УДК 004.75:004.056.53

А. С. Ліщинський
Д. І. Катєльніков

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОНФІДЕНЦІЙНОСТІ ДАНИХ У ХМАРНИХ ТА ЛОКАЛЬНИХ МОДЕЛЯХ ОБРОБКИ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі проведено комплексний порівняльний аналіз рівня конфіденційності даних у хмарних та локальних системах обробки інформації. Розглянуто архітектурні відмінності обох підходів, основні загрози приватності, характерні для хмарної моделі, та переваги локальної обробки даних.

Ключові слова: конфіденційність даних; хмарні сервіси; локальна обробка; захист персональних даних; GDPR; приватність; офлайн-системи.

Abstract

The paper presents a comprehensive comparative analysis of data confidentiality levels in cloud-based and local information processing systems. The architectural differences between both approaches, the main privacy threats inherent in the cloud model, and the advantages of local data processing are examined.

Keywords: data confidentiality; cloud services; local processing; personal data protection; GDPR; privacy; offline systems.

Вступ

Інтенсивний розвиток цифрових технологій та масштабне поширення хмарних сервісів кардинально змінили підходи до збору, зберігання та обробки інформації. Сучасні застосунки – від голосових асистентів до медичних платформ – дедалі частіше делегують обчислювальні задачі віддаленій інфраструктурі, що породжує системні ризики для конфіденційності кінцевого користувача. Разом із тим набувають поширення рішення на основі локальних обчислень, де весь цикл обробки даних відбувається безпосередньо на пристрої без виходу інформації за його межі. Предметом дослідження є конфіденційність даних як властивість системи, що визначається її архітектурою, а об'єктом – хмарні та локальні моделі обробки інформації.

Метою роботи є системне порівняння хмарного та локального підходів за критеріями конфіденційності, виявлення ключових загроз і переваг кожного з них, а також визначення відповідності сучасним регуляторним вимогам.

Архітектура хмарної моделі та її вплив на конфіденційність

Хмарна модель обробки даних ґрунтується на принципі розподілення задач між клієнтським пристроєм і віддаленою серверною інфраструктурою. У типовому сценарії клієнтський застосунок збирає вхідні дані – текст, аудіо, зображення або документи, і передає їх на сервер постачальника послуги через зашифрований мережевий канал. На стороні сервера відбувається власне обробка, після чого результат повертається клієнту. Такий підхід забезпечує постачальнику можливість використовувати потужні обчислювальні ресурси, регулярно оновлювати моделі та алгоритми централізовано, а також масштабувати сервіс відповідно до навантаження.

Проте з точки зору конфіденційності хмарна архітектура генерує кілька категорій ризиків. Перша і найочевидніша – це ризик перехоплення даних під час передачі. Попри повсюдне застосування протоколу transport layer security для шифрування трафіку, дані залишаються вразливими на етапах завантаження та розвантаження на сервері, а також у разі компрометації сертифікатів або атак типу man-in-the-middle. Друга категорія ризиків пов'язана зі зберіганням даних на стороні постачальника. Навіть якщо умови надання послуги формально обмежують використання даних, фактичний контроль над ними переходить до третьої сторони. Постачальник може зберігати дані для цілей налагодження, навчання моделей або аналітики, а у разі юридичного запиту з боку державних органів – передавати їх без відома користувача. Третя категорія це так звані інсайдерські загрози: персонал постачальника

послуг теоретично може мати доступ до даних користувачів, що підтверджується низкою резонансних інцидентів. Зокрема, у 2019 році журналісти встановили, що підрядники компанії Google прослуховували та транскрибували фрагменти аудіозаписів голосового асистента без явної згоди користувачів [1]. Аналогічні інциденти були зафіксовані й у інших великих постачальників хмарних голосових сервісів.

Четвертою суттєвою проблемою є юрисдикційна невизначеність. Дані, що зберігаються на серверах, розташованих в іноземній правовій юрисдикції, підпадають під законодавство відповідної країни, яке може суттєво відрізнятися від норм, що захищають права користувача на батьківщині. Наприклад, американський закон CLOUD Act [2] надає федеральним органам США право вимагати від американських компаній надання даних, що зберігаються на їхніх серверах по всьому світу, незалежно від місця проживання суб'єкта даних.

Архітектура локальної моделі та її переваги

Локальна модель обробки даних реалізує принципово іншу парадигму: весь обчислювальний процес відбувається в межах пристрою користувача, а дані не передаються зовнішнім системам. У контексті мобільних застосунків це означає, що нейромережева модель, алгоритми обробки та сховище результатів розміщуються безпосередньо у файловій системі застосунку та виконуються процесором пристрою. Прикладом реалізації такого підходу є бібліотека Vosk SDK [3], яка забезпечує повноцінне офлайн-розпізнавання мовлення на мобільних пристроях завдяки компактним нейромережевим моделям.

З точки зору конфіденційності локальна модель надає низку фундаментальних переваг. По-перше, повна відсутність мережевої передачі даних унеможливлює їх перехоплення зовнішніми суб'єктами. По-друге, оскільки дані не виходять за межі пристрою, постачальник програмного забезпечення фізично не має до них доступу, що виключає ризики інсайдерських загроз та примусового розкриття даних на вимогу третіх сторін. По-третє, користувач зберігає повний і єдиний контроль над своїми даними: він самостійно вирішує, де і як вони зберігаються, коли видаляються і кому надається доступ. Нарешті, локальна обробка забезпечує функціональність застосунку за будь-яких мережевих умов — у зонах зі слабким сигналом, під час відключень або у середовищах із обмеженим доступом до інтернету.

