients that characterize the strength of system–environment coupling.
Despite their practical success, Markovian models encounter limitations when applied to systems exhibiting long-lived correlations, slow fluctuations, or structured environments. In such cases, non-Markovian dynamics become relevant, giving rise to memory effects, information backflow, and non-exponential decoherence behavior [9-11]. Although various generalizations of master equations have been developed to capture these effects, the physical origin of the corresponding parameters often remains unclear and strongly model-dependent.
The phase of a quantum state is highly sensitive to temporal conditions. Under ideal, homogeneous circumstances, phase evolution remains synchronized across all

components of the system, ensuring the preservation of coherence. In realistic settings, however, effective temporal conditions may differ locally, leading to the accumulation of phase mismatches.

Within the temporal interpretation, such local temporal deviations give rise to phase offsets that evolve differently for different components of the quantum state. When these deviations are slow or weakly fluctuating, they may not immediately destroy coherence but instead introduce correlated phase noise. Over longer time scales, the accumulation of these mismatches leads to an effective suppression of interference terms.

Importantly, this mechanism does not require the introduction of intrinsic randomness at the fundamental level. Instead, decoherence emerges as a consequence of averaging over unresolved or uncontrollable temporal variations. When described in terms of the reduced density matrix, this averaging reproduces the familiar exponential decay of off-diagonal elements associated with phase damping.

Within the proposed framework, quantum coherence corresponds to a state of global phase synchronization. As long as temporal conditions remain sufficiently uniform, phase relations are preserved, and coherent dynamics can be sustained. Decoherence arises when this synchronization is disrupted beyond a critical level, rendering phase relations incompatible in a global description.

This interpretation naturally accommodates both Markovian and non-Markovian regimes. In Markovian scenarios, temporal deviations fluctuate rapidly and independently, leading to memoryless phase damping. In contrast, non-Markovian behavior emerges when temporal fluctuations are correlated over extended time intervals, allowing partial restoration of coherence or non-monotonic decay patterns.

By framing decoherence as a synchronization problem, the temporal interpretation provides a unifying conceptual picture that links phase stability, temporal correlations, and memory effects within a single explanatory scheme.

The temporal interpretation of decoherence has direct implications for the analysis of noise and stability in information systems. In many practical platforms, noise processes are not independent in time but exhibit long-range correlations and slow drift. Such behavior is characteristic of low-frequency noise, including 1/f noise, which plays a dominant role in limiting system performance.

From a temporal perspective, 1/f noise can be interpreted as a manifestation of slow temporal drift affecting phase evolution over extended periods. These slow variations lead to correlated errors that cannot be adequately described by simple Markovian models. Instead, they reflect shared temporal conditions influencing multiple system components simultaneously.

Temporally correlated errors pose a significant challenge for error mitigation and correction strategies, as they violate assumptions of independence commonly used in information processing. The temporal interpretation highlights the importance of considering global temporal structure when analyzing system stability, particularly in distributed architectures and synchronization-sensitive applications.

Conclusions

This work has presented a temporal interpretation of quantum decoherence, in which phase damping is understood as a consequence of disrupted temporal synchronization rather than as an intrinsic stochastic process. Within this framework, quantum coherence corresponds to a state of global phase alignment, while decoherence emerges from local temporal fluctuations and correlations. It has been shown that this interpretation is fully consistent with the standard density matrix formalism and reproduces the familiar features of phase damping without modifying the quantum mechanical equations of motion.

The proposed approach provides a natural explanation for non-Markovian effects, memory phenomena, and low-frequency noise as manifestations of temporally correlated dynamics. In the context of information systems, this perspective highlights the role of shared temporal conditions in the emergence of correlated errors and long-term instability. Overall, the temporal interpretation offers a unified conceptual basis for analyzing decoherence, noise, and memory effects in quantum and complex information systems, complementing existing phenomenological models and contributing to a deeper understanding of phase stability in realistic environments.

REFERENCES

1. ZEH H. D.: On the interpretation of measurement in quantum theory. Foundations of Physics, 1(1970), 69–76.
2. ZUREK W. H.: Decoherence and the transition from quantum to classical. Physics Today, 44(1991)10, 36–44.
3. ZUREK W. H.: Decoherence, einselection, and the quantum origins of the classical. Reviews of Modern Physics, 75(2003), 715–775.
4. SCHLOSSHAUER M.: Decoherence, the measurement problem, and interpretations of quantum mechanics. Reviews of Modern Physics, 76(2005), 1267–1305.
5. SCHLOSSHAUER M.: Decoherence and the Quantum-to-Classical Transition. Springer, Berlin 2007.
6. RIVAS Á., HUELGA S. F., PLENIO M. B.: Quantum non-Markovianity: characterization, quantification and detection. Reports on Progress in Physics, 77(2014), 094001.
7. BREUER H.-P., PETRUCCIONE F.: The Theory of Open Quantum Systems. Oxford University Press, Oxford 2002.
8. LINDBLAD G.: On the generators of quantum dynamical semigroups. Communications in Mathematical Physics, 48(1976), 119–130.
9. GORINI V., KOSSAKOWSKI A., SUDARSHAN E. C. G.: Completely positive dynamical semigroups of N-level systems. Journal of Mathematical Physics, 17(1976), 821–825.
10. RIVAS Á., HUELGA S. F., PLENIO M. B.: Quantum non-Markovianity: characterization, quantification and detection. Reports on Progress in Physics, 77(2014), 094001.
11. PRESKILL J.: Quantum computing in the NISQ era and beyond. Quantum, 2(2018), 79.

ФОРМАЛІЗАЦІЯ ПРОЦЕСУ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ТЕОРЕТИКО-МНОЖИННОГО ПІДХОДУ

Юлія ХОХЛАЧОВА (к.т.н., професор)

Державний торговельно-економічний університет, Київ, Україна
Y.Khokhlachova@knute.edu.ua

Анотація

У роботі представлено теоретико-множинну модель для формалізації процесу оцінювання кіберстійкості об'єктів критичної інфраструктури. Запропонована модель структурує ієрархію цілей, задач, підзадач та базових заходів кіберстійкості через введення множини ідентифікаторів та функцій реалізації. Розроблено систему однозначної індексації множини базових заходів у межах фреймворка MITRE CREF. Продемонстровано практичне застосування моделі на прикладах DDoS-атаки та фішингу для банківських систем.

Ключові слова

кіберстійкість, критична інфраструктура, теоретико-множинна модель, MITRE CREF, оцінювання безпеки, кіберзагрози.

FORMALIZATION OF THE CYBER RESILIENCE ASSESSMENT PROCESS OF CRITICAL INFRASTRUCTURE BASED ON A SET THEORETICAL APPROACH

Abstract

The paper presents a set-theoretic model for formalizing the process of assessing the cyber resilience of critical infrastructure facilities. The proposed model structures the hierarchy of goals, tasks, subtasks, and basic measures of cyber resilience through the introduction of a set of identifiers and implementation functions. A system for unambiguous indexing of the set of basic measures within the MITRE CREF framework has been developed. The practical application of the model is demonstrated on examples of DDoS attacks and phishing for banking systems.

Keywords

cyber resilience, critical infrastructure, set-theoretic model, MITRE CREF, security assessment, cyber threats.

Вступ

Об'єкти критичної інфраструктури (ОКІ) – енергетичні системи, транспортні мережі, фінансові установи, системи охорони здоров'я – залишаються далі більш залежними від цифрових технологій, що робить їх привабливими цілями для кіберзлочинців, активістів та державних гравців. Традиційна парадигма кібербезпеки, що обґрунтовується на принципі

"запобігання та виявлення", виявляється недостатньою в умовах, коли припущення про неминучість успішної компрометації стає реалістичним.
Концепція кіберстійкості (cyber resilience) забезпечує здатність системи не тільки протистояти атакам, але й підтримувати критичні функції під час інциденту, швидко відновлюватися та адаптуватися до нових загроз. Cyber Resiliency Engineering Framework (CREF), розроблений корпорацією MITRE, пропонує комплексний підхід до забезпечення кіберстійкості через структурування цілей, завдань та конкретних технічних дій [1]. Проте практичне застосування CREF ускладнюється відсутністю формалізованих математичних моделей для ефективного оцінювання рівня кіберстійкості.
Використання теоретико-множинного підходу надає можливість створення потужного інструментарію для формалізації складних ієрархічних структур та створення математичних основ для розробки алгоритмів оцінювання.
Аналіз сучасних досліджень критичної прогалини у формалізації процесів оцінювання кіберстійкості:

- *Неструктурованість представлення знань* ускладнює планування захисних заходів та прийняття обґрунтованих рішень;
- *Відсутність кількісних метрик* неможливе об'єктивне оцінювання поточного рівня кіберстійкості;
- *Відсутність формалізованого зв'язку* між типами кіберзагроз та необхідними базовими заходами;
- *Динамічний характер ландшафту* загрожує постійної адаптації стратегій без чіткого математичного апарату.

Метою дослідження є розробка теоретико-множинної моделі даних для формалізації та оцінювання кіберстійкості ОКІ.

Результати дослідження

Формалізація ієрархічної структури

Для побудови необхідної моделі даних використаємо теоретико-множинний підхід. Для цього введемо множину ідентифікаторів цілей, що дозволять забезпечити кіберстійкість ОКІ:

$$\boldsymbol{GS} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{GS}_i \right\} = \left\{ \boldsymbol{GS}_1, \boldsymbol{GS}_2, ..., \boldsymbol{GS}_n \right\}, \quad (1)$$

де $i = \overline{1,n}$, а n – кількість цілей.

Наприклад, при n=4 з урахуванням цілей CREF [1] вираз (1) запишемо, як:

$$\boldsymbol{GS} = \left\{ \bigcup_{i=1}^{4} \boldsymbol{GS}_i \right\} = \left\{ \boldsymbol{GS}_1, \boldsymbol{GS}_2, \boldsymbol{GS}_3, \boldsymbol{GS}_4 \right\} = \left\{ \boldsymbol{ANT}, \boldsymbol{WITH}, \boldsymbol{REC}, \boldsymbol{AD} \right\}. \quad (2)$$

Далі введемо множину ідентифікаторів задач ***OS***, які необхідно вирішити для досягнення цілей, ідентифікатори яких визначені в множині ***GS***:

$$\boldsymbol{OS} = \left\{ \bigcup_{i=1}^{m} \boldsymbol{OS}_i \right\} = \left\{ \boldsymbol{OS}_1, \boldsymbol{OS}_2, ..., \boldsymbol{OS}_m \right\}, \quad (3)$$

де $\boldsymbol{OS}_i$ – ідентифікатор *i*-ої задачі ($i=\overline{1,m}$), а m – кількість ідентифікаторів задач.

Наприклад, при *m*=8 з урахуванням [1] формулу (3) представимо, як:

$$\boldsymbol{OS}=\left\{\bigcup_{i=1}^{m}\boldsymbol{OS}_i\right\}=\left\{\boldsymbol{OS}_1,\boldsymbol{OS}_2,...,\boldsymbol{OS}_8\right\}=\left\{\boldsymbol{PA},\boldsymbol{PR},\boldsymbol{CN},\boldsymbol{CS},\boldsymbol{RE},\boldsymbol{UN},\boldsymbol{TR},\boldsymbol{RA}\right\}. \quad (4)$$

Для вирішення задач, визначених їхніми ідентифікаторами в множині $\boldsymbol{OS}_i$ ($i=\overline{1,m}$) (див. (2)) введемо множину ідентифікаторів підзадач $\boldsymbol{OS}_{ij}$, пов'язаних з вирішенням кожної i-ї задачі:

$$\boldsymbol{OS}_i=\left\{\bigcup_{j=1}^{m_i}\boldsymbol{OS}_{ij}\right\}=\left\{\boldsymbol{OS}_{i1},\boldsymbol{OS}_{i2},\boldsymbol{OS}_{i3},...,\boldsymbol{OS}_{im_i}\right\}, \quad (5)$$

де $\boldsymbol{OS}_{ij}$ – ідентифікатор кожної *j*-ої підзадачі ($j=\overline{1,m_i}$) i-ої задачі, а m_i ($i=\overline{1,m}$) – кількість підзадач, необхідних для вирішення i-ої задачі.

З урахуванням (5) вираз (3) запишемо в наступному вигляді:

$$\boldsymbol{OS}=\left\{\bigcup_{i=1}^{m}\left\{\bigcup_{j=1}^{m_i}\boldsymbol{OS}_{ij}\right\}\right\}=\left\{\begin{array}{l}\left\{\boldsymbol{OS}_{11},\boldsymbol{OS}_{12},...,\boldsymbol{OS}_{1m_1}\right\},\\ \left\{\boldsymbol{OS}_{21},\boldsymbol{OS}_{22},...,\boldsymbol{OS}_{2m_2}\right\},...,\\ \left\{\boldsymbol{OS}_{m1},\boldsymbol{OS}_{m2},...,\boldsymbol{OS}_{mm_m}\right\}\end{array}\right\}. \quad (6)$$

Для вирішення підзадач, визначених у множині їх ідентифікаторів $\boldsymbol{OS}_{ij}$ ($i=\overline{1,m}$; $j=\overline{1,m_i}$) (див. (3)) введемо множину функцій $OS_{ijk}(\bigcup_{l=1}^{a_{ijk}}A_{ijkl})$ для реалізації базових заходів кожної m_i-ої підзадачі на основі множини відповідних методів $\bigcup_{l=1}^{a_{ijk}}A_{ijkl}$, тоді:

$$\boldsymbol{OS}_{ij}=\left\{\bigcup_{k=1}^{m_{ij}}\boldsymbol{OS}_{ijk}(\bigcup_{l=1}^{a_{ijk}}A_{ijkl})\right\}=\left\{OS_{ij1}(\bigcup_{l=1}^{a_{ij1}}A_{ij1l}),OS_{ij2}(\bigcup_{l=1}^{a_{ij2}}A_{ij2l}),...,OS_{ijm_{ij}}(\bigcup_{l=1}^{a_{ijm_{ij}}}A_{ijm_{ij}l})\right\}, \quad (7)$$

де OS_{ijk} – функція, що реалізує базові заходи ($k=\overline{1,m_{ij}}$), m_{ij} – кількість базових заходів для вирішення m_i-ої підзадачі, A_{ijkl} ($l=\overline{1,a_{ijk}}$) – *l*-й аргумент, що визначає метод (підхід, технічне рішення тощо) для реалізації базового *k*-го заходу m_i-ої підзадачі, a_{ijk} – кількість можливих аргументів для реалізації базового *k*-го заходу (примітка: у випадку відсутності методу, підходу, універсального технічного рішення тощо, то ця окрема умова означає, що $l=\overline{1,0}$ і, як слідство, функція не має аргументів).

Система індексації

Кожен базовий захід отримує унікальний ідентифікатор виду *Задача.Підзадача.Базові заходи (Методи)*.

Всього формалізовано 114 базових заходів кіберстійкості з прив'язкою до 8 задач та 4 цілей.

Практичне застосування

Приклад 1: DDoS-атака на банківський API

Для цього сценарію обрані базові заходи:

- *CN.S2.A1*(*AM,CA,SI*) – оцінка впливу на місію;
- *CN.S2.A2*(*AR,CA*) – ізоляція атакованих компонентів;
- *RE.S1.A1*(*AM,CA*) – відновлення функціональності;
- *UN.S1.A1*(*AM,CA*) – використання спільної інформації про загрози;
- *UN.S3.A1*(*CA*) – відстеження стану безпеки;
- *TR.S1.A1*(*R,CP*) – виявлення точок відмови.

Приклад 2: Фішингова атака на банк

Обрані базові заходи для цього сценарію відрізняються акцентом на людський фактор:

- *CN.S1.A1*(*AM,CA,SI*) – підтримка критичних функцій;
- *CN.S2.A1*(*AM,CA,SI*) – обмеження впливу компрометації;
- *RE.S1.A2*(*AM,SI*) – виявлення скомпрометованих об'єктів;
- *UN.S1.A1*(*AM,CA*) – аналіз рибальських захворювань;
- *UN.S2.A1*(*CP,CA*) – навчання персоналу;
- *TR.S1.A1*(*R,CP*) – вдосконалення захисту;
- *TR.S2.A2*(*R,CP*) – адаптація навчальної програми.

Висновки

Розроблена теоретико-множинна модель вперше забезпечує:

1. *Повну формалізацію* ієрархічної структури CREF через математичні множини та відношення;
2. *Однозначну ідентифікацію* всієї множини базових заходів кіберстійкості;
3. *Формалізований зв'язок* між типами кіберзагроз та необхідними заходами;
4. *Математичну основу* для переходу від якісних експертних оцінок до кількох методів оцінювання;
5. *Адаптивність* до спеціальних вимог різних типів ОКІ.

Порівняно з існуючими підходами, модель забезпечує високий рівень розробленості за всіма критеріями: формалізація ієрархії, математичні компоненти, система індексації та зв'язок із загрозами.

Додаткові напрямки дослідження включають розробку методу розрахунку інтегральних показників кіберрезильєнтності, створення системи підтримки рішень та автоматизованих інструментів оцінювання для різних типів ОКІ.

