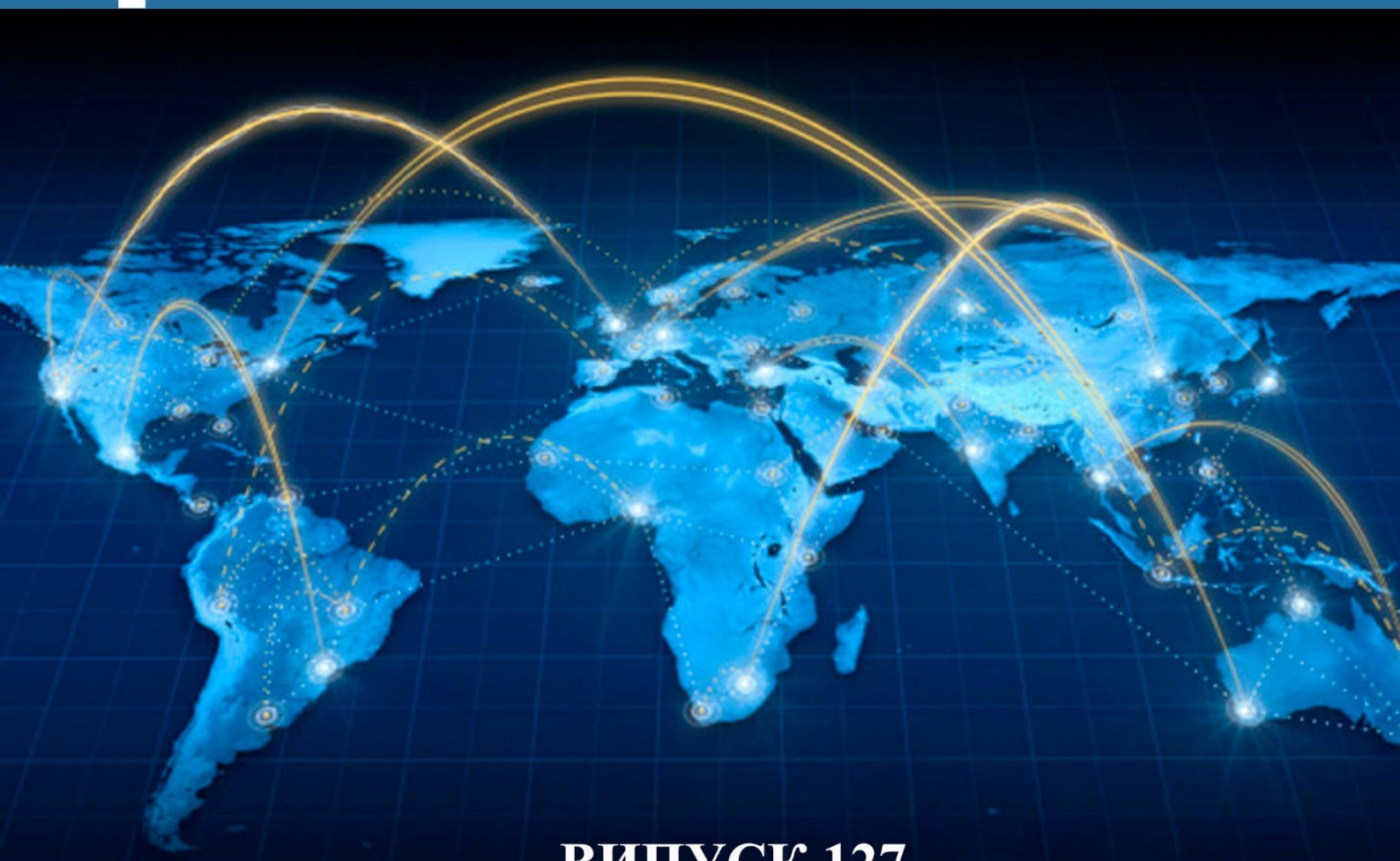
МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА
ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»



ВИПУСК 127

31 березня 2026 р.

м. Переяслав

УНІВЕРСИТЕТ ГРИГОРІЯ СКОВОРОДИ
В ПЕРЕЯСЛАВІ
РАДА МОЛОДИХ УЧЕНИХ УНІВЕРСИТЕТУ
ГО «ІНСТИТУТ СУСПІЛЬНОГО РОЗВИТКУ
І НАУКОВИХ ДОСЛІДЖЕНЬ»

Матеріали
Міжнародної науково-практичної інтернет-конференції

«ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАУКИ І ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ»

31 березня 2026 року
Вип. 127

Збірник наукових праць

Переяслав – 2026

УДК 001+37(100)
ББК 72.4+74(0)
Т 33

Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції та перспективи розвитку науки і освіти в умовах глобалізації»: зб. наук. праць. Переяслав, 2026. Вип. 127. 254 с.