Відповідність регуляторним вимогам

Обидва підходи по-різному співвідносяться з чинними нормативними актами у сфері захисту персональних даних. Загальний регламент захисту даних ЄС [4] закріплює низку принципів, дотримання яких є обов'язковим для всіх систем, що обробляють персональні дані. Серед них – принцип мінімізації даних, відповідно до якого збирати та обробляти слід лише ті дані, що є необхідними для конкретної мети; принцип обмеження зберігання, що забороняє тримати дані довше, ніж це потрібно; та принцип privacy by design, що зобов'язує враховувати захист даних вже на етапі проектування системи.

Хмарна модель ускладнює дотримання цих принципів, оскільки розробник змушений покладатися на відповідність постачальника хмарного сервісу регламенту та укладати з ним угоду про обробку даних. Будь-яке порушення на стороні постачальника автоматично створює юридичну відповідальність для розробника. Крім того, передача потребує окремого правового обґрунтування відповідно до глави V GDPR.

Локальна модель натомість органічно відповідає принципу privacy by design: захист забезпечується самою архітектурою системи, а не договірними зобов'язаннями. Оскільки персональні дані не залишають пристрій, питання транскордонної передачі даних, укладення угод із постачальниками та контролю за їхніми діями знімаються автоматично. Аналогічний підхід відображено і в Законі України «Про захист персональних даних» [5], який визначає оператора персональних даних як суб'єкта, що забезпечує фізичну, технічну та організаційну захищеність даних. Локальна архітектура суттєво спрощує виконання цих вимог.

Порівняльний аналіз за ключовими критеріями

Узагальнюючи викладене, можна систематизувати відмінності між підходами за такими критеріями. З точки зору передачі даних хмарна модель вимагає обов'язкової передачі інформації через мережу, тоді як локальна модель повністю виключає будь-який зовнішній трафік, пов'язаний з обробкою. Щодо контролю над даними у хмарній моделі контроль фактично розподіляється між користувачем і

постачальником, тоді як у локальній – залишається виключно за користувачем. Стосовно ризику витоку хмарна модель несе ризики, пов'язані з передачею, зберіганням на сервері та інсайдерськими загрозами; локальна модель обмежує ризик лише фізичним доступом до самого пристрою. За критерієм відповідності GDPR хмарна модель вимагає значних юридичних та організаційних зусиль, тоді як локальна модель відповідає ключовим принципам регламенту за самою своєю природою. Нарешті, щодо незалежності від мережі хмарні рішення є непрацездатними за відсутності з'єднання, а локальні – функціонують автономно.

Необхідно, однак, визнати й обмеження локального підходу. Нейромережеві моделі для офлайн-обробки займають значний обсяг пам'яті пристрою та вимагають певних обчислювальних ресурсів. Хмарні сервіси, що оперують централізованими суперкомп'ютерними кластерами, можуть демонструвати вищу точність на складних або нестандартних даних. Крім того, оновлення локальних моделей потребує дій з боку самого користувача, тоді як хмарні сервіси оновлюються прозоро та централізовано.

Проведений аналіз засвідчує принципову перевагу локальної моделі обробки даних з точки зору забезпечення конфіденційності. Вона усуває системні ризики, притаманні хмарній архітектурі, відповідає вимогам сучасного законодавства про захист персональних даних і надає користувачу повний контроль над власною інформацією. Для систем, що обробляють чутливі або персональні дані, офлайн-підхід є не лише технічно обґрунтованим, а й юридично та етично відповідальним вибором.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Google contractors are listening to your Assistant recordings [Electronic resource] / VRT NWS. – Electronic data. – 2019. – Mode of access: https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping (date of access: 18.04.2026). – Title from the screen.
2. Clarifying Lawful Overseas Use of Data Act (CLOUD Act) [Electronic resource] : Bill S.2383 / 115th United States Congress. – Electronic data. – Mode of access: https://www.congress.gov/bill/115th-congress/senate-bill/2383 (date of access: 19.04.2026). – Title from the screen.
3. Vosk Speech Recognition Toolkit [Electronic resource] / Alphacep (Vosk API). – Electronic data. – Mode of access: https://github.com/alphacep/vosk-api (date of access: 19.04.2026). – Title from the screen.
4. Regulation (EU) 2016/679 (General Data Protection Regulation) [Electronic resource] : Final text of the GDPR including recitals. – Electronic data. – 2016. – Mode of access: https://gdpr-info.eu (date of access: 20.04.2026). – Title from the screen.
5. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. – Електронні дані. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 20.04.2026). – Назва з екрана.

Ліщинський Артем Сергійович - студент групи 2ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: mister.lishinscky@gmail.com.

Катєльніков Денис Іванович. – к.т.н., доцент, доцент кафедри ПЗ, Вінницький національний технічний університет, м. Вінниця, e-mail: katielnikov@vntu.edu.ua.

Lishchynskyi Artem Serhiyovych - student of the 2PI-22b group, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mister.lishinscky@gmail.com.

Katielnikov Denis I. – Ph.D., Associate Professor, Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: katielnikov@vntu.edu.ua.