REFERENCES

1. Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the

Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report.
2. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160*, Vol. 2 Rev. 1.
3. Linkov, I., Eisenberg, D. A., Plourde, K., et al. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471-476.
4. Kott, A., & Linkov, I. (Eds.). (2019). Cyber Resilience of Systems and Networks. *Springer International Publishing*.
5. Hossain, M. S., Moniruzzaman, M., Muhammad, G., et al. (2014). Big data-driven service composition using parallel clustered particle swarm optimization in mobile environment. *IEEE Transactions on Services Computing*, 9(5), 806-817.
6. Yurii Khlaponin, Mohammed Nuther Ismail Sabah M. Kallow Mohammed Jasim Ridah Mahmood Jawad Abu-Al Shaeer. Quantitative Insights and Challenges in Big Data from a Statistical Perspective/ *Journal of Ecohumanism*, 2024, 3(5), pp. 290–307. DOI:10.62754/joe.v3i5.3907

RESEARCH ON THE CONTROL SYSTEM OF A ROBOTIC PLATFORM FOR DEMINING USING THE WEBSOCKET PROTOCOL

Andriy DUDNIK (Doctor of Sciences, Associate Professor)[1,2]
Dmytro KVASHUK (PhD, Associate Professor)[3,4]

[1]Taras Shevchenko National University, Kyiv, Ukraine
[1]Department of Network and Internet Technologies
[2]Interregional Academy of Personnel Management
[2]Department of Computer Information Systems and Technologies
[3]State University Kyiv Aviation Institute, Kyiv, Ukraine
[3]Department of Electrical Engineering, Energy Management and Mechatronics
[4]Interregional Academy of Personnel Management
[4]Department of Computer Information Systems and Technologies
[1,2]a.s.dudnik@gmail.com, [3,4]dmytro.kvashuk@npp.kai.edu.ua

Abstract

The paper presents a WebSocket-based control approach for a demining robotic platform and proposes enhancements to the Robot Context Protocol (RCP) by replacing JSON text messages with binary frames to reduce overhead and improve control-channel throughput. A real-time control profile is introduced, featuring command prioritization, time-to-live constraints, acknowledgment modes, and stale-message discard/replacement policies. A prototype platform and thin-client web ground station are evaluated using latency, bandwidth, packet loss, reconnect stability, and computational overhead metrics, demonstrating improved control predictability alongside easier integration and scaling.

Keywords

WebSocket, binary messages, JSON, telemetry, real-time control, Robot Context Protocol, demining, robotic platform.

Introduction

Modern robotic platforms are increasingly controlled remotely via web interfaces, as browser-based "thin clients" simplify access, ensure cross-platform compatibility regardless of the operator's OS, and reduce workstation hardware requirements. For real-time exchange of commands and telemetry, WebSocket is frequently chosen as a straightforward mechanism for persistent bidirectional communication. However, porting WebSocket from typical web applications into the online control loop of robotic systems presents a critical limitation. By itself, the protocol does not define sufficient reliability rules for real-time control; it merely provides a messaging channel without establishing semantic or verified frameworks for robotic platform management.

In practice, the reliability of WebSocket-based control diminishes under conditions of unstable network links and variable loads. This leads to increased control signal latency, packet loss or duplication, message queuing, connection drops, and ambiguity regarding command relevance and execution order. Such issues jeopardize the robotic platform's behavioral integrity and make predictable control impossible without additional middleware. Specifically, there are no standardized mechanisms for command prioritization or time constraints (TTL/deadlines), nor are there defined policies for critical operation acknowledgment or backpressure handling.

Nevertheless, given that this networked control technology for robotic systems is in its early stages, its relevance is driven by the transition from isolated control objects to networked robotic systems. In this context, there is a need for an application-layer protocol that retains the simplicity of web technologies while introducing control rules, resource semantics, access control, and mechanisms to enhance management reliability.

Therefore, to improve this control method, it is necessary to enhance the protocol layer responsible for the content and rules of exchange rather than just the "communication channel." This involves augmenting WebSocket with a semantic description of the robot's resources (specifying availability, units, and constraints, as well as permitted commands) and real-time control rules (priorities, command execution timeouts, congestion control, and critical operation confirmation). This approach will ensure more reliable and predictable control, reduce errors caused by incorrect data formats or out-of-bounds commands, simplify the integration of new modules and multi-robot scaling, and enable the web interface to automatically adapt to the specific capabilities of each platform.

The purpose of this article is to experimentally evaluate the efficiency of transitioning from JSON messages to binary frames in a WebSocket control channel for a robotic platform, based on traffic intensity and Round-Trip Time (RTT) metrics, and to substantiate the feasibility of such a transition to enhance responsiveness and optimize bandwidth utilization..

Research results

It is widely adopted as a transport protocol for bidirectional communication between the operator and the robotic platform due to its low overhead and seamless integration

with web technologies and robotics frameworks [1–4]. In most systems, WebSocket is used specifically for control and telemetry, while video data is transmitted via dedicated multimedia protocols due to differing latency and bandwidth requirements [1–6].

Nevertheless, WebSocket only establishes the communication mechanism and does not define the application-level rules essential for reliable online robot control. Existing literature highlights a lack of standardized mechanisms for command prioritization, temporal relevance, critical operation acknowledgement, and congestion control, which complicates integration and increases the risk of error [1–3], [5], [6].

To address these limitations, several approaches have been proposed to formalize robot resources, capabilities, and constraints, alongside self-discovery mechanisms—notably within the Robot Context Protocol and Model Context Protocol [7]. However, many aspects of real-time performance, security, and multi-robot system support remain only partially implemented.

Practical examples range from sophisticated architectures with web-oriented ground control stations [9] to low-cost microcontroller-based solutions [10], though the latter do not mitigate the risks of data loss and latency. Research [11] confirms that migrating to WebSocket significantly reduces latency and traffic but requires further optimization, such as transitioning to binary formats and introducing real-time control profiles with prioritized commands.

Subsequent work focused on optimizing the network control of the robotic platform by enhancing the communication protocol and improving real-time controllability. To achieve this, the performance of the WebSocket channel was investigated in two message transmission modes: text-based (JSON) and binary. A more compact encoding method was selected, and a formal packet structure was established (message type, identifier, timestamps or sequence numbers, payload, and integrity checks). Binary packet encoding and decoding were implemented on both the web interface and the robot's onboard module, followed by an experimental evaluation of the impact on data volume, latency, and computational overhead.

In parallel, a real-time control profile was introduced, formalizing command classes (emergency, motion control, service, telemetry) and their respective processing rules: execution time constraints, pruning of stale commands, and acknowledgments for critical actions. To ensure prioritized execution, a queuing and message dispatching mechanism was implemented, allowing high-priority commands to be processed first, even under network congestion or instability. The final stage involved testing under conditions of variable latency and packet loss, comparing metrics before and after optimization. This confirmed an increase in data transmission speed and improved platform control reliability.

A robotic platform prototype was developed to conduct the experiments. The electrical subsystem is based on the Rover 5 chassis with two brushed DC motors. Motion control is achieved via polarity switching and pulse-width modulation (PWM) through an L298N driver. The functional diagram of the platform is shown in Fig. 2, the operational algorithm in Fig. 3, and the physical implementation in Fig. 4.

In the current configuration, the control board acts as a server, while the user's browser serves as the client. Control inputs are generated by a virtual joystick, and coordinates are transmitted to the web server maintaining the WebSocket connection. The server-side logic is based on the ESP32Async library [13], while the control interface utilizes a JavaScript joystick library [14] and auxiliary controls. The result is a functional prototype for testing a WebSocket-based control system (Fig. 1).
Since the WebSocket standard supports both text and binary frames, a rigorous "text vs. binary format" comparison was conducted, focusing on how encoding and message structure affect performance and reliability. To ensure an objective evaluation, a structured experimental design was employed, involving fixed factors (format, message size, exchange frequency, control scenarios, and load) across multiple repetitive trials. Network conditions—including latency, jitter, packet loss, and bandwidth constraints—were emulated using tc netem.

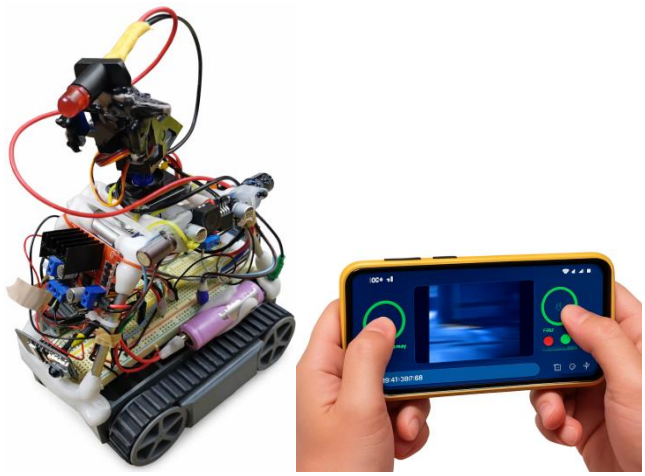


Fig. 1. Developed prototype for testing WebSocket-based control systems for robotic platforms

The resulting data underwent statistical analysis, including the calculation of confidence intervals and hypothesis testing. This approach established a reproducible experimental framework, providing a reasoned assessment of how transitioning from text-based JSON to binary messages enhances exchange rates and improves the reliability of real-time robotic platform control.
To conduct the experiment, network traffic between the operator's web client and the ESP8266 board was captured using Wireshark [15], focusing specifically on the WebSocket control channel. An active Wi-Fi interface was selected on the operator's computer, and a capture filter was applied based on the TCP port and the board's IP address, as WebSocket cannot be directly filtered as a standalone protocol during the live recording stage. Upon completion, frame analysis was performed using display filters to isolate WebSocket traffic, categorizing exchange modes by frame type (text and binary). To isolate individual control sessions, the "Follow TCP Stream" feature was utilized. Subsequently, the total bytes and packets per connection were recorded via Wireshark's statistics windows, and throughput time-series graphs were generated

to ensure a precise comparison between JSON and binary exchange modes under identical scenarios.

A series of controlled trials followed, where the operator maneuvered the platform via the web interface using a virtual joystick according to fixed scenarios of equal duration. For each run, the exchange format (text_json or binary), command transmission frequency, number of clients, and network profile were defined. Performance and reliability metrics—including latency, jitter, packet loss, reconnections, and data intensity—were recorded. A total of 20 trials were conducted, with all parameters and measured values documented in unified tables: one for experimental variables and another for trial results to facilitate a comparative analysis of the control modes.

Based on the results of the 20 trials (10 pairs of text_json vs. binary), it was established that the binary mode consistently yields lower control latency, reduced traffic intensity, and slightly fewer packet losses. The distribution of these trials, plotted across average latency and traffic intensity coordinates, is presented in Fig. 2, providing visual confirmation of the advantages of binary exchange for the control channel.

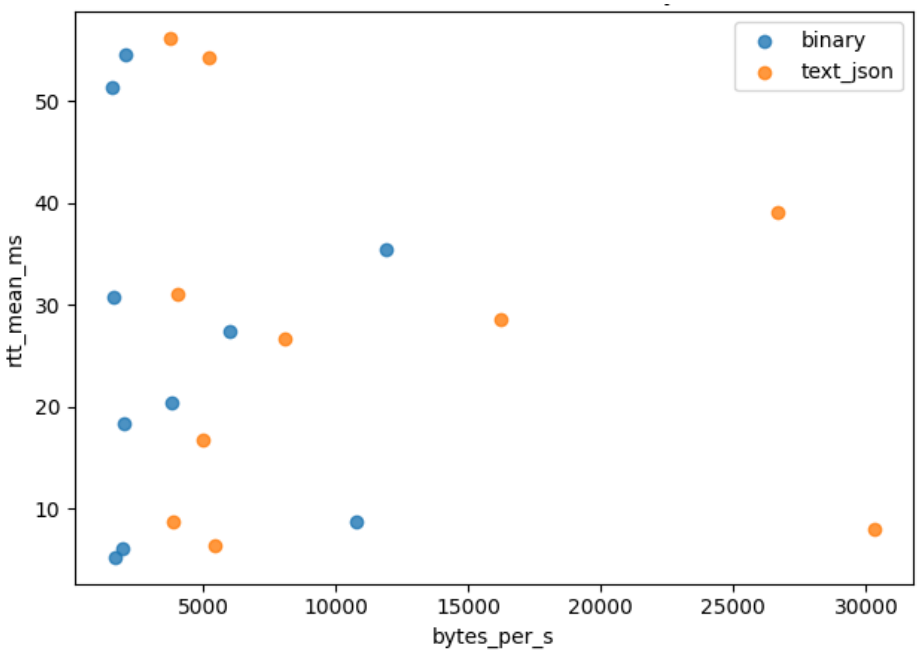


Fig. 2. Average control latency (RTT) vs. WebSocket channel traffic intensity in text (JSON) and binary exchange modes

Indeed, the data indicates that the binary operational mode yields more significant results in terms of control efficiency

Conclusions

A comparison of two modes for transmitting control messages via WebSocket — text-based (JSON) and binary — demonstrated the superiority of binary exchange across key control channel performance metrics. Based on a paired analysis of 10 comparable scenarios, it was established that the binary mode reduces traffic intensity

by an average of approximately 6,505 bytes/s, meaning fewer data resources are required to transmit the same control inputs. Regarding control responsiveness, evaluated via Round-Trip Time (RTT), a trend toward a reduction in average latency by approximately 1.72 ms was observed in binary mode. Consequently, transitioning from JSON to binary frames ensures more efficient bandwidth utilization of the control channel and potentially enhances the operational reaction speed of the control system.

REFERENCES

[1] L. Srinivasan, J. Scharnagl, and K. Schilling, "Analysis of WebSockets as the New Age Protocol for Remote Robot Tele-operation," IFAC Proceedings Volumes, vol. 46, no. 29, pp. 83–88, 2013, doi: 10.3182/20131111-3-KR-2043.00032.

[2] N. Pico, G. Mite, D. Morán, M. S. Alvarez-Alvarado, E. Auh, and H. Moon, "Web-Based Real-Time Alarm and Teleoperation System for Autonomous Navigation Failures Using ROS 1 and ROS 2," Actuators, vol. 14, no. 4, art. 164, 2025, doi: 10.3390/act14040164.

[3] Z. Kapić, A. Crnkić, E. Mujčić, and J. Hamzabegović, "A Web Application for Remote Control of ROS Robot Based on WebSocket Protocol and Django Development Environment," IOP Conference Series: Materials Science and Engineering, vol. 1208, no. 1, art. 012035, 2021, doi: 10.1088/1757-899X/1208/1/012035.

[4] "ROS Web Control Center," ROS.org, Jan. 26, 2016. [Online]. Available: https://www.ros.org/news/2016/01/ros-web-control-center.html

[5] P. Stoev, D. Chikurtev, T. Stefanov, D. Dimitrov, and D. Vitanova, "Remote Control of a Teleoperated Multi-Purpose Mobile Robot Platform Using a Web-Based Graphical Interface, via MQTT and Web Sockets," in Proceedings of the 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Canary Islands, Spain, Jul. 19–21, 2023. Piscataway, NJ, USA: IEEE, 2023, pp. 1–6, doi: 10.1109/ICECCME57830.2023.10252491.

[6] "ROS Control Center: A web-based control center for ROS robots," GitHub repository. [Online]. Available: https://github.com/pantor/ros-control-center

[7] L. Lee and J. Lau, "Robot Context Protocol (RCP): A Runtime-Agnostic Interface for Agent-Aware Robot Control," arXiv preprint arXiv:2506.11650, 2025. [Online]. Available: https://arxiv.org/abs/2506.11650

[8] O. Kavas-Torris, S. Y. Gelbal, M. R. Cantas, B. Aksun-Guvenc, and L. Guvenc, "V2X Communication between Connected and Automated Vehicles (CAVs) and Unmanned Aerial Vehicles (UAVs)," Sensors, vol. 22, no. 22, art. 8941, 2022, doi: 10.3390/s22228941.

[9] G. Billon, "Nodejs-Websockets-GCS: Web based Ground Control Station for unmanned vehicles talking MAVLink," GitHub repository. [Online]. Available: https://github.com/gaelbillon/Nodejs-Websockets-GCS

[10] Ch. Liang, "WiFi WebSocket Remote Robot," Instructables, 2018. [Online]. Available: https://www.instructables.com/WiFi-WebSocket-Remote-Robot/

[11] L. Srinivasan, J. Scharnagl, Z. Xu, N. Faerber, D. K. Babu, and K. Schilling, "Design and Development of a Robotic Teleoperation System using Duplex WebSockets suitable for Variable Bandwidth Networks," IFAC Proceedings Volumes, vol. 46, no. 29, pp. 57–61, 2013, doi: 10.3182/20131111-3-KR-2043.00029.

[12] DFRobot, "Rover 5 Introduction (ROB0055)." [Online]. Available: https://dfimg.dfrobot.com/enshop/image/data/ROB0055/Rover%205%20Introduction.pdf

[13] “ESP Async WebServer (Asynchronous HTTP and WebSocket Server Library),” Arduino Libraries Documentation. [Online]. Available: https://docs.arduino.cc/libraries/esp-async-webserver/
[14] R. D’Amico, “JoyStick 2 – The new version: A simple JoyStick that uses HTML5 Canvas and Vanilla JavaScript,” GitHub repository. [Online]. Available: https://github.com/bobboteck/JoyStick
[15] Wireshark Foundation, “Wireshark (Network Protocol Analyzer).” [Online]. Available: https://www.wireshark.org/.

