Representation Learning at NeurIPS. 2024. arXiv:2410.17787v2.
4. Altman E. et al. Realistic Synthetic Financial Transactions for Anti-Money Laundering Models. *NeurIPS*. 2023. arXiv:2306.16424.

Sustainable information technology for auditable financial anomaly prediction aligned with the EU AI Act, ESG and CSRD standards

UDK 004.8:502.131.1]:657.6:[341.171:061.1EU]

Mykola Zlobin[1]

[1]Chernihiv Polytechnic National University, [1]mykolay.zlobin@gmail.com

The digital transformation of EU financial institutions requires a shift from experimental AI models to industrial, auditable, and sustainable AI systems. This transition is central to the goals of the AIFEU project, which focuses on artificial intelligence in EU financial institutions. In banking, AI is increasingly used for credit scoring, fraud detection, anomaly monitoring, and risk assessment. Creditworthiness and credit-scoring AI systems are classified as high-risk under Annex III of the EU AI Act, while fraud-detection systems, although treated differently in the legal classification, still require strong governance because they affect operational risk, customer protection, and institutional accountability. This creates a direct need for financial AI systems that are transparent, stable, and resource-aware. The scientific contradiction is clear: models optimized solely for predictive accuracy may become fragile in real-world conditions, suffer from backtest overfitting, and incur unnecessary computational and environmental costs.

This paper presents Sentinel as a sustainable information technology for predicting financial anomalies. Sentinel is not defined as a single predictive model. It is a modular information technology designed to support the full analytical cycle. It connects raw data processing, model stability diagnostics, sustainability evaluation, resource-aware training, and automated reporting. The architecture follows a regulation-first logic. This means auditability, traceability, stability, and sustainability are not added after model training. They are embedded in the technical architecture from the beginning. Sentinel consists of 4 functional modules: Adaptive data engine, Diagnostic algorithmic core, Green AI guard, and reporting layer.

The first module is the Adaptive Data Engine. It implements the Data processing method for financial datasets with extreme class imbalance, noise, and leakage risk. In the experiment, the credit-card fraud dataset contained only 0.18% fraudulent cases. This creates a serious risk because a model can appear accurate while failing to detect rare anomalies. Sentinel addresses this through leakage-safe preprocessing. The method includes robust scaling, stratified sampling, under-sampling, outlier removal, and out-of-fold target encoding for categorical variables. These operations protect the integrity of the input data and support the logic of Article 10 of the EU AI Act, which emphasizes data quality, data governance, data preparation, and bias mitigation for high-risk AI systems, also supporting ESG and CSRD compliance.

The second module is the Diagnostic algorithmic core. It implements a stability diagnostic model based on dispersion indicators: variance, interquartile range, and 95% confidence interval. Unlike standard validation relying only on average accuracy or error, this module evaluates model stability across folds and complexity levels. It

identifies the Knee point of complexity, where further model growth no longer improves generalization and increases instability risk. In the stability experiment, the Knee point was identified at 400 leaf nodes, with MAE = 242,906.

The third module is the Green AI guard. It implements the Sustainability scoring model, known as the P-score. P-score is not only a predictive metric. It is a multi-objective Model that combines predictive quality, training time, energy consumption, and CO_2 footprint. Unlike standard approaches that select the model with the lowest error, P-score penalizes resource-intensive configurations. In the Bitcoin LSTM experiment, the Balanced model achieved a P-score of 0.86, while the resource-intensive configuration achieved a P-score of 0.63.

The fourth module is the reporting layer. It transforms technical outputs into audit-ready documents. The first artifact is the Model utility bill. It summarizes data integrity, predictive performance, statistical stability, energy use, CO_2 footprint, and resource efficiency. The second artifact is the ESG Audit Trail. It records preprocessing versions, validation evidence, P-score results, training budget, final model decisions, and regulatory-relevant information.

The simulations verified the practical value of Sentinel. In the fraud detection experiment, the Adaptive data engine neutralized the initial 0.18% imbalance and achieved an ROC-AUC of 0.9787 with a Support Vector classifier. In the stability experiment, the Diagnostic core identified the Knee point at 400 leaf nodes and produced dispersion-based evidence through Variance, IQR, and 95% Confidence interval. In the Bitcoin experiment, P-score selected the more sustainable configuration and avoided a resource-intensive model that emitted 8.4 times more CO_2. In the LightGBM experiment, budget-aware training reduced the training cycle by up to 52% while improving predictive performance.