ГОЛОВНИЙ РЕДАКТОР:
Кикоть С. М. – кандидат історичних наук, заступник голови ГО «Інститут суспільного розвитку і наукових досліджень»

РЕДАКЦІЙНА КОЛЕГІЯ:
Воловик Л. М. – кандидат географічних наук, доцент
Гузун А. В. – кандидат біологічних наук, доцент
Євтушенко Н. М. – кандидат економічних наук, доцент
Носаченко В. М. – кандидат педагогічних наук, доцент
Руденко О. В. – кандидат психологічних наук, доцент
Садиков А. А. – кандидат фізико-математичних наук, доцент (Казахстан)
Скляренко О. Б. – кандидат філологічних наук, доцент
Халматова Ш. С. – кандидат медичних наук, доцент (Узбекистан)
Юхименко Н. Ф. – кандидат філософських наук, доцент

Збірник матеріалів конференції вміщує результати наукових досліджень наукових співробітників, викладачів вищих навчальних закладів, докторантів, аспірантів, студентів з актуальних проблем гуманітарних, природничих і технічних наук

Відповідальність за грамотність, автентичність цитат, достовірність фактів і посилань несуть автори публікацій

© Університет Григорія Сковороди в Переяславі
© Рада молодих учених університету
© ГО «Інститут суспільного розвитку і наукових досліджень»

6. Eloundou, T., Manning, S., Mishkin, P. & Rock, D. (2024). GPTs are GPTs: Labor market impact potential of large language models. Science, 384(6702), eadi1585. https://arxiv.org/abs/2303.10130

7. Lewandowski, M. (2024). Artificial intelligence as a catalyst for social innovation: A literature review. European Research Studies Journal, 27(4), 122-140. https://ersj.eu/journal/4222

УДК 004.94

Artemii Muzychenko, Maryna Vyshnevska
(Kyiv, Ukraine)

BALANCING AI MODEL PERFORMANCE WITH ROBUST DATA ENCRYPTION

This article examines the critical challenge of maintaining high performance in artificial intelligence models while integrating robust data encryption mechanisms. It analyzes the fundamental trade-offs between computational overhead introduced by encryption and the accuracy, latency, and throughput requirements of modern AI systems, and explores emerging techniques such as homomorphic encryption, federated learning, and secure multi-party computation.

Keywords: *artificial intelligence, data encryption, homomorphic encryption, federated learning, model performance, privacy-preserving machine learning, secure computation, neural networks.*

У статті досліджується критична проблема забезпечення високої продуктивності моделей штучного інтелекту при одночасній інтеграції надійних механізмів шифрування даних. Аналізуються фундаментальні компроміси між обчислювальними витратами, що виникають внаслідок шифрування, та вимогами до точності, затримки і пропускної здатності сучасних систем ШІ, а також розглядаються перспективні технології, такі як гомоморфне шифрування, федеративне навчання та безпечні багатосторонні обчислення.

Ключові слова: *штучний інтелект, шифрування даних, гомоморфне шифрування, федеративне навчання, продуктивність моделей, машинне навчання зі збереженням конфіденційності, безпечні обчислення, нейронні мережі.*

The rapid advancement of artificial intelligence across pivotal domains is presently positioning data security as the paramount concern in technological discourse. "The growing reliance on AI systems that process sensitive personal and corporate data has intensified the need for robust encryption frameworks" [3, p. 12].

Nonetheless, implementing encryption throughout AI workflows incurs considerable computational overhead. Processing secured datasets may trail their unprotected equivalents by a significant margin in speed, and certain protective mechanisms intrinsically alter the procedures by which data is managed. This piece endeavors to offer an in-depth examination of viable approaches that harmonize robust data security with efficient AI operation – as well as the real-world obstacles impeding the practical realization of confidential AI systems.

Fundamentals of AI and Encryption Integration. It runs on math-heavy processes that need raw data to learn patterns. "Modern AI systems, particularly deep neural networks, require direct arithmetic access to training data, which fundamentally conflicts with the goal of keeping that data encrypted" [6, p. 142].