ARTIFICIAL INTELLIGENCE SYSTEMS IN THE INTERNET OF THINGS: EMERGING TECHNOLOGIES AND PRACTICAL APPLICATIONS

Maksym MAKARENKO

Head of the NGO “Center for Digital Research”

Abstract

The paper examines the integration of artificial intelligence (AI) with the Internet of Things (IoT) to create intelligent systems. Architectural approaches to deploying AI solutions are considered, including cloud, edge, and hybrid computing models. The role of deep learning technologies, in particular convolutional neural networks, in processing data from IoT devices is analyzed. The impact of fifth-generation networks (5G) on the development of AIoT systems is highlighted. Key areas of practical application are presented, including healthcare, transport, energy, and smart cities. The main challenges related to security, data privacy, and the ethical nature of AI solutions are identified, and prospects for the further development of the synergy between AI and IoT are outlined.

Keywords: artificial intelligence, Internet of Things, AIoT, machine learning, edge computing, cloud computing, 5G, smart cities, deep learning, cybersecurity.

Introduction

Artificial intelligence (AI) and the Internet of Things (IoT) are currently experiencing rapid development and are increasingly being combined to create intelligent systems. IoT provides a global network of physical devices, sensors, and instruments that collect big data, while AI enables the analysis of this data and its transformation into useful information and decisions. The mutual integration of cloud and edge computing with AI and IoT provides a reliable pathway for transforming raw sensor data into meaningful knowledge, enabling real-time decision-making and predictive analytics. Practice shows that the combination of AI and IoT increases operational efficiency, promotes service personalization, and supports evidence-based decision-making in various sectors—from healthcare to industry and urban resource management.

Research Results

Accumulated experience in implementing the so-called “AIoT” (Artificial Intelligence of Things) indicates that AI is most often used for tasks such as forecasting, object and event recognition, and real-time decision-making based on data. Common data types processed by AI algorithms in IoT systems include numerical streams from sensors (temperature, pressure, indicators, etc.). Today, the most active area of application is healthcare, followed by agriculture and transport. At the same time, the majority of existing AIoT solutions are at early stages of development and have not yet undergone full validation in real-world conditions. From the perspective of AI methods, modern IoT systems most often use deep learning—in particular, convolutional neural networks (CNNs) dominate, mainly in the form of supervised learning on large datasets [2, 3].

The integration of AI solutions into IoT infrastructure requires consideration of system architecture and the placement of computing components. The classical approach involves cloud computing, where data from IoT devices is sent to a processing center (the cloud), where powerful AI algorithms analyze it and send results back. Cloud platforms (such as AWS, Azure, GCP) provide scalable resources for storing and processing massive IoT data streams, simplify the deployment of machine learning models, and ensure centralized analytics [1]. This enables the implementation of complex services—from anomaly detection to predictive maintenance—in various domains such as telemedicine and smart cities.

However, transmitting all data to the cloud creates network load and causes latency, which is critical for real-time applications. Therefore, the edge computing approach is gaining popularity, where AI algorithms are deployed closer to data sources—at the level of gateways, local servers, or the devices themselves. Edge data processing reduces latency and traffic volume, enabling faster responses to events. The implementation of Edge AI has become possible thanks to optimized frameworks (TensorFlow Lite, PyTorch Mobile, etc.) that allow neural network inference even on resource-constrained microcontrollers. Thus, latency-sensitive or critical tasks (such as detecting dangerous situations via surveillance cameras or emergency equipment control) can be performed locally without waiting for responses from remote servers [1].

In general, various models for deploying AI in the IoT ecosystem are possible: cloud-based, edge-based, and hybrid. In practice, purely cloud or purely edge solutions are the most common, while hybrid architectures (where part of the processing is done locally and part in the cloud) are used less frequently. At the same time, the hybrid approach appears promising, as it allows dynamic workload distribution: time-sensitive tasks are handled locally, while resource-intensive computations (such as training large models) are performed in the cloud. Important aspects of AI–IoT integration include ensuring reliable communication between devices (using protocols such as MQTT, CoAP, HTTP(S)) and creating standardized interfaces for compatibility among heterogeneous system components.

As noted above, edge computing is one of the key technologies linking AI and IoT. Thanks to advances in hardware (high-performance microcontrollers, single-board

computers, AI chips), machine learning can be performed directly on devices or local network nodes. This enables minimal latency and rapid response to events, while reducing dependence on constant internet connectivity. For example, modern smart cameras can locally use neural networks to detect motion or danger in video streams and instantly notify of incidents without transmitting the entire stream to the cloud.

The deployment of fifth-generation (5G) communication networks significantly expands opportunities for AIoT systems. 5G provides high bandwidth and ultra-low latency, as well as support for massive device connectivity, which is critical for IoT environments. Combining 5G with AI technologies opens the way to new levels of performance. For instance, autonomous vehicles require uninterrupted and fast communication between the vehicle, infrastructure sensors, and cloud servers—made possible by 5G, which enables near real-time data exchange. Reviews note that the integration of IoT and AI combined with the potential of 5G creates a synergy capable of significantly improving modern urban and industrial systems [5]. Looking ahead, the emergence of 6G networks is already being predicted, which will embed intelligence even deeper into network infrastructure. It is expected that sixth-generation network elements will be able to learn, adapt to their environment, and autonomously optimize data processing, leading to new concepts such as fully cognitive cities and environments.

Recent advances in artificial intelligence, particularly deep learning, have become a driving force behind the development of intelligent IoT systems. Modern computer vision, natural language processing, and predictive analytics algorithms are all based on multi-layer neural networks capable of detecting complex hidden patterns in large datasets. This is extremely relevant for IoT, as sensors generate continuous streams of diverse data, and traditional methods are often unable to extract useful patterns. Neural networks have proven effective in tasks such as classification, event detection, and prediction based on sensor data. According to recent reviews, convolutional neural networks (ConvNets) are currently the most widely used AI methods in IoT systems. Therefore, the development of deep learning architectures—including lightweight models optimized for edge computing—largely determines the progress of AI–IoT synergy. Promising directions also include explainable AI to enhance transparency in decision-making for critical applications, and distributed learning approaches to preserve data privacy. The combination of these approaches is intended to strengthen trust in AIoT solutions and expand their adoption in sensitive domains.

Let us consider several key areas where the combination of AI and IoT already demonstrates significant results:

Healthcare. Smart medical devices and wearable sensors (the Internet of Medical Things) collect patient health data 24/7—heart rate, blood pressure, glucose levels, and more. AI algorithms analyze these large datasets and can detect alarming deviations or early symptoms of diseases. For example, remote monitoring systems for patients with heart failure already use AI to interpret data from implanted sensors and warn physicians in advance about deterioration in patient condition. Studies show that integrating AI into such IoT systems improves diagnostic accuracy and enables more patient-centered treatment outcomes. Other popular applications include

smartwatches and fitness trackers that monitor basic health indicators and alert users in case of anomalies, as well as smart pillboxes (IoT-enabled medication containers) that monitor adherence to medication schedules [6].

Transport. In the transport sector, the synergy of IoT and AI is manifested in the implementation of intelligent transportation systems. One of the most striking examples is autonomous vehicles. Such vehicles are equipped with dozens of IoT sensors (lidars, cameras, radars) that continuously scan the environment, as well as onboard AI systems that interpret this data for real-time control. An autonomous vehicle must instantly recognize objects on the road, plan routes considering traffic conditions, and communicate with infrastructure (traffic lights, road sensors). This has become possible thanks to the combination of powerful neural network algorithms for computer vision and high-speed wireless communication (modern V2X protocols, particularly those based on 5G). Another aspect involves urban traffic management systems: IoT sensors (cameras, road detectors) collect data on traffic flow, while AI optimizes traffic light operation in real time, reroutes flows, and predicts congestion. This increases road capacity and reduces delays for passengers. Similar projects are already being implemented in the concepts of smart intersections and highways [3].

Energy. IoT and AI are transforming the energy sector through the implementation of smart grid technologies. Modern power grids are equipped with thousands of sensors and smart meters that monitor consumption, voltage, and equipment condition in real time. AI is used to analyze energy consumption patterns and forecast demand, enabling more efficient load balancing between generation and consumption and avoiding peak overloads [1]. For example, neural networks can predict electricity consumption spikes based on time of day or weather conditions and proactively adjust grid operation modes or activate backup generators. In addition, predictive maintenance of critical grid components (transformers, substations) is based on IoT data: by analyzing temperature, vibration, and other indicators, AI can predict potential failures and recommend scheduled replacement before breakdowns occur. Such intelligent energy systems already demonstrate increased reliability of power supply and reduced losses. In the broader urban context, AI algorithms optimize various energy processes—from street lighting control to load distribution between conventional and renewable energy sources—contributing to overall energy efficiency.

Smart City. The Smart City concept integrates various domains—transport, energy, utilities, security, environment—into a single intelligent infrastructure. IoT provides comprehensive sensor coverage and cyber-physical systems throughout the city (smart lighting, parking sensors, environmental monitors, etc.), while AI provides tools for holistic analysis of this heterogeneous data. AI in smart cities enables real-time processing of massive information streams from diverse sources (cameras, sensors, social media) and optimization of urban processes. For example, systems for monitoring the condition of bridges and buildings are already being implemented, where AI analyzes data from hundreds of sensors and warns of structural risks. Other applications include smart street lighting (automatic brightness adjustment based on

traffic and time of day), intelligent waste collection systems (garbage truck routes optimized by AI based on container fill levels), real-time monitoring of air quality and noise pollution with corresponding responses from municipal services, and more. Estimates suggest that around 30% of urban applications already integrate AI in one way or another to enhance sustainability, safety, and comfort, and this share is rapidly growing [4]. For instance, neural networks help forecast public transport passenger flows and optimize schedules, or analyze video streams from cameras to enhance public safety. All of this makes urban governance more proactive: problems are detected and resolved before residents even report them. Smart cities built on the IoT+AI combination have the potential to significantly improve quality of life by making urban infrastructure more resilient, efficient, and responsive to citizens' needs.

Despite the obvious advantages, the close integration of AI and the Internet of Things generates a number of challenges and risks that must be addressed. At the technical level, one of the main problems is data security and privacy. Billions of IoT devices generate sensitive data (health, location, human activity), and their transmission and processing by AI models must be securely protected. Concerns remain regarding data leaks, unauthorized access, and misuse of information. This necessitates end-to-end encryption, reliable device authentication, and new regulatory frameworks to protect user privacy. Experts note that growing cybersecurity and privacy threats require both updated legislation and technical solutions (such as differential privacy and blockchain for IoT transaction verification) to ensure ethical and secure AIoT deployment [2].

Social risks include potential biases and errors in AI systems, which in the IoT context may have direct physical consequences. If an algorithm controlling transport or a medical device makes an error due to incorrect data or inherent model bias, it may cause accidents or harm human health. Therefore, research in explainable and trustworthy AI, the development of validation and testing methods for AIoT systems prior to deployment, and the implementation of ethical standards and certification are critically important [3].

Despite these challenges, the prospects for further AIoT development are extremely broad. Significant opportunities arise in areas such as precision agriculture (where combining soil sensor and drone data with AI can dramatically increase yields and optimize resource use), environmental monitoring (automated tracking of environmental conditions and forecasting of hazardous phenomena), Industry 4.0 (self-adjusting factories with minimal equipment downtime), and many others. Successfully addressing current security and standardization issues will pave the way for large-scale AIoT adoption. A network of intelligent devices working collaboratively based on AI will become an integral part of everyday life, enhancing comfort, safety, and sustainability. This development already forms the basis for concepts such as the "Internet of Everything," where every device is not only connected but also intelligent. Experts emphasize that sustainable progress in this direction requires both technological innovation (new algorithms, hardware, network solutions) and sound policy—developing regulatory standards that ensure ethical AI

use in IoT, data protection, and consideration of societal interests. Under these conditions, the synergy of AI and the Internet of Things promises a true digital revolution across various sectors, the results of which we will observe in the near future.

Conclusions

Thus, artificial intelligence systems in the Internet of Things represent one of the most promising directions in modern IT. They already deliver practical benefits and, in the near future, have the potential to fundamentally transform everyday life, production, and urban environments. The integration of AI and IoT makes it possible to create a world where devices are not only connected but truly intelligent, capable of making autonomous decisions for the benefit of people. The future success of AIoT will depend on the joint efforts of researchers, engineers, and society in overcoming existing barriers and responsibly implementing these technologies.

REFERENCES

[1] I. Ficili, M. Giacobbe, G. Tricomi, and A. Puliafito, «From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI», *Sensors*, vol. 25, no. 6, p. 1763, 2025. https://doi.org/10.3390/s25061763

[2] A. Marengo, «Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms», *Internet of Things*, vol. 27, p. 101318, 2024. https://doi.org/10.1016/j.iot.2024.101318

[3] U. Khadam, P. Davidsson, and R. Spalazzese, «A systematic literature review on AI in IoT systems: Tasks, applications, and deployment», *Internet of Things*, vol. 34, p. 101779, 2025. https://doi.org/10.1016/j.iot.2025.101779

[4] M. E. E. Alahi, A. Sukkuea, F. W. Tina, *et al.*, «Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends», *Sensors*, vol. 23, no. 11, p. 5206, 2023. https://doi.org/10.3390/s23115206

[5] N. Omheni, H. Koubaa, and F. Zarai, «Artificial Intelligence for 5G and 6G Networks: A Taxonomy-Based Survey of Applications, Trends, and Challenges», *Technologies*, vol. 13, no. 12, p. 559, 2023. https://doi.org/10.3390/technologies13120559

[6] L. Shaw and H. A. Gohel, «Role of artificial intelligence in health monitoring using IoT based wearable sensors: A survey», *Internet of Things*, vol. 34, p. 101761, 2025. https://doi.org/10.1016/j.iot.2025.101761

ORGANIZATION OF RASPBERY PI LABORATORY WORK IN REMOTE MODE

Hennadii MOHYLNYI (PhD, Associate Professor)[1]
Olha SMAHINA (PhD, Associate Professor)[2]
Iryna SHVETS (Postgraduate, Senior Lecturer)[3]

Luhansk Taras Shevchenko National University, Lubny, Poltava region, Ukraine
Department of Information Technologies and Systems
[1]g.mogilniy@gmail.com, [2]smagina1804@gmail.com, [3]irinachipenkooo@gmail.com

Abstract

The paper investigates the methodology of organizing remote work in a training laboratory based on Raspberry Pi microcomputers running the Ubuntu OS. The aspects of integration into the Microsoft AD domain infrastructure and setting up remote access using Gnome-remote are shown. Particular attention is paid to the automation of administration of training stands, in particular, the mechanisms of cleaning the system and forcing a reboot after the end of sessions. Technical challenges when working with peripheral devices are identified. The proposed approach provides a learning environment for training IoT specialists in blended learning.

Keywords

operating system, Microsoft domain, Ubuntu, remote access, training stand, RDP, Gnome-remote

Introduction

Embedded Systems and Microcontrollers Market is demonstrating exponential growth, which creates a strong demand for qualified specialists who are able not only to program ready-made solutions, but also to design complex hardware and software complexes, configure sensor interaction, and master modern Internet technologies.

In this context, the higher education system faces a serious challenge: how to ensure high-quality practical training of engineers in the conditions of dynamic changes in the technological stack and, which is especially relevant today, in conditions of limited access to physical classrooms. The traditional model of organizing training laboratories, which involves the exclusive physical presence of students at hardware stands, is becoming insufficiently flexible.

However, the study of microcontrollers and IoT has its own specifics, which cannot be completely covered by virtual simulators (such as Proteus, Tinkercad or Cisco Packet Tracer). Simulators, despite their convenience, operate in idealized conditions and do not reproduce real physical processes, network delays, hardware failures and the nuances of working with real electrical signals. Therefore, there is an urgent need to organize a new type of training laboratories that combine physical equipment with remote access technologies, allowing students to write code, upload it to a real microcontroller and observe the result of the work (via webcams or telemetry) from anywhere in the world.

The purpose of the research. The purpose of this work is to develop and implement a comprehensive system for organizing the work of training laboratory based on Raspberry PI, providing the ability to conduct laboratory classes both in person and remotely using real equipment.

Research results

The development of single-board computers, in particular the Raspberry Pi series, has led to the emergence of a wide ecosystem of operating systems adapted to the specific needs of users: from initial programming training to professional deployment of industrial Internet of Things (IoT) solutions. The choice of software platform today is a determining factor that outlines the limits of performance and security of a computing system.

Currently, there are several operating systems that can be used on the Raspbery PI: Raspberry Pi OS, Ubuntu, DietPi, Home Assistant OS, RetroPie, LibreELEC, Kali Linux, Arch Linux ARM and others [1-6].

However, for educational purposes, Ubuntu for Raspberry Pi (especially for models 4, 400 and 5) was chosen as the base OS - it is not just an „alternative", but a standard for many developers: it has one of the largest software repositories, container support, adapted to the 64-bit ARM architecture of the Raspberry Pi [2]. The full-fledged Desktop provides a modern interface (GNOME) that looks and works like a full-fledged PC. This is the best choice for learning programming or web editing. The new version of Ubuntu 24.04.3 LTS for desktops, laptops and Raspbery PI has long-term support, which means five years of free security and maintenance updates, extended to 12 years with Ubuntu Pro. There is the latest version of the Ubuntu operating system 25.10, which comes with nine months of security and maintenance updates, until July 2026.