Sentinel enables EU financial institutions to meet legal and organizational expectations while improving operational performance. It supports EU AI Act-oriented documentation through data governance, stability evidence, robustness assessment, and audit-ready reporting.

Acknowledgments: This research is carried out within the framework of the ERASMUS+ Jean Monnet project «Artificial Intelligence in the EU Financial Institutions» (Project number 101127170 — AIFEU — ERASMUS-JMO-2023-HEI-TCH-RSCH) and TURBO project (Project number 101129315-TURBO-Erasmus-EDU-2023-CBHE). Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the EU nor the granting authority can be held responsible for them.

1. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. – 2024.
2. Bailey D.H., Borwein J.M., López de Prado M., Zhu Q.J. The probability of backtest overfitting. Journal of Computational Finance. – 2016. – Vol. 20, №4. – P. 39–69.
3. Dal Pozzolo A., Caelen O., Johnson R.A., Bontempi G. Calibrating probability with undersampling for unbalanced classification. 2015 IEEE

Symposium Series on Computational Intelligence. – 2015. – P. 159–166.
4. Strubell E., Ganesh A., McCallum A. Energy and policy considerations for deep learning in NLP. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. – 2019. – P. 3645–3650.

Дослідження специфікації ZigBee та стандарту IEEE 802.15.4

УДК 004.7

Максим Марченко[1], Євгенія Іванченко[2],
Ігор Іванченко[3], Анна Васьковська[4]

Державний університет інформаційно-комунікаційних технологій,
[1]mv.marchenko@duikt.edu.ua, [2]e.ivanchenko@duikt.edu.ua,
[3]i.ivanchenko@duikt.edu.ua, [4]a.vaskovska@duikt.edu.ua

Розроблення протокольної структури передавання повідомлень у сенсорних мережах здійснювалося з 2000 року науковими колективами двох організацій:

- цільовою групою TG 15.4 комітету IEEE 802 зі стандартизації LAN/MAN, яка займалася створенням стандарту, що визначає протоколи рівнів PHY і MAC для LR-PAN. Перша редакція стандарту (IEEE 802.15.4-2003) була затверджена у жовтні 2003 р., а друга версія (IEEE 802.15.4-2006) - у вересні 2006 р.;
- групою розробки специфікації ZigBee Alliance, діяльність якої була спрямована на стандартизацію протоколів вищих рівнів LR-PAN. Перша редакція стандарту (ZigBee Specification 1.0) була затверджена у грудні 2004 р., а дві наступні версії (ZigBee Specification 2006 та ZigBee Specification 2007) - у грудні 2006 р. та листопаді 2007 р. відповідно.

Специфікації ZigBee передбачають використання двох верхніх рівнів стеку протоколів вузлів низькошвидкісних мереж: мережевого та прикладного, внаслідок чого загальна протокольна система взаємодії вузлів має чотирирівневу структуру (рис. 1). Рівні взаємодії, визначені специфікаціями ZigBee, функціонують як надбудова над рівнями, регламентованими стандартами IEEE 802.15.4.

Необхідність створення персональних мереж із невисокою швидкістю передачі даних (Low Rate PAN - LR PAN), на рівні кількох десятків кбіт/с, зумовлена глобальною тенденцією до автоматизації практично всіх сфер діяльності людини. Розвиток низькошвидкісних PAN відбувався паралельно з автоматизацією побутових пристроїв і впровадженням систем розподіленого контролю та управління (Distributed Control System - DCS), починаючи з 80-х років XX століття. Метою дослідження є аналіз архітектури, протокольної структури та особливостей функціонування низькошвидкісних персональних мереж LR PAN, побудованих на основі стандарту IEEE 802.15.4 та специфікацій ZigBee. Їхня науково-технічна основа формувалася з двох ключових складових:

- з одного боку, створення широкого спектра сенсорів (sensor) - елементів, призначених для вимірювання фізичних величин різної природи та формування електричних сигналів, які відображають значення цих величин;