1. Homomorphic Encryption (HE). Encryption usually means you must unlock data before working with it. Yet homomorphic encryption changes that idea completely. Instead of unlocking, math happens right inside the locked package. "Homomorphic encryption enables computations on ciphertexts, generating an encrypted result that, when decrypted, matches the result of

operations performed on the plaintext" [1, p. 3]. Although shrouded in secrecy, encrypted information remains workable for AI through this particular arrangement. Nevertheless, achieving full homomorphic encryption imposes a significant burden on processing speed; computations can experience dramatically increased execution times relative to their unencrypted counterparts. Recently, advancements within the CKKS and TFHE schemes have somewhat reduced this performance disparity. The appropriate technique selection hinges on the nature of the required arithmetic: CKKS is better suited for the approximate computations frequently encountered in neural network contexts, whereas TFHE is ideal for the precise logical operations characteristic of decision trees.

2. Federated Learning (FL). "Federated learning enables multiple parties to collaboratively train a shared model without exchanging raw data, thereby preserving data privacy at its source" [5, p. 487]. Instead of centralizing all information, federated learning allows data to remain with the original devices or institutions, transmitting only the necessary model refinements. This approach has seen increasing adoption recently, particularly in medical fields and mobile device applications. Nevertheless, certain challenges emerge, such as significant communication overhead among participants, discrepancies in data distributions, and vulnerabilities where malicious entities could manipulate the update gradients. Deploying defenses like incorporating differential privacy or implementing secure aggregation protocols can mitigate these associated risks.

Performance Impact and Mitigation Strategies. Integrating encryption into AI workflows inevitably affects performance. Understanding and mitigating this impact is critical for practical deployment.

- Latency Overhead. Introducing encryption into AI inference workflows substantially increases computational lag. In time-critical uses like self-driving systems or discerning fraudulent activities, even delays measured in milliseconds are often intolerable. Mitigating this involves leveraging hardware acceleration, which can be achieved using specialized FPGA and ASIC circuitry, or through GPU-enhanced Homomorphic Encryption (HE) processing boasting speed enhancements reaching 100 times. Furthermore, model optimization methods, including quantization and pruning, contribute to lessening the processing overhead.
- Accuracy Degradation. Within the CKKS framework and comparable methodologies, the introduction of inherent noise leads to its gradual accumulation throughout the layers of a neural network, consequently diminishing the precision observed in deeper architectures. To counteract this degradation, several corrective approaches have been developed: training models intrinsically responsive to this noise, employing knowledge distillation techniques, or utilizing polynomial activation functions that integrate smoothly with Homomorphic Encryption (HE) schemes. Specifically, substituting the standard ReLU function with polynomial approximations has demonstrated considerable potential.
- Communication Costs. In federated learning, repeated exchange of model parameters creates substantial overhead. "Communication efficiency is one of the primary bottlenecks in federated learning, as gradient updates must be transmitted across potentially slow or unreliable networks" [2, p. 8]. Techniques like gradient compression, quantized communication, and FedAvg incorporating top-k sparsification are capable of achieving a hundredfold reduction in the amount of data transmitted, all without sacrificing the speed or success of convergence.
- Model Architecture Adaptation. Not all architectures are equally amenable to encrypted computation. "The choice of model architecture fundamentally determines the feasibility and efficiency of privacy-preserving inference, as operations like comparisons and non-linear activations are particularly expensive under encryption" [4, p. 1156]. Neural networks employing polynomial activation functions, alongside decision tree groupings, exhibit better congruence with Homomorphic Encryption (HE) when contrasted with blueprints that incorporate operations lacking polynomial properties. Specifically engineered designs, including CryptoNets and GAZELLE, have been developed to facilitate rapid inference while operating in an encrypted domain.

- Differential Privacy Integration. By incorporating precisely calibrated random fluctuations into the results, one can achieve provable, mathematically sound assurances of privacy. The parameter denoted by epsilon governs the balance struck between safeguarding sensitive information and maintaining the usefulness of the data output.

Security Threats and Vulnerabilities. The apparent promise of privacy mechanisms doesn't guarantee flawless operation; vulnerabilities persist, necessitating fixes before AI-level encryption can be fully secured. A single weak link has the potential to compromise the entire system, elevating the importance of even minor flaws. Under pressure, specific safeguards can fail abruptly and silently, dissipating instantly, much like ice melting under the sun. Resilience proves irrelevant if unnoticed fissures create access points for unauthorized parties. Genuine security involves more than erecting defenses; it resides in the ability to detect their points of failure.

The key vulnerabilities in current privacy-preserving AI systems include:

- Gradient leakage in federated learning, where shared model updates reveal training data characteristics.
- Side-channel attacks on encrypted inference, where timing or power consumption patterns expose information about encrypted data.
- Adversarial examples crafted to exploit vulnerabilities in encrypted models, where attacks are harder to detect under encryption.
- Key management failures in distributed systems, where compromised encryption keys can expose entire datasets retroactively.