It is known that the standard SSH system service is used to remotely control Raspberry Pi from another device on the local network, which is easily installed using the sudo apt-get install ssh command and is necessary for additional management or administration. A more thorough analysis of the literature and Internet sources allowed us to find other additional software tools: Xrdp, NoMachine, X2go. These additional software tools have various features and require the installation of additional packages. Therefore, it was decided to consider only the Gnome-remote component, which is standard in Ubuntu settings, within the framework of this work, and to consider the capabilities of other software tools in the framework of the next study.

In general, creating a training stand, with remote use mode, can be reduced to the following steps.

Step 1. Configure a static IP address and DNS. Be sure to specify the address of the Microsoft AD domain controller as the DNS server. Make these settings using the "Settings" application in the "Network" menu. In addition, it is recommended to edit the files: /etc/systemd/resolve.conf – add the DNS and domains fields, as well as the /etc/hosts file – add the main resources of your network.

Step 2. Join the Microsoft AD domain to integrate the user list. Install additional packages sssd, realmd, adcli and others using the command sudo apt-get install sssd, realmd, adcli Checking the availability of the Microsoft AD domain: sudo realm -v discover < domain name >

We pay attention to the required additional packages that will be listed at the end of the command and, if necessary, install these packages.

Join the AD domain.

sudo realm join -v -U < domain administrator name > < domain name >

We grant the right to create a home folder in the application: sudo pam-auth-update

Step 3. Activate the Gnome-remote service. We perform these settings using the “Settings” application of the “System” menu – “Remote Desktop”, then the “Remote Desktop” tab. We set the username and password. This user should not be in the system. Using these parameters (username and password), we already have the opportunity to connect to the Raspberry PI using the “Remote Desktop” application. After connecting, a list of users who have recently used this Raspberry PI will be displayed.

When using the Remote Desktop client in Windows, certain configuration features are installed:

1. In the "Screen" tab, you need to carefully select the screen resolution parameters. In some cases, and especially in the "Full Screen" mode, the connection does not occur.

2. It is advisable to edit the service file that is created using the "Save" button, find the line: use redirection server name:i:0 and change it to use redirection server name:i:1 [7].

If you are using the Raspberry PI for personal use, these steps will be sufficient. However, if you want to use the Raspberry PI as a learning platform, you will need to perform additional setup.

Step 4. In the process of using remote access, it turned out that users do not have the right to use external ports. It was established that it is possible to use special control using the UDEV component [8]. Using special files (.rules extension), it is possible to assign certain access to external devices/ports. Udev rules are stored in the /etc/udev/rules.d folder. It is better to create a separate file for your rules and add the following sinks, for example, for using an external camera and a USB port:

KERNEL=="video[0-9]*", MODE="0666"

KERNEL=="ttyACM0", MODE="0666"

Step 5. It also turned out that users should see the results of working with the training stand. To do this, you need to configure automatic loading of the camera viewing application, for example cheese. This can be done using a special file cheese.desktop in the /etc/xdg/autostart/ directory and granting the right to "read" this file. The structure of this file is similar to other * desktop files.

Step 6. Additionally, it turned out that there is a need for a mandatory system reboot and a time limit for working with the stand, for example, 90 minutes, so that other users can use this educational stand. The system reboot must be done to remove all port settings and additional devices that the student user has made. One option is to

use the command: sudo shutdown -r +90 (or the sleep 5400 && sudo reboot command). This command must be activated when the user logs in. This can also be done using an additional special file *.desktop in the /etc/xdg/autostart directory, granting the right to “read” this file, but setting the parameter Exec= sudo shutdown -r +90. It should be noted that this use case allows users to cancel the reboot, which is a significant drawback.

To use this command, you must have SUDO privileges.

On the other hand, it turned out that setting a usage time limit is not enough in the case when the user himself, prematurely terminates work with the stand. For this, it is necessary to automate the system reboot when the user logs out.

One possible step is to edit the file /etc/gdm3/PostSession/Default — this is a system cleanup script that is executed by the login manager (GDM) at the last moment of the user session. To do this, you need to insert a condition before the line exit 0. For example:

```
TARGET_GROUP=" IOT  USERS@MYDOMAIN "
if id -nG "$USER" | grep -Fq "$TARGET_GROUP"; then
sleep 10
/sbin/reboot
fi
```

Special attention should be paid to the TARGET_GROUP parameter, which is the value of the group of users for whom this rule is applied. In certain cases, the group name may have a different syntax.

Step 7. In some cases, it is necessary to grant the right to execute certain commands in SUDO mode. To do this, use the additional configuration of the /etc/sudoers file and add the necessary terms to execute these commands without the need to enter the SUDO password. For example, for the group "IOT USERS@MYDOMAIN":

```
%"IOT\ USERS"@MYDOMAIN ALL=(ALL) NOPASSWD: /sbin/reboot
%"IOT\ USERS"@MYDOMAIN ALL=(ALL) NOPASSWD: /sbin/ shutdown
```

Also note that certain operating system releases may have some peculiarities in using group names from the Microsoft domain.

Step 8. Additional system restrictions. In the process of using remote access, it was found that it is necessary to limit the number of simultaneous connections and automate the termination of sessions that were not completed correctly or were accidentally interrupted. It was found that the Gnome-remote package does not have configuration options for limiting the number of simultaneous connections, which is certainly **a significant drawback.** One of the simple ways can be to use the iptables package and the iptables-persistent service, which are difficult to configure, conflict with the firewall and can block the entire system as a whole. For example, it is possible to limit the number of connections via TCP port 3389 (RDP) and use a command similar to the following: sudo iptables –I INPUT –p tcp –dport 3389 –m connlimit --connlimit-above 1 --connlimit-mask 0 –j REJECT

where INPUT is a chain of rules for incoming packets;

-p tcp – Protocol TCP;

--dport 3389 – Destination Port;

--connlimit-above 1 – trigger condition: “If the number of connections is MORE than 1”;
--connlimit-mask 0 – grouping mask;
-j REJECT – reject and send an error message.
In addition, it turned out that periodically, according to a certain schedule, it is necessary to configure a reboot of the **training stand system** and then notify all users of this schedule. Otherwise, there may be an overload of the processor or insufficient RAM. To do this, it is possible to use the cron system service and add a system reboot to the schedule using the sudo crontab - e command. For example, 0 14 * * * /sbin/shutdown -r now - reboot the system at 0 minutes, 14 hours, every day, every month, every day of the week. It should also be noted that the cron service schedule must run from the root user so that ordinary users - students - do not have the opportunity to change it.

Conclusions

Based on the research, it can be concluded that the organization of a new type of training laboratories based on Raspberry Pi allows you to combine physical equipment with remote access technologies, which is critically important for training engineers in conditions of limited access to classrooms. Choosing Ubuntu OS version 24.04 LTS or 25.10 as the base platform is one of the possible solutions, which provides a modern GNOME interface, has long-term support and is a de facto standard for IoT developers.
For effective management of the Raspberry PI stand, the system was successfully integrated with the Microsoft AD domain using the sssd, realmd and adcli packages, which allows for centralized management of user access. Using the standard Gnome-remote component provides remote connection, although it requires careful configuration of screen resolution settings and access rights to external devices through UDEV rules.
For efficient operation of the stand, a method of automatic loading of applications, for example, cameras, for remote viewing of the results of work with the stand, is proposed. An important aspect is ensuring the autonomy of the stand, which is achieved by limiting the time of use and automatically rebooting the system after the end of the user session by editing the /etc/gdm3/PostSession/Default script, as well as using the cron service to prevent overloading of hardware resources.
Despite certain shortcomings of Gnome-remote, such as the lack of a built-in limit on simultaneous connections, this issue is solved by using iptables rules to limit connections on port 3389. Thus, the proposed comprehensive approach allows you to create an environment for conducting laboratory classes in remote mode using real equipment.
It should be noted that this study did not consider alternative tools such as Xrdp, NoMachine or X2go, which have slightly different functionalities for educational purposes. In addition, for the effective use of the proposed stand, it is necessary to take into account the peculiarities of network infrastructure settings and providing

user access via the Internet, which requires special attention from the point of view of security and ease of use.

REFERENCES

[1] “Raspberry Pi software” [Online]. Available: https://www.raspberrypi.com/software/
[2] Ubuntu on a Raspberry Pi” [Online]. Available: https://ubuntu.com/download/raspberry-pi
[3] “LibreELEC Raspberry” [Online]. Available: https://libreelec.tv/downloads/raspberry
[4] “DietPi download” [Online]. Available: https://dietpi.com/#download
[5] “Kali Linux” [Online]. Available: https://www.kali.org/
[6] “RetroPie” [Online]. Available: https://retropie.org.uk/
[7] “RDP file setting: "use redirection server name" [Online]. Available: https://serverfault.com/questions/963651/rdp-file-setting-use-redirection-server-name
[8] “An introduction to Udev: The Linux subsystem for managing device events” [Online]. Available: https://opensource.com/article/18/11/udev

ANALYSIS OF VMWARE VCENTER CAPABILITIES FOR USE IN THE EDUCATIONAL PROCESS

Hennadii MOHYLNYI (PhD, Associate Professor)[1]
Svitlana PEREIASLAVSKA (PhD, Associate Professor)[2]
Volodymyr DONCHENKO (Postgraduate, Senior Lecturer)[3]

Luhansk Taras Shevchenko National University, Lubny, Poltava region, Ukraine
Department of Information Technologies and Systems
[1]g.mogilniy@gmail.com, [2]pereyaslav9@gmail.com, [3]ifmit.s.2014@gmail.com

Abstract

This article analyzes VMware vCenter's capabilities for educational purposes. It rationalizes the creation of a virtual training platform using hierarchical role-based access control (RBAC). An algorithm for configuring user roles and folder structures to ensure strict isolation of student resources in sandboxes is proposed. This approach allows students to safely develop practical cloud service administration skills through a web interface, ensuring system integrity and autonomy without the risk of damage to the main hardware.

Keywords

Virtual system, ESX, vCenter, VMware vSphere operating system, Microsoft domain, educational process, educational laboratory, role-based access model.

Introduction

In the context of rapid digitalization and the transition of business processes to cloud environments, virtualization technologies have become a fundamental component of modern IT infrastructure. To date, the VMware vSphere platform has been reduced to two key versions: vSphere Foundation (VVF) and Cloud Foundation (VCF) [1-3]. However, VMware by Broadcom solutions are the de facto industry

standard in enterprise virtualization, providing reliability, scalability, and flexibility for managing data center resources.

Nowadays, employers require graduates not only to know virtualization architecture, but also practical skills in administration, cluster deployment, and virtual network management. However, deploying physical labs for each student is a financially costly and difficult task to maintain.

Using VMware vCenter in the educational process partially addresses this problem, enabling the concept of a cloud training ground. A critically important advantage of this approach is the ability to provide remote access to laboratory facilities with additional network infrastructure settings. In the context of the spread of distance and blended learning, the ability to work with the enterprise infrastructure via a web interface (vSphere Client) from anywhere in the world becomes especially important. It contributes to a deeper assimilation of the material. In addition, with certain settings, vCenter can guarantee security and isolation: complex operations are performed in a virtual space, eliminating the risk of damage to the main equipment, even when connected remotely via VPN or a secure gateway.

The purpose of the research. Based on a comprehensive analysis of the capabilities of the VMware vCenter software component, develop ways to create a virtual learning environment.

Research results

After the Broadcom acquisition, a significant number of licenses were canceled. There are now two main subscription packages and one additional one.

- VMware Cloud Foundation (VCF) – «All Inclusive».
- VMware vSphere Foundation (VVF) – «Basic Virtualization».
- vSphere Standard / Essentials Plus. Saved only for the smallest.

Each license type includes the ESX component - the lowest layer of software. The ESXi 7 component is the first basic element of the training environment. After installation, the main ESXi configuration tool will be available - access via a browser to the network adapter address configured during deployment to Management.

vCenter Server is a centralized management platform for VMware vSphere infrastructure. It is a key component without which clustering (HA, DRS), distributed switch (vDS), vMotion and lifecycle management (Lifecycle Manager) are impossible. vCenter Server is the second basic component of the training environment. At the moment, the following versions exist:

- vCenter Server 7.x
- vCenter Server 8.x
- vCenter Server / VCF 9 (The Future / New Standard)

It is necessary to take into account the compatibility of ESX and vCenter versions. Table 1 lists the compatible versions [4].

Table 1. Interoperability Matrix

vCenter Server Version	Supported ESXi Versions	Comment
vCenter 9.0	ESXi 9.0 ESXi 8.0 U3	Support for ESXi 7.0 and earlier versions has been fully removed. Before upgrading to vCenter 9.0, ensure that all hosts are running ESXi version 8.0 Update 3 or later.
vCenter 8.0	ESXi 8.0 ESXi 7.0 ESXi 6.7 (until EOL)	The most flexible option for transitional environments. Enables management of mixed-version clusters during migration.
vCenter 7.0	ESXi 7.0 ESXi 6.7 ESXi 6.5	ESXi 8.0 is not supported. Hosts running ESXi 8.0 cannot be connected to vCenter Server 7.0.

It has been established that the access control subsystem in vCenter 7 is based on a hierarchical role-based access control (RBAC) model. Correct configuration of this component is a critical condition for ensuring data integrity and confidentiality, since 80% of security incidents in virtual environments are associated with access rights configuration errors, rather than vulnerabilities in the software code.

The security architecture is built on a strict relationship between three fundamental entities: Subject – Role – Object [5]. A deep understanding of their interaction is necessary to build a secure control loop and avoid the effect of «excessive privileges».

Access subjects are entities that initiate a request to perform an operation: users (user groups) and service accounts.

A role in vCenter is not just a set of rights, but a definition of a functional profile. There are the following types of roles: System Roles, Sample Roles, and Custom Roles.

Objects in vCenter include certain inventory objects. This is the most complex and often misunderstood aspect of vSphere. A key conceptual error is the perception of vCenter as a single hierarchical tree. In fact, vCenter manages four parallel dimensions (trees) of objects:

1. Hosts and Clusters: Represent physical computing resources.
2. VMs and Templates: Logical organization of workloads.
3. Storage: Hierarchy of storage systems (Datastores, Datastore Clusters).
4. Networking: Hierarchy of networks and virtual switching (DVS, Port Groups).

It should be noted that assigning rights in one tree never automatically extends to objects in other trees, even if they are logically related. Thus, if you create a folder (Folder) «Virtual X» in the VMs and Templates view (tree) and grant a user administrator rights to this folder, they will be able to manage the VMs. However, he will not see the Datastores on which the disks of these VMs are located and the networks to which they are connected, since these are objects in other trees.

Based on the identified risks in the organization of the educational process and the Zero Trust principle, a detailed access system has been developed. The main emphasis is on abandoning standard roles in favor of custom roles, which will allow us to eliminate conflicts between the inventory "trees" and ensure safe operation. The main idea of creating a training virtual environment is to select, develop, and assign certain non-standard roles (Custom Roles) to certain objects of the vCenter software component.

It is proposed to place the virtual laboratory in built-in, additional objects:

- Catalog of virtual machines and templates
- Catalog of networks and switches

The catalog (catalogs) of virtual machines and templates is intended for students (learners) to create training virtual machines according to parameters controlled by the teacher.

The catalog of networks and switches is intended for the teacher to place certain virtual switches (networks) used by students to create a separate network environment. Depending on the task, it is possible to provide students with the opportunity to create certain networks (port groups). However, experience shows that it is enough to create these networks and provide students with read-only access. In fact, this means that students have the opportunity to use certain isolated networks, and thus, when performing laboratory work, get their own personal network that does not conflict with other networks in the entire information system. In general, six additional roles were developed to create a virtual environment.

As a result of a comprehensive analysis of the vCenter role model and the features of the educational process organization, a sequence of actions necessary to create a learning environment was developed:

1. Connect the vCenter component to Microsoft AD.
2. Create additional groups in Microsoft AD on the AD controller server.
3. Create additional virtual machine directories for the location of student virtual machines.
4. Create additional directories for virtual networks for using the virtual environment.
5. Place the initial virtual machines for students in the directory.
6. Develop Roles to configure restrictions on the processes of creating virtual machines, using or creating networks, using hosts or clusters, and using certain storage (disks).
7. Assign certain Roles for certain Ms AD groups to directories for storing virtual machines.

8. Assign certain Roles for certain Ms AD groups to directories for virtual networks and create these virtual networks.

9. Assign certain Roles for certain Ms AD groups to the necessary storage.

10. Assign specific Roles to specific Ms AD groups on hosts or clusters.

Conclusions

Based on a comprehensive analysis of the vCenter role model, a sequence of actions for the deployment of a virtual infrastructure based on VMware vSphere has been developed. The key feature of the deployed environment is its adaptation to a multi-user learning model, where the ESXi hypervisor and the vCenter Server system act not only as a technical foundation, but also as a managed space. This is achieved through a deep hierarchical structuring of the inventory, where the use of specialized folders (Folders) and the assignment of certain combinations of Subject - Role allows you to logically isolate the resources of individual training groups and individual projects within a single hardware complex.

The creation of a training environment is based on the configuration of the access control model (RBAC), which can be adapted to the specifics of training scenarios. Unlike standard corporate settings, here the main emphasis is on creating «sandboxes-directories» for students, which is ensured by strictly restricting rights at the level of virtual machines, network interfaces, and data storage. Such determination of access rights guarantees the impossibility of destructive influence on the general infrastructure or the results of the work of other participants in the educational process, while maintaining a sufficient level of autonomy to perform complex laboratory tasks.

REFERENCES

[1] “broadcom completes acquisition of vmware” [online]. Available:. Https://www.broadcom.com/company/news/financial-releases/61541

[2] vmware cloud foundation” [online]. Available:. Https://ftpdocs.broadcom.com/cadocs/0/contentimages/vcf_spd_june2024.pdf

[3] “vmware vsphere foundation” [online]. Available:. Https://ftpdocs.broadcom.com/cadocs/0/contentimages/vvf_spd_may2024.pdf

[4] “product interoperability matrix” [online]. Available:. Https://interopmatrix.broadcom.com/interoperability

[5] “vmware-vsphere-7-0” [online]. Available:. https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/vsphere/vsphere/vmware-vsphere-7-0.pdf

ANALYSIS OF THE SPECIFICS OF TRAINING BACHELORS IN COMPUTER ENGINEERING IN THE IOT FIELD UNDER MARTIAL LAW

Hennadii MOHYLNYI (PhD, Associate Professor)[1]
Mykola SEMENOV (PhD, Associate Professor)[2]
Volodymyr DONCHENKO (Postgraduate, Senior Lecturer)[3]

Luhansk Taras Shevchenko National University, Lubny, Poltava region, Ukraine
Department of Information Technologies and Systems
[1]g.mogilniy@gmail.com, [2]nick@edu2dl.net, [3]ifmit.s.2014@gmail.com

Abstract

The article provides an analysis of the features of training bachelors in the specialty "Computer Engineering" in the conditions of martial law. Special attention is paid to the adaptation of infrastructure support in the direction of the Internet of Things (IoT) to the conditions of blended learning and energy instability. The effectiveness of the implementation of the hybrid model "Laboratory as a Service" (LaaS), which integrates virtual simulators (digital twins), individual sets of mobile equipment and remote access systems, is substantiated.

Keywords

Computer Engineering, Internet of Things (IoT), Embedded Systems, Industry 4.0, Blended Learning, Remote Laboratory, Lab as a Service (LaaS).

Introduction

The rapid development of the Industry 4.0 paradigm and global digitalization are fundamentally reshaping the requirements for specialists in the field of Computer Engineering. The Internet of Things (IoT), embedded systems, and cyber-physical systems are no longer highly specialized niches; instead, they have become integral components of the modern technological ecosystem, ranging from smart home solutions to automated military command and control systems.

In Ukraine, this transformation is further complicated by the unprecedented challenges posed by martial law. Under these conditions, Higher Education Institutions (HEIs) are required not only to modernize the content of educational programs in line with global standards but also to fundamentally rethink the organization of the educational process itself. Traditional laboratory-based training models are becoming partially or entirely impractical due to security risks, restricted access to facilities, and energy instability.

A modern bachelor’s graduate in Computer Engineering is therefore expected to possess a comprehensive and interdisciplinary set of competencies, including low-level microcontroller programming, printed circuit board (PCB) design, deployment of cloud-based services, basic data processing technologies, and cybersecurity skills aimed at ensuring the reliable operation of critical infrastructure.

The purpose of the research is to conduct a comprehensive analysis of the characteristics of bachelor's training in the specialty Computer Engineering with a focus on IoT technologies at leading Ukrainian universities, as well as to identify effective mechanisms for adapting the educational process and laboratory infrastructure to blended learning conditions and potential power outages.

Research results

At the initial stage of the study, publicly available information from the official websites of leading Ukrainian universities was analyzed, including curricula and educational and professional programs for bachelor's training in Computer Engineering for the 2024–2025 academic year. The analysis revealed that the curricula primarily emphasize computer architecture, system programming, cybersecurity, and Internet of Things technologies. A list of university web resources and official program descriptions used in the analysis is provided in the references [1–13].

Based on the conducted analysis and the authors' practical experience, it can be concluded that a modern bachelor's graduate in Computer Engineering must possess a set of competencies covering the entire lifecycle of computer systems. The key professional competencies include:

Hardware and software design: the ability to develop and maintain both hardware components (electronic circuits, FPGA-based solutions) and system or application-level software;

Embedded systems and IoT engineering: the ability to design and program IoT devices with integration into fog and cloud computing environments;

Microprocessor and single-board systems: the use, configuration, and operation of modern microcontroller and mini-computer platforms to solve applied engineering problems;

Design automation: the use of computer-aided design (CAD) systems for developing components of computer systems, printed circuit boards, and systems-on-chip (SoC).

The study of IoT technologies, microcontrollers, and embedded systems within bachelor's programs in Computer Engineering is implemented through a combination of mandatory and elective disciplines with a strong practical orientation.

Modern curricula demonstrate a clear trend toward strengthening the practical component of training, which is realized through several groups of disciplines:

1. Microcontrollers and microprocessor systems, forming the foundation for understanding hardware architecture and low-level programming.
2. Embedded and cyber-physical systems, focusing on the development of computing systems integrated into complex physical environments.
3. Internet of Things and network infrastructure, combining sensor technologies, data transmission, and cloud-based data processing.
4. Specialized hardware design and systems-on-chip, aimed at training advanced specialists capable of developing custom hardware solutions.

The quality of Computer Engineering education critically depends on the state of the laboratory infrastructure. Consequently, university laboratories are gradually

transforming from traditional computer classrooms into specialized engineering hubs and FabLabs. At the introductory level, rapid prototyping platforms such as Arduino and ESP8266/ESP32 are widely used, enabling students to obtain visible results quickly and thereby increasing learning motivation.

At more advanced stages, professional training involves development boards based on STM32 microcontrollers (Nucleo and Discovery series), as well as single-board computers such as Raspberry Pi and BeagleBone. A high level of practical competence is further supported by the use of FPGA development boards (e.g., Terasic DE10-Nano, Altera Cyclone, Xilinx Artix). Industrial automation is studied using Siemens Simatic and Festo training stands. Essential measuring equipment includes digital oscilloscopes, logic analyzers, and signal generators.

The software component encompasses the full development toolchain for embedded systems, including integrated development environments (VS Code with PlatformIO, STM32CubeIDE, Keil uVision), electronic design automation tools (Altium Designer, KiCad), version control and CI/CD systems (Git, Jenkins), and programming languages such as C/C++, Python, and Java/Kotlin.

In conditions of armed conflict, frequent air raid alerts, and limited access to university facilities, Ukrainian HEIs are increasingly adopting hybrid learning models, where the concept of Laboratory as a Service (LaaS) plays a central role. One of the primary adaptation mechanisms is the use of virtualization technologies and digital twins. Extensive use of software simulators partially compensates for the lack of physical access to laboratory equipment, including Cisco Packet Tracer for networking, Proteus and Tinkercad Circuits for electronic design, and Wokwi and QEMU for microcontroller emulation.

Another important approach is the implementation of Lab-at-Home solutions. Several universities (including Odesa Polytechnic, Volodymyr Dahl East Ukrainian National University, and Kharkiv National University of Radio Electronics) provide students with individual hardware kits, such as Arduino Starter Kits or Raspberry Pi Zero devices, for the duration of a semester. This approach allows laboratory work to be completed safely and independently of campus access schedules.

The most technologically complex but highly effective solution is the organization of remote access to physical laboratory equipment. In this model, educational stands are deployed in laboratories and accessed by students via VPN or SSH. Students upload code to real controllers and observe system behavior through live video streams. However, such laboratories require reliable uninterruptible power supplies and automated system recovery mechanisms to ensure continued operation during power outages.

Conclusions

To ensure the quality and continuity of Computer Engineering education under martial law and blended learning conditions, several strategic development directions must be prioritized. First, the modernization of laboratory infrastructure must be accompanied by measures aimed at energy autonomy. Remote laboratories should

function as energy-resilient units equipped with backup power systems and alternative communication channels.

Second, inter-university resource sharing should be strengthened through the creation of unified digital hubs, enabling students from temporarily displaced or damaged institutions to access unique equipment hosted by other universities.

Third, curricula should incorporate dual-use technologies, ensuring that future IoT engineers understand the specific requirements and constraints of military and security-related applications. Finally, cybersecurity remains a critical component of IoT education. Training programs must include mandatory modules on secure boot mechanisms, the use of secure elements, and firewall and VPN configuration. These competencies are essential not only for protecting critical infrastructure but also for preventing the misuse of university systems in cyberattacks.

Overall, the analysis demonstrates that Ukrainian universities exhibit a high degree of resilience and adaptability, successfully adjusting bachelor's programs in Computer Engineering to extremely challenging conditions.

REFERENCES

[1] "Kompiuterni systemy ta merezhi. Osvitno-profesiini prohramy pershoho (bakalavrskoho) rivnia vyshchoi osvity". Natsionalnyi tekhnichnyi universytet Ukrainy «Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho». [Online]. Available: https://osvita.kpi.ua/F7_OPPB_KSM

[2] "Systemne prohramuvannia ta spetsializovani kompiuterni systemy. Osvitno-profesiini prohramy pershoho (bakalavrskoho) rivnia vyshchoi osvity". Natsionalnyi tekhnichnyi universytet Ukrainy «Kyivskyi politekhnichnyi instytut imeni Ihoria Sikorskoho». [Online]. Available: https://osvita.kpi.ua/F7_OPPB_SPSKS

[3] "Osvitni prohramy". Kafedra intelektualnykh kibernetychnykh system. Derzhavnyi universytet «Kyivskyi aviatsiinyi instytut». [Online]. Available: https://ccs.nau.edu.ua/napryami-pidgotovki/opp

[4] "Spetsialnist F7 Kompiuterna inzheneriia | KhNURE - Kharkivskyi natsionalnyi universytet radioelektroniky". NURE. [Online]. Available: https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-f7-komp-iuterna-inzheneriia

[5] "Polozhennia, standarty, OPP i navchalni plany". Kafedra informatsiinykh tekhnolohii ta kompiuternoi inzhenerii. Natsionalnyi tekhnichnyi universytet "Dniprovska politekhnika". [Online]. Available: https://it.nmu.org.ua/ua/edu_ped_work/OKX_OPP_edu_plans.php

[6] "Osvitni prohramy LNTU". Kafedra kompiuternoi inzhenerii ta bezpeky. Lutskyi natsionalnyi tekhnichnyi universytet. [Online]. Available: https://lntu.edu.ua/uk/studentu-0/navchannya/osvitniy-programi?field_fakultet_op_target_id=All&field_kafedra_op_target_id=All&field_osvitniy_stupin_op_target_id=All&field_rik_op_target_id=All&field_spetsialnist_op_target_id=2161&field_osvitnya_prohrama_op_target_id=All

[7] "Osvitni prohramy". Natsionalnyi universytet "Chernihivska Politekhnika". [Online]. Available: https://op.stu.cn.ua/view/total_view.php

[8] "Osvitni prohramy:: Kafedra Kompiuternoi inzhenerii :: Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii". Derzhavnyi universytet informatsiino-komunikatsiinykh tekhnolohii. [Online]. Available: https://duikt.edu.ua/ua/1824-osvitni-programi-kafedra-kompyuternoi-inzhenerii

[9] "Sait kafedry". Kafedra kompiuternoi inzhenerii ta elektroniky. Kremenchutskyi natsionalnyi universytet imeni Mykhaila Ostrohradskoho. [Online]. Available: https://cee.kdu.edu.ua/

[10] "OPP. Bakalavrskyi riven. 123 Kompiuterna inzheneriia / F7 Kompiuterna inzheneriia". luguniv.edu.ua. [Online]. Available: https://luguniv.edu.ua/?page_id=61087

[11] “Sait kafedry kompiuternykh system ta merezh”. Kryvorizkyi natsionalnyi universytet (KNU). [Online]. Available: http://www.ksm.knu.edu.ua/
[12] “Skhidnoukrainskyi natsionalnyi universytet imeni Volodymyra Dalia.” Navchalni resursy u systemi Moodle. [Online]. Available: http://moodle2.snu.edu.ua/course/view.php?id=3953
[13] “Kompiuterni systemy ta merezhi”. Natsionalnyi universytet «Odeska politekhnika» Osvita. Nauka. Profesionalizm. [Online]. Available: https://op.edu.ua/education/programs/bac-123-2

JUSTIFICATION OF THE CRITERIA FOR ASSESSING THE INTERFERENCE IMMUNITY OF COHERENT RECEPTION OF SIGNALS WITH MULTI-POSITION PHASE MANIPULATION IN THE PRESENCE OF IMPULSE NON-FLUCTUATIONAL OBSTACLES

Oleksandr Turovsky (Professor)[1]
Oleksandr Drobyk, (PhD, Associate Professor)[2]
Nazarii Blazhennyi (PhD, Associate Professor)[3]
Tetiana Meleshko (PhD, Associate Professor**)**[4]
Yevhen Bondarenko (Postgraduate)[5]

[1,2,3,4,5] State University of Information and Communication Technologies, Kyiv, Ukraine
[1] Department of Technical Cyber Defense Systems
[2] Educational and Scientific Institute of Telecommunications
[3] Department of Mobile and Video Information Technologies
[4] Department of Mobile and Video Information Technologies
[5] Department of Technical Cyber Defense Systems

[1] s19641011@ukr.net, [2]odrobik@ukr.net, [3] blasennij@ukr.net,
[4] sorokunnet@ukr.net, [5] bondarenko.alfa.inet@gmail.com

Abstract

The article considers a new scientific problem regarding the appropriate method for estimating the noise immunity of coherent reception of signals with multiple position phase changes in the presence of pulsed random interference.
The rule for determining the noise immunity of coherent reception of signals with multiple position phase changes in the presence of non-fluctuating interference is defined and substantiated, and the signal error probability is proposed. The structure of the model for calculating the noise immunity of coherent reception of signals with multiple positions with phase manipulation in the presence of pulsed random interference is described and illustrated. The proposed model is derived from the probability of symbol and bit errors in a signal with multiple positions relative to the permissible level of impulse noise in the presence of different levels of the signal/noise ratio at the input of the coherent receiver.

Keywords: noise immunity, pulsed non-fluctuating interference, signals with multi-position phase manipulation.

Introduction

The conflict between increasing the efficiency of discrete signal transmission in the context of ever-increasing requirements for efficiency and noise immunity, while maintaining a high degree of spectral resolution, requires the search for new data transmission methods.

Among the entire list of existing technologies for digital transmission of important data in modern telecommunication networks, the importance of signal transmission technologies that have several phases of phase control should be recognized [1].

Increasing the efficiency of the use of telecommunication networks based on signal transmission technology with several involved positions is directly related to limitations and harmful processes that negatively affect the speed of digital data transmission, their volume and the reliability of received signals, which is associated with noise immunity. Obviously, one of the negative processes is the influence of interference and interference that prevent a significant increase in the efficiency of telecommunication networks due to a decrease in signal noise immunity and the loss of part of the corresponding data during transmission by the input device of the telecommunication network.

One example of this is a certain number of interferences that are disruptive and vary in size, which is considered non-fluctuating. One of the largest is the total number of chaotic impulse non-resonant interferences. One of their main characteristics is the lack of periodicity in action, which is due to the input signal of the path, which receives non-periodic single-pulse signals from radio sources of various types [2,3].

The purpose of the research. The presence of aperiodic waves in the receiving path of processing input signals of a telecommunication network based on multi-position phase shift keying technology creates a new scientific task of assessing the noise immunity of coherent signal reception in the presence of pulsed non-fluctuating interference of various types.

Research results

A signal with multiple positions in phase shift keying has a possible value *M* at the time of the clock interval T [2,3].

The classical receiver of the correlation signal of the form in the presence of white Gaussian noise operates on the basis of calculating the convolution integrals I, the oscillations of the input signal x(t) and M additional signals [2,4].

For the reliability of the analysis, we assume that the coherent receiver has an accurate phase and one synchronization marker.

Correct decoding of the j-th channel symbol is related to the condition where: $p(I_j > I_i)$ – the probability of transmitting the jth symbol is greater than the probability of transmitting the other symbols in the ith set [1,5].

It should be taken into account that all prior probabilities of the channel symbols are equal, and the symmetry of the signal constellation with respect to

position is also the same. This will facilitate the determination of the overall probability of successful signal acquisition. P_s, as the probability of receiving a signal with index "0" . Further, the probability of a symbol error during the reception of a channel symbol is identical.

Let us assume that the input of a coherent receiver contains both the desired signal and white Gaussian noise *n(t).* In addition, there are non-fluctuating interferences $s_n(t)$ (Fig. 1) [6].