A significant hazard in federated learning arises from malicious participants injecting corrupted updates intended to deliberately steer the global model astray. This mechanism allows for the clandestine introduction of harmful backdoors into the system, capability of bypassing cryptographic safeguards. Consequently, the imperative is to swiftly identify anomalous behaviors, compelling defensive strategies to effectively discern deception while concurrently maintaining consensus on robust outcomes.

Current Challenges and Future Prospects. Despite significant advances, the path toward production-ready privacy-preserving AI systems remains challenging. The main obstacles include:

- Computational Scalability. Right now, encrypting big deep learning tasks creates too much slowdown. Running a language model securely still cannot be done. Even though faster chips are helping close the difference, live predictions with encryption need better tech on both fronts. Hardware tuned for lattice math plus optimized software for GPUs might get us there.
- Standardization and Interoperability. Fragments spread when no single rule guides how private AI should work. One group’s way of locking data often clashes with another’s, thanks to mismatched codes and differing ideas about what counts as safe. When measurements for secrecy and checks on protection become common ground, progress moves faster. Trust grows only once everyone agrees on what belongs inside the box.
- Regulatory Compliance. Rules like GDPR, HIPAA, and CCPA set rules that sometimes clash with how encrypted AI systems work. Take the right to be forgotten - it brings up tricky issues when trying to delete someone's data from shared learning models. Efforts now focus on methods allowing machines to forget specific inputs. These approaches aim to respect privacy without breaking model integrity.

Right now, real-world uses mostly involve basic systems like spotting tumors in scrambled X-rays or checking loan risks without seeing personal data. Cloud giants have started rolling out privacy-first computing tools, speeding up progress across the board. Reading minds won’t happen soon – but decoding outputs from giant AI brains using encryption might arrive by 2035.

Conclusion. Genuine reliability is found at the intersection of rapid operation and secure handling. When technological systems exhibit swift performance alongside robust confidentiality measures, confidence is established. Not all platforms achieve this equilibrium. Certain ones prioritize velocity, disregarding necessary protective barriers. Conversely, others become paralyzed by excessive prudence.

The safeguarding mechanisms of the future will significantly depend on advancements in cryptographic algorithms, specialized processing units designed for cryptographic operations, novel methodologies for managing protected datasets, alongside pragmatic regulatory frameworks established by authorities. Collaborations uniting software architects, artificial intelligence researchers, system implementers, and policy framers must proceed synchronously, developing practical guidelines that enable the public to place faith in AI systems safeguarding sensitive information.

REFERENCES

1. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Computing Surveys*. 2018. Vol. 51(4). P. 1-35.

2. Kairouz, P. et al. Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*. 2021. Vol. 14(1-2). P. 1-210.

3. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*. 2020. Vol. 37(3). P. 50-60.

4. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Vaikuntanathan, V. CryptoNets: Applying Neural Networks to Encrypted Data. *Proceedings of the 33rd International Conference on Machine Learning*. 2016. Vol. 48. P. 201-210.

5. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. A Survey on Security and Privacy of Federated Learning. *Future Generation Computer Systems*. 2021. Vol. 115. P. 619-640.

6. Boulemtafes, A., Derhab, A., & Challal, Y. A Review of Privacy-Preserving Techniques for Deep Learning. *Neurocomputing*. 2020. Vol. 384. P. 21-45.

УДК 378:004.77(045)

Олена Салфетнікова
(Балаклія, Україна)

ФОРМУВАННЯ ЦИФРОВОЇ РЕЗИСТЕНТНОСТІ СТУДЕНТІВ ТА СТВОРЕННЯ ЕКОСИСТЕМИ ТРАНСФОРМАТИВНОГО НАВЧАННЯ НА ЗАНЯТТЯХ З ІНФОРМАТИКИ

У статті обґрунтовано необхідність переходу від класичної парадигми «комп'ютерної грамотності» до формування цифрової стійкості (резистентності) студентів у межах занять з інформатики. Проаналізовано цифрову резистентність як динамічну здатність особистості не лише володіти технологічним інструментарієм, а й ефективно відновлюватися та розвиватися в умовах постійних кіберзагроз та інформаційної невизначеності.

Ключові слова: *цифрова стійкість (резистентність), трансформативне навчання, освітня екосистема, інформатика.*

The article substantiates the need to move from the classical paradigm of "computer literacy" to the formation of digital resilience (resistance) of students within computer science classes. Digital resilience is analyzed as a dynamic ability of an individual not only to own technological tools, but also to effectively recover and develop in conditions of constant cyber threats and information uncertainty.

Key words: *digital resilience, transformative learning, educational ecosystem, computer science.*