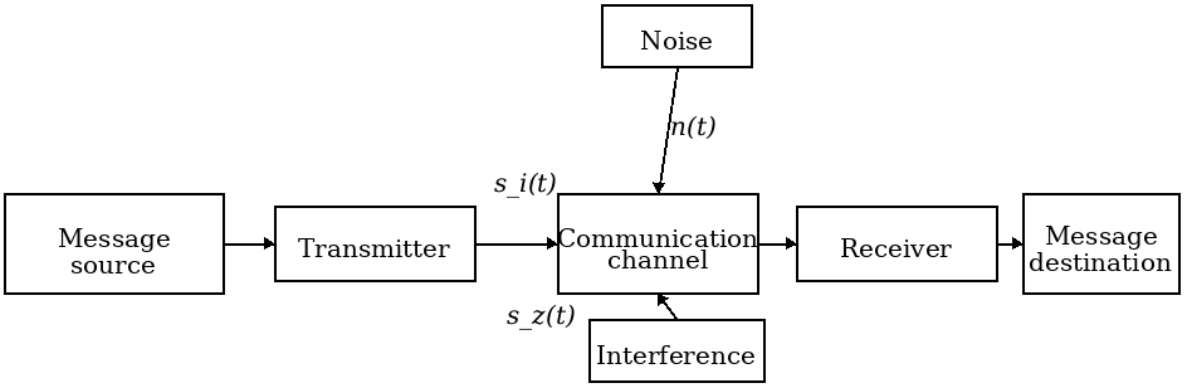


Fig. 1. Structural diagram of a data transmission system in a telecommunication network based on multi-position phase shift keying technology

The choice of criterion for measuring the impact of impulse non-fluctuating interference $s_n(t)$ on the noise immunity of the signal will be based on measuring the average value of non-fluctuating interference.

The process, which is included in the functional dependence of the convolution integrals of the input oscillation *x(t),* and M reference signals, is defined in the form [1,4]:

$$x(t) = s_i(t) + s_n(t) + n(t)$$

We fix the initial phase φ_n of the interference vector $s_n(t)$.

Then we will assume the total vector $s_i(t) + s_n(t)$ to be conditionally deterministic, but the processes I_i at the outputs of the demodulator correlators will be random.

Due to Gaussian noise, their distribution is normal.

Once these calculations are complete, it is easy to determine the conditional probability of error, for example, using the parameter Due to Gaussian noise, their distribution is normal.

Once these calculations are complete, it is easy to determine the conditional probability of error, for example, using the parameter . This is included in expression.

Next, we define the conditional probabilities of symbol and bit errors $P_{eb}(\varphi_n)$.

To obtain the unconditional probability of a bit error, it is necessary to average the obtained results. $P_{eb}(\varphi_n)$ by random variable φ_n:

$$P_{eb} = \frac{1}{2\pi}\int_{-\pi}^{\pi} P_{eb}(\varphi_n) d\varphi_n$$

As a result, based on the interdependence of bit and symbol errors, expression (5), which is the main criterion for determining the degree to which non-fluctuating interference affects the stability of a signal with several positions in its phase, we choose the symbol error probability, expression (9). It is impossible to derive an exact formula for the error probability, therefore, numerical averaging is used to obtain the final result.

Conclusions

The paper considers a new scientific problem regarding the appropriate method for estimating the noise immunity of coherent reception of signals with multiple position phase changes in the presence of non-fluctuating interference.

1. The rule for determining the noise immunity of coherent reception of signals with multiple position phase changes in the presence of non-fluctuating interference is defined and substantiated, and then the probability of signal error is proposed.

2. The methodology for calculating the threshold of auditory noise immunity relative to multiple position phase changes in the presence of stationary interference is developed and demonstrated.

3. The proposed model is derived from the probability of symbol and bit error in a signal with multiple positions relative to a typical level of non-fluctuating interference for different values of the signal-to-noise ratio at the input of the coherent receiver.

REFERENCES

[1] Balashov, V. O., Vorobienko, P. P., Lyakhovetskyi, L. M., & Pedyash, V. V. (2012). *Broadband signal transmission systems*. Ed. ONAZ center named after O. S. Popova.

[2] Popivskyi, V. V., Lemeshko, O. V., Kovalchuk, V. K., Plotnikov, M. D., & Kartushyn, Yu. P. (2012). *Telecommunication systems and networks: Structure and main functions* (Vol. 1). http://www.znanius.com/3534.html

[3] Zaitsev, S. V. (2011). A mathematical model of a communication channel with OFDM signals and intentional interference. *Mathematical Machines and Systems, (4)*, 166–175. http://dspace.nbuv.gov.ua/handle/123456789/83639

[4] Steklov, V. K., Berkman, L. N., & Kilchytskyi, E. V. (2004). *Optimization and modeling of communication devices and systems*. Technika.

[5] Saiko, V. G., & Amirkhanov, E. D. (2015). *Basics of new generation digital radio communication and radio access networks*. DUT.

[6] Shahtarin, B. I., Kazakov, L. N., & Kalashnikov, K. S. (2014). *Communication systems with orthogonal frequency channel division*. Hotline–Telecom.

[7] Palagin, V. V. (2015). Models and methods of signal processing when interacting with correlated non-Gaussian noise. *Electronic Modeling, 37*(6), 19–34.

[8] Prokofiev, M., Kulish, V., Vashchenko, M., Dvorsky, V., et al. (2015). Evaluation of the quality coefficient of noise interference in active information protection systems. *Legal, Regulatory and Metrological Support of the Information Protection System in Ukraine, 1*(29), 11–20.

PREDICTIVE CLOUD LOAD BALANCING MODEL BASED ON BEHAVIORAL AND DYNAMIC CHARACTERISTICS OF NODES FOR IOT WORKLOADS

Vitalii ALKEMA[1]
Maksym KALASHNYK[2]
Oleh SHKLYAR[3]

[1,2,3]*State University Kyiv Aviation Institute (KAI)*
[1] vitalii.alkema@gmail.com, [2] e-mail: 294776@stud.kai.edu.ua, [3] oleh.shklyar@gmail.com

Анотація

У роботі розглядається проблема ефективного розподілу динамічних та стохастичних навантажень Інтернету речей (IoT) у хмарних середовищах. Традиційні реактивні методи балансування, що базуються на миттєвих показниках використання ресурсів, часто не здатні своєчасно реагувати на різкі сплески трафіку, що призводить до короткочасних перевантажень та зниження якості обслуговування (QoS). Для вирішення цієї проблеми запропоновано модель предиктивного балансування навантаження, яка враховує поведінкові та динамічні характеристики обчислювальних вузлів. На відміну від підходів, орієнтованих на миттєвий стан («зріз»), запропонований метод оцінює вузли на основі часових ознак: трендів навантаження, швидкості змін, варіабельності та короткострокових прогнозів. Використання прогнозної оцінки придатності вузла дозволяє виконувати проактивний розподіл запитів, запобігаючи виникненню перевантажень. Запропонований підхід підвищує стабільність системи та оптимізацію ресурсів в умовах пікових навантажень IoT.

Ключові слова

обчислення на периферії, подієво-орієнтована архітектура, виявлення аномалій, контекстуальна обробка, прийняття рішень у реальному часі, хмарні обчислення, Інтернет речей (IoT), балансування навантаження, інтегральний індекс, прогнозування, LSTM, нейронна мережа, оптимізація ресурсів, час відгуку, стохастичний трафік, QoS, маршрутизація.

Abstract

This paper addresses the challenges of managing dynamic and stochastic Internet of Things (IoT) workloads in cloud environments. Traditional reactive load balancing strategies, which rely on instantaneous resource metrics, often fail to respond adequately to rapid traffic fluctuations, resulting in transient overloads and QoS degradation. To overcome these limitations, we propose a predictive cloud load balancing model that incorporates the behavioral and dynamic characteristics of computing nodes. Unlike snapshot-based approaches, the proposed method evaluates nodes based on temporal features, including load trends, rate of change, variability, and short-term forecasts. By calculating a predictive suitability score, the model enables proactive request redistribution, effectively preventing potential overloads. The proposed approach enhances system

stability and resource optimization, ensuring robust performance under bursty IoT traffic conditions.

Keywords
edge computing, event-driven architecture, anomaly detection, contextual processing, real-time decision-making, cloud computing, Internet of Things (IoT); load balancing, integral index, forecasting, LSTM, neural network, resource optimization, response time, stochastic traffic, QoS, routing.

Introduction

IoT-generated workloads are inherently dynamic, stochastic, and bursty, often characterized by short-term peaks and abrupt changes in request intensity [3, 11]. These properties pose serious challenges to maintaining stable performance and quality of service (QoS) in cloud environments.

Traditional cloud load balancing mechanisms are predominantly reactive and rely on instantaneous resource utilization metrics such as CPU load, memory usage, or network throughput [6, 9]. While such approaches are simple and widely adopted, they often fail to respond adequately to rapid workload fluctuations typical of IoT systems [10]. As a result, cloud nodes may experience transient overloads, increased response latency, and degradation of service reliability before balancing decisions take effect.

To address these limitations, predictive load balancing has emerged as a promising direction, enabling proactive decision-making based on short-term workload forecasting [1, 5]. However, many existing predictive approaches focus solely on forecasting individual resource metrics or aggregate load values, without considering the behavioral dynamics of cloud nodes over time [2, 4]. In practice, nodes with similar instantaneous utilization levels may exhibit significantly different future behavior due to differences in workload trends, variability, and temporal stability.

In this work, we propose a predictive cloud load balancing model that explicitly incorporates behavioral and dynamic characteristics of cloud nodes when handling IoT workloads [7, 8]. Instead of relying solely on current resource measurements, the proposed approach models node behavior through temporal features such as load trends, rate of change, variability, and short-term forecasts. This enables the load balancer to anticipate potential overload conditions and perform preventive request redistribution.

The main objective of this study is to enhance the adaptability and robustness of cloud load balancing under highly dynamic IoT traffic conditions by shifting from reactive, snapshot-based decision-making to behavior-aware predictive control.

Main material

Consider a cloud infrastructure consisting of a set of computing nodes

$$\mathcal{N} = \{n_1, n_2, \dots, n_K\},$$

each providing computational resources to process incoming IoT-generated service requests.

Each node n_i is characterized at time t by a vector of monitored resource metrics:
$\mathbf{R}_i(t) = (c_i(t), m_i(t), d_i(t), b_i(t)),$

where $c_i(t)$ denotes CPU utilization, $m_i(t)$ memory usage, $d_i(t)$ disk activity, and $b_i(t)$ network load.

IoT workloads generate a stream of requests with time-varying arrival rates, leading to non-stationary load patterns. The key challenge is to assign incoming requests to cloud nodes in such a way that:

- overload situations are prevented,
- response latency is minimized,
- and resource utilization is balanced over time [4].

Unlike traditional approaches, which base decisions on instantaneous values of $\mathbf{R}_i(t)$, we aim to incorporate **behavioral and dynamic characteristics** of nodes derived from temporal observations of resource usage [7].

Behavioral and Dynamic Characterization of Nodes

To capture node behavior, we introduce a behavioral state representation based on temporal analysis of resource metrics. For each node n_i, the following characteristics are considered over a sliding time window:

- **Load trend** – direction and magnitude of resource usage change;
- **Rate of change** – first-order derivative of the aggregated load;
- **Variability** – variance or dispersion of resource metrics;
- **Short-term forecast** – predicted load level in the near future;
- **Stability indicator** – resistance to sudden workload fluctuations.

These features jointly describe how a node behaves over time rather than how it appears at a single moment. Nodes exhibiting rapidly increasing load or high variability are treated as less favorable candidates for future request assignment, even if their current utilization is moderate.

Predictive Load Balancing Model

Based on the extracted behavioral characteristics, a predictive model is employed to estimate the near-future load state of each node [1, 5]. The predicted state is then used by the load balancer to perform **preventive request allocation**, avoiding nodes that are likely to become overloaded.

The decision-making process follows three main steps:

1. Continuous monitoring and aggregation of node resource metrics.
2. Behavioral state estimation and short-term load prediction.
3. Proactive load balancing based on predicted node suitability.

This approach allows the system to react *before* performance degradation occurs, which is particularly important in IoT scenarios with sudden traffic bursts [11].

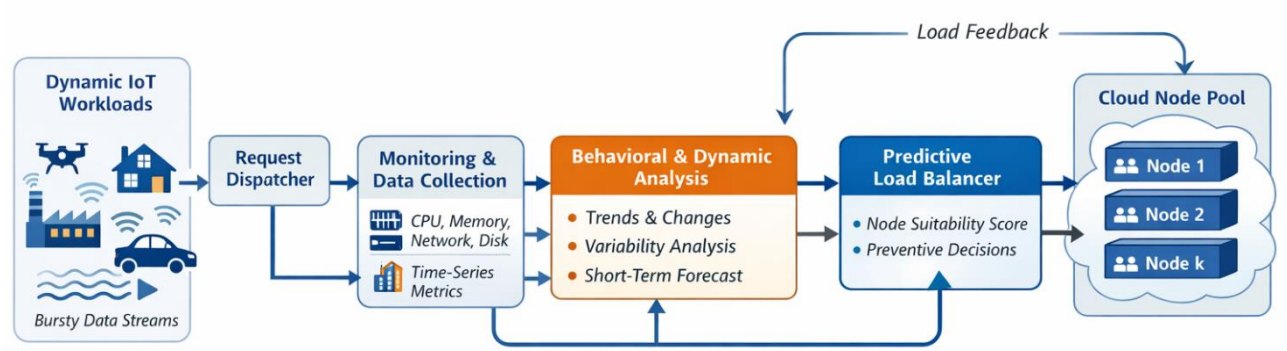


Fig 1. the architecture of the proposed predictive cloud load balancing model designed for dynamic IoT workloads.

Figure 1 illustrates the architecture of the proposed predictive cloud load balancing model designed for dynamic IoT workloads. Incoming IoT requests are first received by the request dispatcher, which serves as an entry point to the cloud infrastructure. The dispatcher forwards requests to the monitoring and data collection module, where time-series resource metrics of cloud nodes, including CPU utilization, memory usage, network load, and disk activity, are continuously collected.

Based on the monitored data, a behavioral and dynamic analysis module extracts temporal characteristics of node operation, such as workload trends, rate of change, variability, and short-term load forecasts. These characteristics provide a behavioral representation of node states, capturing not only their instantaneous resource utilization but also their expected future behavior.

The extracted behavioral features are then supplied to the predictive load balancer, which computes a node suitability score reflecting the anticipated load conditions in the near future. Using this predictive assessment, the load balancer performs preventive request allocation, avoiding nodes that are likely to experience overload and favoring those with more stable and predictable behavior.

Finally, requests are assigned to the cloud node pool, consisting of multiple computing nodes. Feedback on actual load conditions is continuously returned to the monitoring module, enabling iterative refinement of behavioral analysis and predictive decisions. This closed-loop architecture allows the proposed model to proactively adapt to dynamic IoT traffic patterns and maintain balanced resource utilization across the cloud infrastructure.

REFERENCES

[1] Zhang B et al. SWT-CLSTM: A hybrid model for cloud workload prediction combining smooth wavelet transform and contrastive learning. Journal of King Saud University Computer and Information Sciences. 2025. 37. DOI: 10.1007/s44443-025-00316-8.

[1] Batahari M. et al. Dynamic Load Balancing in Cloud Computing Using Machine Learning. Conference: 3rd International conference on business analytics for technology and security. 2025.

[2] Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. Vol. 29(7). P. 1645–1660.
[3] Lilhore U.K. et al. A multi-objective approach to load balancing in cloud environments integrating ACO and WWO techniques. Scientific Reports. 2025. Vol. 15, 12036. DOI: 10.1038/s41598-025-96364-1.
[4] Bansal S., Kumar M. Deep Learning-based Workload Prediction in Cloud Computing to Enhance the Performance. Third International Conference on Secure Cyber Computing and Communication (ICSCCC). 2023. DOI: 10.1109/ICSCCC58608.2023.10176790Corpus
[5] Kunwar V. et al. Load Balancing in Cloud — A Systematic Review. Advances in Intelligent Systems and Computing. 2018. DOI: 10.1007/978-981-10-6620-7_56.
[6] Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context-aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials. 2014. Vol. 16(1). P. 414–454.
[7] Shklyar O.I., Balanyuk Y.V., Kudrenko S.O. Load balancing and cloud node resilience enhancement algorithm based on predicted integral index. Problems of informatization and management. Vol. 3 (83). KAI. 2025. DOI: 10.18372/2073-4751.83.20512
[8] Ameen J.N., Begum S.J. Evolutionary Algorithm Based Adaptive Load Balancing (EA-ALB) in Cloud Computing Framework. Intelligent Automation & Soft Computing. 2022. 34(2). P. 1281-1294. DOI: 10.32604/iasc.2022.025137.
[9] Ranesh Naha R. et al. Deadline-based dynamic resource allocation and provisioning algorithms in Fog-Cloud environment. Future Generation Computer Systems. 2019. 104. DOI: 10.1016/j.future.2019.10.018.
[10] Akkad M., Döllner J. Event-driven architectures for real-time IoT systems. Procedia Computer Science. 2021. Vol. 184. P. 208–215.

INTERFERENCE IMMUNITY OF MIMO SYSTEMS UNDER DIFFERENT PROBABILITY DISTRIBUTIONS OF FADING

Olha MARCHUK (Postgraduate student)[1]
Vladyslav HERASYMCHUK (Postgraduate student)[2]

[1]State University of Information and Communication Technologies, Department of Telecommunication Systems and Networks: olamarchuk11@gmail.com
[2]State University of Information and Communication Technologies, Department of Telecommunication Systems and Networks: l3urius@gmail.com

Summary

This study presents a comparative analysis of diversity signal processing methods in MIMO communication systems [1, p. 32] under Rayleigh and truncated normal fading conditions using computer simulation with QPSK modulation. By transmitting one million symbols and evaluating signal-to-noise ratios and bit error probabilities, the interference immunity of different combining algorithms was assessed. The results show that truncated normal fading leads to a significantly higher error probability compared to Rayleigh fading, requiring a larger fading margin in communication system design. It is also demonstrated that the suboptimal signal combining method effectively reduces the bit error rate when the signal-to-noise ratios in the diversity channels are unequal, confirming its practical efficiency for MIMO systems operating under non-uniform channel conditions.

Main part of the work

To determine the gain of a particular method for processing diversity signals, their comparison was carried out by means of computer simulation of two diversity channels with QPSK modulation under Rayleigh and truncated normal fading probability distributions. The experimental plan consisted of transmitting 1,000,000 symbols and calculating the resulting signal-to-noise ratio for various algorithms for processing two diversity signals with different signal-to-noise ratios, while maintaining a fixed signal-to-noise ratio in one of the channels.

As efficiency criteria for methods of processing diversity signals, it is possible to use the signal-to-noise ratio level and the error probability [2, p. 5], based on experimental and theoretical determination of the error probability, to assess the interference immunity of MIMO communication systems under different probability distributions of fading. This required a large amount of experimental and computational work.

Let us consider a simulation algorithm for signal processing in two diversity channels under different probability distributions of fading. Such an algorithm makes it possible, using a computer, to calculate the signal-to-noise ratio for various signal processing algorithms, for example, under Rayleigh and truncated normal fading distributions. The developed algorithm is shown in Fig. 1.

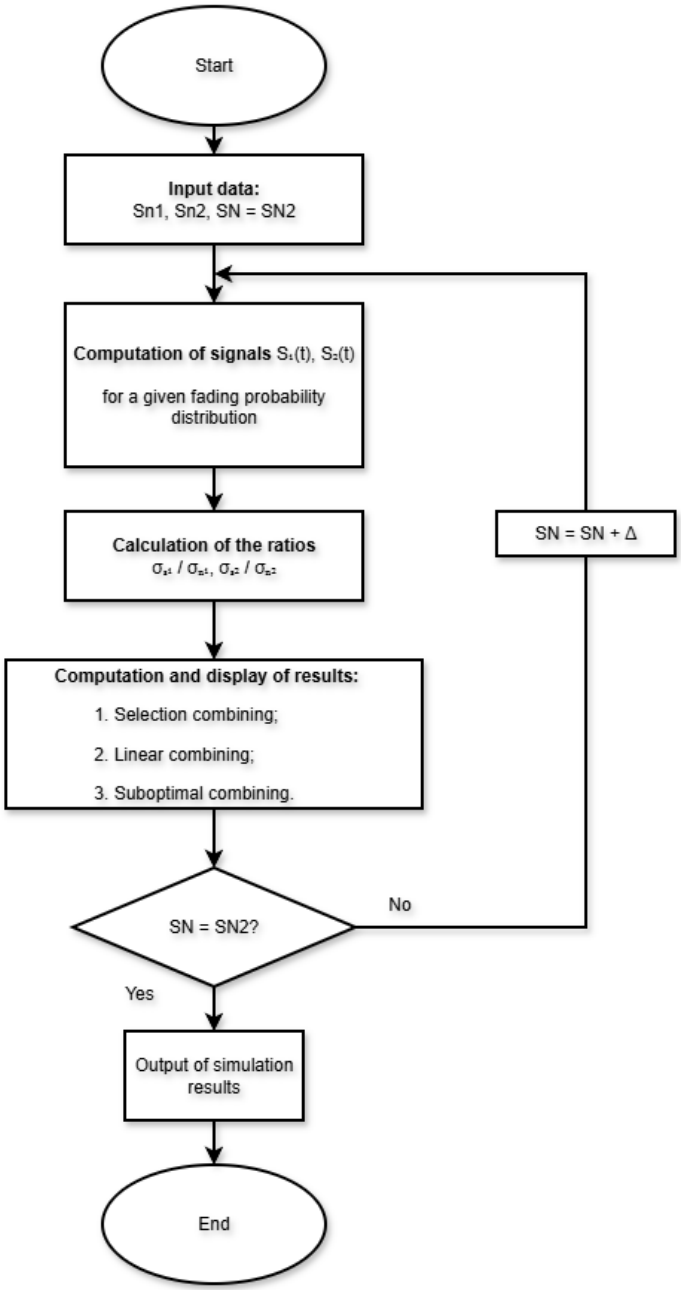


Fig. 1. Algorithm for comparing signal processing methods in MIMO systems under different probability distributions of fading

Fig. 2 presents the experimentally obtained error probabilities for the truncated normal fading distribution. Comparing these results, it can be noted that for the truncated normal fading distribution the error probability is almost an order of magnitude higher than the error probability for Rayleigh fading. This indicates that when designing communication links, it is necessary to account for a larger fading margin than in the Rayleigh fading model.

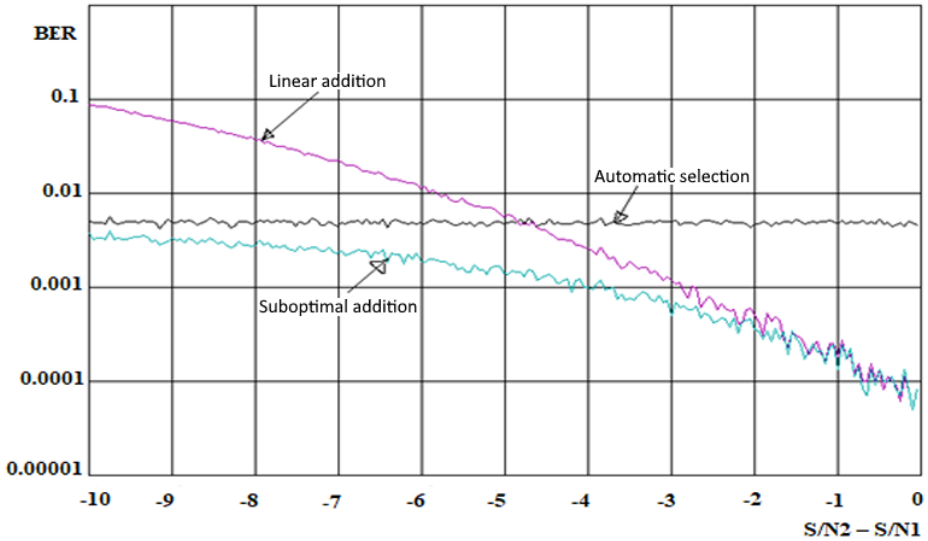


Fig. 2. Error probability for the Rayleigh fading probability distribution model

The analysis of the obtained results showed that the use of the suboptimal MIMO signal combining method is capable of significantly reducing the bit error rate (BER) when there is a difference in the signal-to-noise ratios in the diversity channels.

Conclusion

The conducted simulation-based analysis confirms that the performance of MIMO systems strongly depends on the statistical properties of channel fading and the applied signal combining method. The results demonstrate that truncated normal fading causes a substantially higher error probability than Rayleigh fading [3, p. 3], which necessitates increased fading margins during communication link design. Among the considered processing techniques, the suboptimal combining method shows the best robustness in scenarios with unequal signal-to-noise ratios across diversity channels, providing a significant reduction in bit error rate. Therefore, suboptimal signal combining can be regarded as an effective and practical approach for improving the reliability of MIMO communication systems under realistic and non-ideal fading conditions.

REFERENCES

1. Molisch, A. F. *Wireless Communications*. 2nd ed. Hoboken, NJ: John Wiley & Sons, 2011.
2. Paulraj, A., Nabar, R., Gore, D. *Introduction to Space-Time Wireless Communications*. Cambridge: Cambridge University Press, 2003.
3. Sharma, V., Kumar, P. Performance analysis of wireless fading channels based on Taylor series approximation. *International Journal of Circuit Theory and Applications*, 2021, vol. 49, no. 2, pp. 410–425.

INFORMATION CONCEPT FOR LIVING AND ARTIFICIAL INFORMATION SYSTEMS

Yurii KHLAPONIN (Doctor of Science, Professor)

State University of Trade and Economics, Kyiv, Ukraine
y.khlaponin@gmail.com

Abstract

Based on the combination of knowledge in the field of information technologies and well-known results of biological research, the paper demonstrates that the reproduction of living cells cannot occur without the use of information stored in DNA. The concept of information for living and artificial information systems is formulated as the meaning of a message that does not depend on the form of its representation. Such meaning leads to the execution of specified actions by systems without intelligence or influences, to some extent, decision-making in intelligent systems.

Keywords

Information, information system, DNA, meaning, intelligent systems, cell reproduction.

Introduction

The first step toward defining the concept of information can be considered Norbert Wiener's well-known statement: *"Information is information, not matter or energy."* However, this thesis does not answer the fundamental question: what is information? The difficulty lies in the absence of a clear and universally accepted definition, although the term is widely used in almost all domains of modern science. The purpose of this work is to find an answer to this question and solve existing problems along the way.

Research results

One of the productive approaches to clarifying this concept is the analysis of processes occurring in living cells from the standpoint of the theory of formation of information systems [1]. Living cells represent natural information systems in which information processes can be observed at the molecular level using modern research tools.

The most important of these processes is reproduction. Without it, life would exist for only one generation. Nevertheless, the role of information in reproduction is often not explicitly defined. An attempt to remove this shortcoming was made in a work [4], where elementary operations on information were identified, that is showed in a table 1.

Table 1

Actions that can be performed on information

Name of action on information	Performer of the action
Perception (due to sensitivity)	Information system
Memorization	Information system
Copying	Information system

Storage	Any physical medium
Destruction (partial or complete)	Some physical process
Use in selection procedures	Information system
Accidental distortion	Random physical process
Deliberate distortion	Information system
Transformation (encoding)	Information system
Creation (due to imagination)	Information system
Perception from other systems (through media)	Information system

An explanation of the possibility of combining several functions of information systems in one physical element will be provided after considering the minimum set of properties of these systems, which is presented in Table 2.

Table 2

Minimum properties of an information system

Property designation	Property name	Property description
M (*Memory*)	Memory	Storage of information in a form that allows it to be used to select a particular action
S (*Sensor*)	Sensitivity	Perception of certain characteristics of the external environment
C (*Choice*)	Ability to choose	Ability to choose a particular action depending on the stored information and external factors
E (*Execution*)	Ability	Ability to perform selected actions

In some systems, all these properties are implemented by one physical element.

All information processes that are required for cell division are performed in a certain sequence.

It is well known that in order to copy information, you need to have access to the medium with the information that needs to be copied, as well as the tools to read this information and make a copy of it. This cycle is the basis of life, because without it reproduction cannot occur.

Basic research material

To define information, it is necessary to draw a strict boundary between what is information and what is not. Information always resides on a material carrier. This carrier may possess numerous properties, but only some of them convey information.

A crucial feature of information is that accurate copying to another carrier preserves it completely. Therefore, the principal characteristic of information is its meaning.

From this standpoint, the foundation of cell reproduction should be considered not merely enzyme-accelerated chemical reactions but the information contained in the DNA molecule. This information acts as instructions perceived and executed by cellular mechanisms according to the laws of physics, chemistry, and biology. In the case of living cells capable of division, information is transmitted from the DNA

molecule and is perceived as instructions for performing certain actions by the cell's mechanisms.

For artificial information systems, except an artificial intelligence and neural networks, information also leads to the execution of certain actions. For intelligent systems, information does not necessarily lead to the execution of a certain action. These systems perceive information as a proposal that can influence their decision to perform a particular action. By the presence of intelligence, we will understand the ability to influence the execution of their own actions. In all cases, an information system, receiving messages, instructions, signals, knowledge, etc., must identify their meaning, which is the main characteristic of any information. Further actions of the system depend on its intellectual abilities.

The definition of the concept of information can be summarized as follows:

Information is the meaning of messages that does not depend on the form of their representation, which leads to the execution of certain actions by systems without intelligence, or affects to one degree or another the decision-making on the execution of actions by intelligent systems.

Impossibility of creating information in the absence of information

Information is created by information systems and stored on material carriers until destruction inevitably occurs due to the motion of matter. If all information in the Universe were destroyed, no source for its re-emergence would remain.

Matter and energy are not threatened with disappearance; they do not require self-preservation. Only information is vulnerable. Its preservation is achieved through copying, which in living organisms is performed by mechanisms such as DNA polymerase. Consequently, without life, information would have no chance of continued existence.

Having only matter and energy in the complete absence of information, it is impossible to create an information system, since for this it is necessary to lay down information with a specific meaning. There is no information without meaning, and this meaning is not accidental, but subordinated to the goal of ensuring (or improving the conditions for) the existence of a system of a higher level of the hierarchy. Matter with energy in any combinations are not capable of generating such a goal, and without having a goal, it is impossible to give meaning to the information that is laid down. Only information systems of the highest level of the hierarchy, which can generate and implement their own goals, are capable of this.

The meaning of the results obtained

Information is always placed on a material medium, and the entire material world is in constant motion. Therefore, there is no possibility of eternal storage of information on a specific medium, but thanks to copying, information can be stored for any length of time.

The existence of life can only be explained by the eternity of its existence together with vital information.

Conclusions

Living cells are natural information systems in which information processes can be observed at the molecular level. The most important of these processes is reproduction, without which life would persist for only one generation.

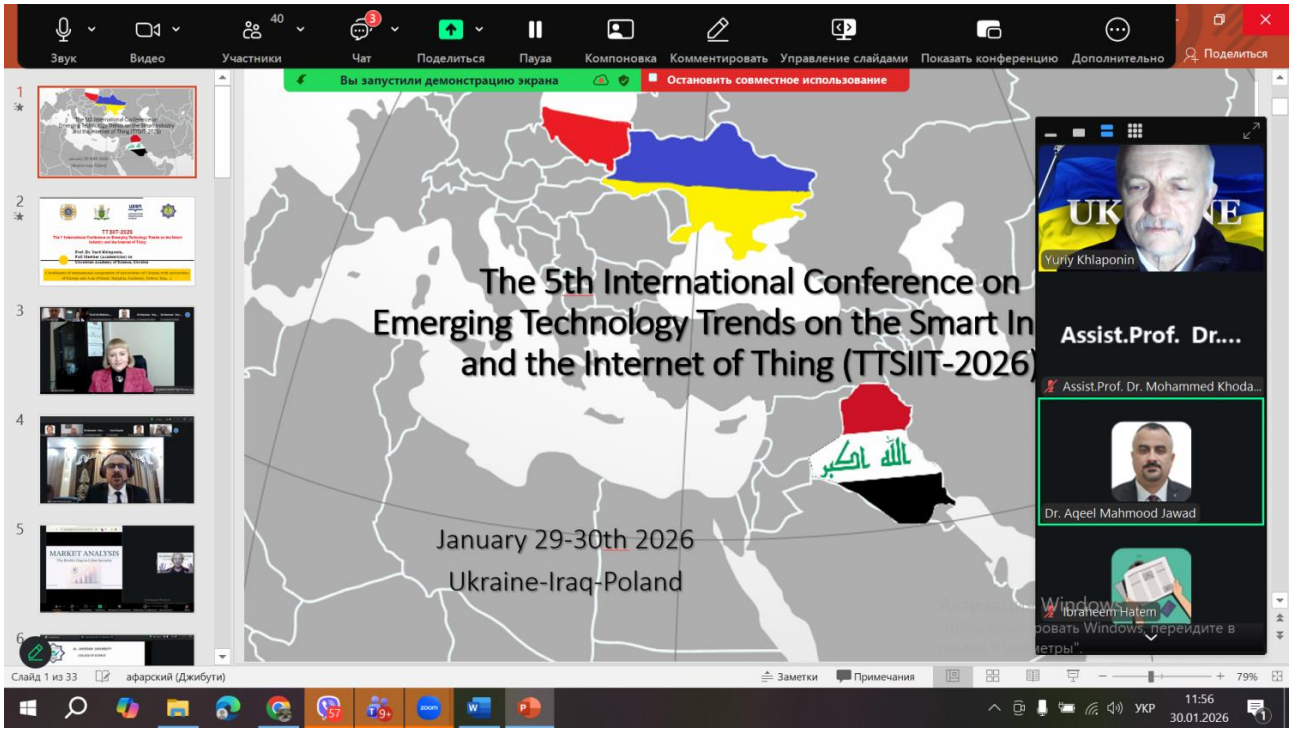
The basis of reproduction is information located on a physical carrier in the form of DNA. This information represents instructions executed by cellular mechanisms. For artificial non-intelligent systems, information can also be treated as instructions for performing actions. For intelligent systems, information may influence decisions rather than determine them directly. Such systems perceive any information as a message that can influence their decisions to one degree or another, along with previous knowledge.

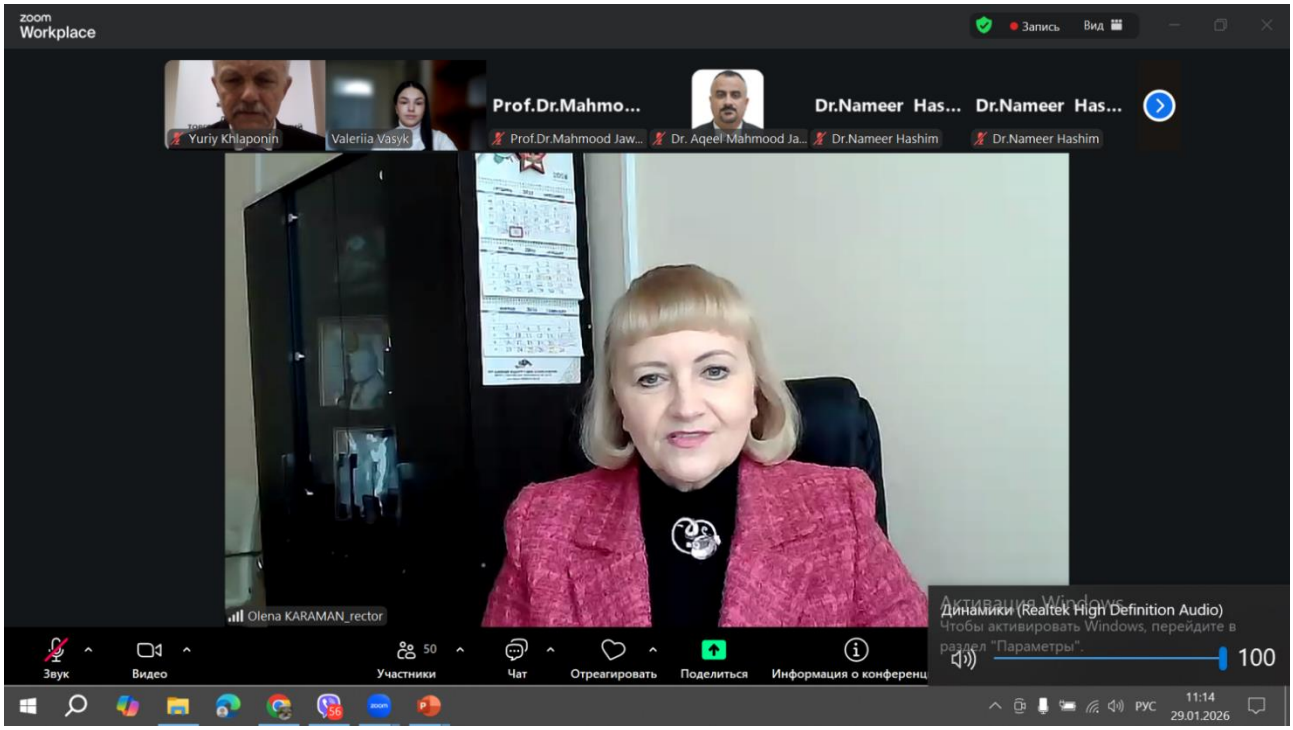
The generalized definition is therefore as follows: **information is the meaning of messages, independent of the form of their representation, which leads to the execution of actions by non-intelligent systems or influences decision-making in intelligent ones.**

REFERENCES

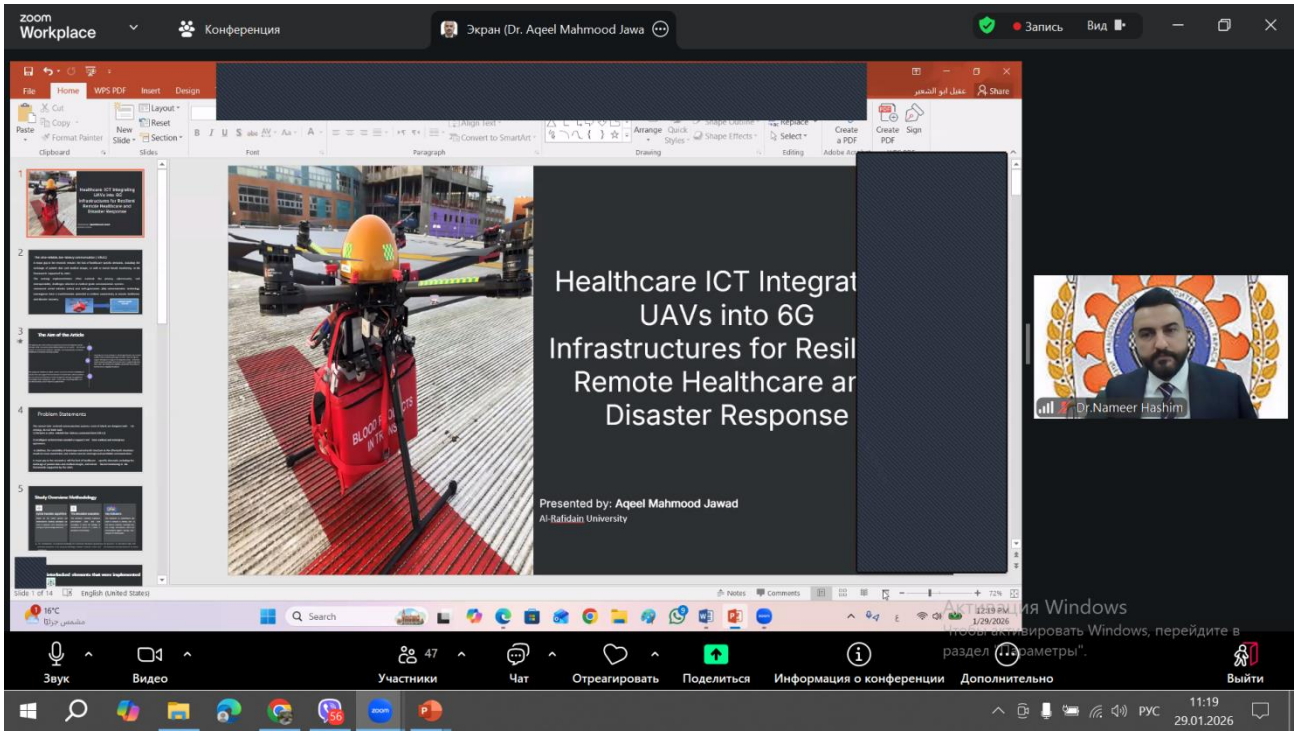
1. Khlaponin, Yu., Vyshniakov, V. *Fundamentals of the theory of formation of information systems*. Smart Technologies, 1(14), 56–61, 2024.
2. Gibson, D.G., Glass, J.I., et al. *Creation of a bacterial cell controlled by a chemically synthesized genome*. Science, 329(5987), 52–56, 2010.
3. Hutchison, C.A., Chuang, R.Y., et al. *Design and synthesis of a minimal bacterial genome*. Science, 351(6280), aad6253, 2016.
4. Vyshniakov, V. *An open path to understanding information and its origin*. Grail of Science, 39, 478–495, 2024.
5. Promoter_(genetics). From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Promoter_(genetics)
6. Genome. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Genome
7. Transfer RNA. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Transfer_RNA
8. Aminoacyl tRNA synthetase. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Aminoacyl_tRNA_synthetase

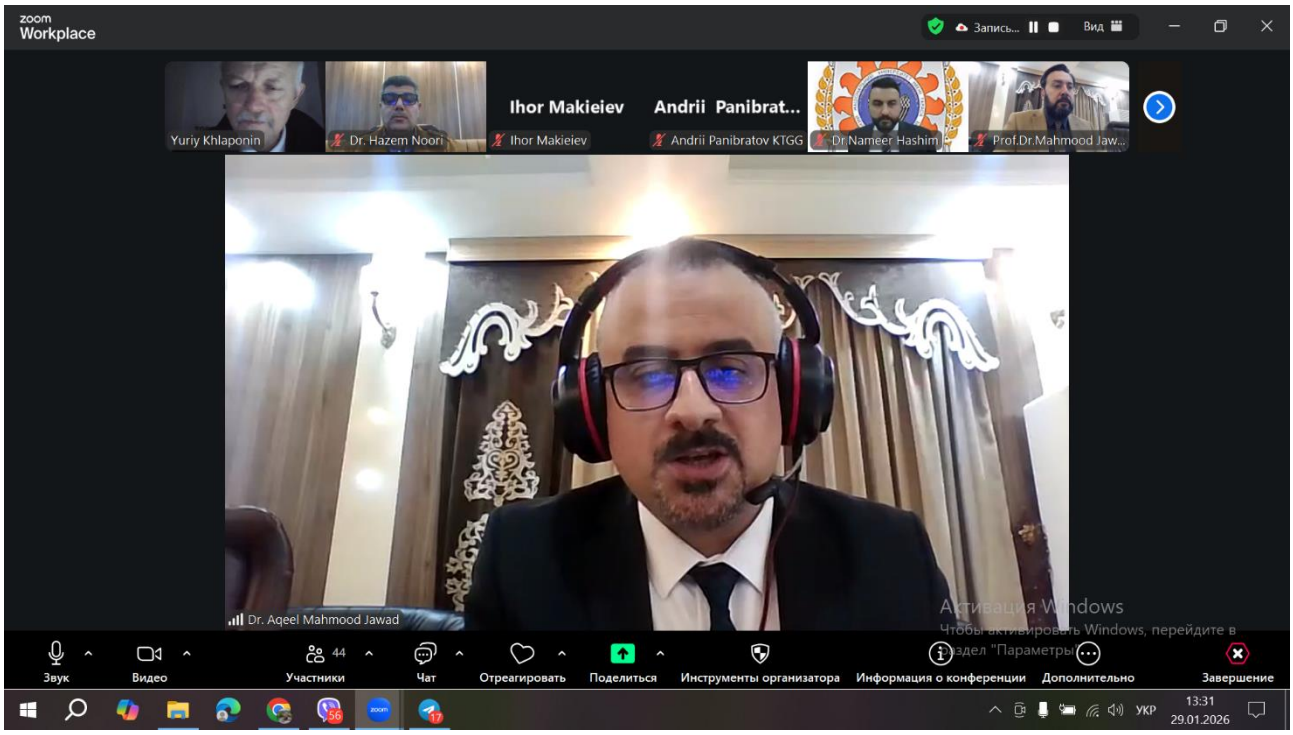
ФОТО З КОНФЕРЕНЦІЇ

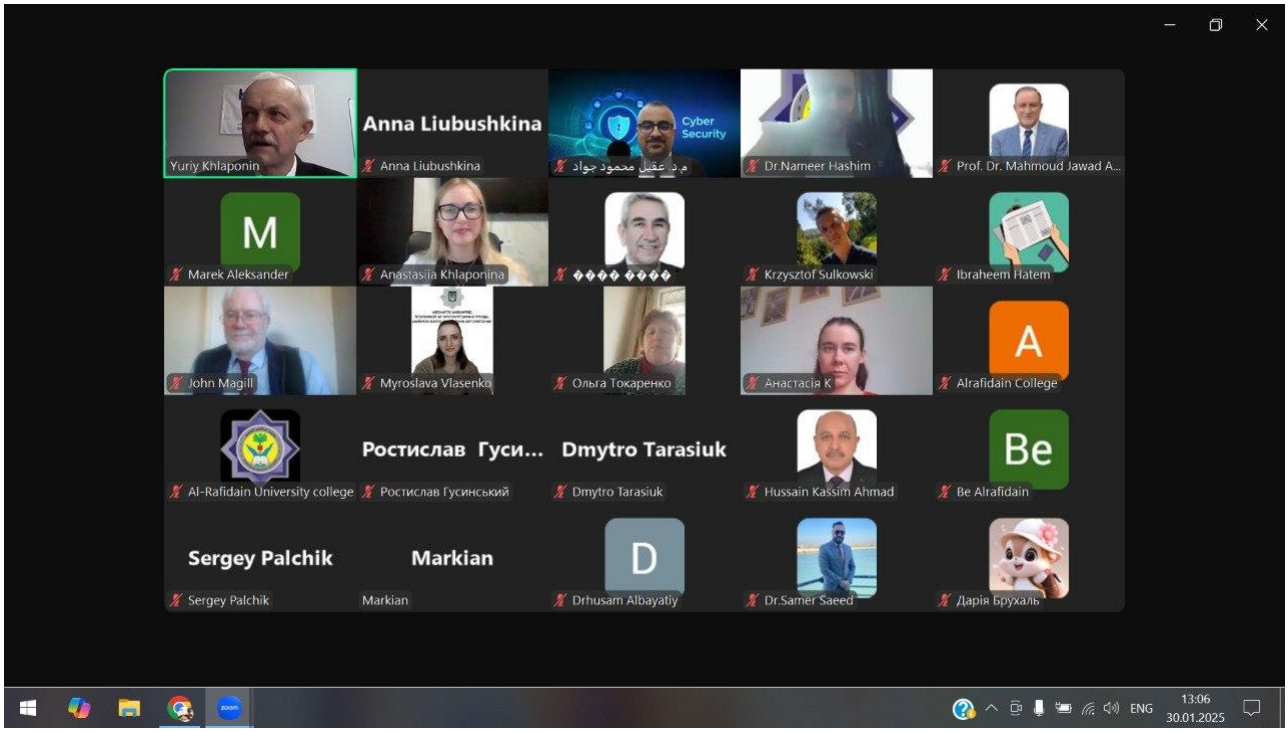



zoom
Workplace
Запись
Вид
Yuriy Khlaponin
Valeriia Vasyk
Prof.Dr.Mahmo...
Prof.Dr.Mahmood Jaw...
Dr. Aqeel Mahmood Ja...
Dr.Nameer Has...
Dr.Nameer Hashim
Dr.Nameer Has...
Dr.Nameer Hashim
Olena KARAMAN_rector
Динамики (Realtek High Definition Audio)
100
Звук
Видео
50
Участники
Чат
Отреагировать
Поделиться
Информация о конференц
РУС
11:14
29.01.2026


zoom
Workplace
Конференция
Экран (Adam Usher)
Запись...
Вид
docs.google.com/presentation/d/1fGBom...
MARKET ANALYSIS
The Reality Gap in Cyber Security
By: Adam Usher
BUSINESS DEVELOPMENT LEAD
Adam Usher
Звук
Видео
49
Участники
Чат
Отреагировать
Поделиться
Инструменты организатора
Информация о конференции
Дополнительно
Выйти
УКР
11:48
29.01.2026


zoom Workplace
Конференция
Экран (Dr. Aqeel Mahmood Jawa
Запись
Вид
Healthcare ICT Integrat
UAVs into 6G
Infrastructures for Resil
Remote Healthcare ar
Disaster Response
Presented by: Aqeel Mahmood Jawad
Al-Rafidain University
Dr.Nameer Hashim
Звук
Видео
Участники
Чат
Отреагировать
Поделиться
Информация о конференции
Дополнительно
Выйти
РУС
11:19
29.01.2026


zoom Workplace
Запись...
Вид
Yuriy Khlaponin
Dr. Hazem Noori
Ihor Makieiev
Andrii Panibrat...
Dr.Nameer Hashim
Prof.Dr.Mahmood Jaw...
Dr. Aqeel Mahmood Jawad
Звук
Видео
Участники
Чат
Отреагировать
Поделиться
Инструменты организатора
Информация о конференции
Дополнительно
Завершение
УКР
13:31
29.01.2026


Yuriy Khlaponin
Anna Liubushkina
Anna Liubushkina
Cyber Security
Dr.Nameer Hashim
Prof. Dr. Mahmoud Jawad A...
Marek Aleksander
Anastasiia Khlaponina
Krzysztof Sulkowski
Ibraheem Hatem
John Magill
Myroslava Vlasenko
Ольга Токаренко
Анастасія К
Alrafidain College
Al-Rafidain University college
Ростислав Гуси...
Ростислав Гусинський
Dmytro Tarasiuk
Dmytro Tarasiuk
Hussain Kassim Ahmad
Be Alrafidain
Sergey Palchik
Sergey Palchik
Markian
Markian
Drhusam Albayatiy
Dr.Samer Saeed
Дарія Брухаль
ENG
13:06
30.01.2025


uken
Uniwersytet Komisji
Edukacji Narodowej
w Krakowie
Certificate
OF PARTICIPATION
THIS CERTIFICATE IS PROUDLY PRESENTED TO
Adam Usher
The 5th International Conference on Emerging Technology Trends in Smart Industry
and the Internet of Things (TTSIIT)
January 29th–30th, 2026
This Conference is Organized By
Al-Rafidain University / Iraq
State University of Trade and Economics / Ukraine
University of the National Education Commission, Krakow / Poland
Luhansk National University
named after Taras Shevchenko / Ukraine
Prof. Dr. Mahmood Jawad Abut Alshaeer
Rector of Al Rafidain University College Republic of Iraq
Dr. Aqeel Mahmood
Organizer
Prof. Dr. Yurii Khloponin
Organizer
Prof. Dr. Olena Karaman
Rector of Luhansk National University
named after Taras Shevchenko

ДЛЯ НОТАТОК

Наукове видання

V Міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”

ТЕЗИ ДОПОВІДЕЙ УЧАСНИКІВ
V Міжнародної науково-практичної конференції “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”
29-30 СІЧНЯ 2026 року

Підписано до друку 30.01.2026. Формат 60x90/16
Ум. друк. арк. 2,5. Обл. вид. 0,9

Видавець і виготовлювач
Державний торговельно-економічний університет
вул. Кіото, 19. Київ, Україна, 02156