КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1123
УДК 004.056.55:004.738.5:004.7

Науменко Сергій Васильович
аспірант
Черкаський національний університет імені Богдана Хмельницького, Черкаси, Україна
ORCID: 0000-0002-6337-1605
naumenko.serhii1122@vu.cdu.edu.ua

Михайловський Павло Васильович
аспірант
Черкаський національний університет імені Богдана Хмельницького, Черкаси, Україна
ORCID: 0009-0008-4324-1724
mykhailovskyi.pavlo1123@vu.cdu.edu.ua

Розломій Інна Олександрівна
кандидат технічних наук, доцент
доцент кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет, Черкаси, Україна
ORCID: 0000-0001-5065-9004
inna-roz@ukr.net

МОДЕЛЬ ІЗОЛЬОВАНОЇ ОБРОБКИ КОНФІДЕНЦІЙНИХ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ

Анотація. Стаття присвячена розробці моделі ізольованої обробки конфіденційних даних у хмарному середовищі, орієнтованої на сценарії використання в системах Інтернету речей. Актуальність дослідження зумовлена зростанням обсягів чутливої інформації, що передається до хмарних платформ для обробки, за умов обмеженої або відсутньої довіри до хмарного провайдера. Запропонований підхід базується на застосуванні технологій Trusted Execution Environment, які забезпечують апаратно захищене середовище виконання для критичних обчислень. Розроблена модель передбачає чітке розмежування функціональних компонентів хмарної інфраструктури з виділенням enclave-контейнера як єдиного елемента, що має доступ до відкритого змісту даних. Усі конфіденційні операції, включаючи дешифрування, валідацію, обчислення та формування результатів, виконуються виключно в межах довіреного середовища. Незахищені хмарні сервіси взаємодіють лише з зашифрованими або агрегованими даними, що унеможливлює несанкціонований доступ до чутливої інформації навіть у разі компрометації операційної системи або гіпервізора. Запропоновано модель потоків даних, яка описує маршрутизацію інформації між IoT-пристроями, enclave та зовнішніми сервісами з урахуванням типів даних і рівнів доступу. Формалізовано процес обробки у вигляді послідовності перетворень зашифрованих даних у довіреному середовищі з подальшим поверненням результатів у контрольованому вигляді. Побудовано політики доступу та правила передачі результатів, що відповідають принципам мінімального розкриття інформації та нульової довіри. Практичну реалізацію моделі продемонстровано на прикладі прототипу з використанням технології Intel SGX для обробки медичних показників, отриманих від IoT-пристроїв. Проведений порівняльний аналіз із традиційними підходами до хмарної обробки підтвердив переваги запропонованого рішення за рівнем ізоляції та контролю доступу при збереженні масштабованості. Отримані результати свідчать про доцільність застосування розробленої моделі в системах, що працюють з конфіденційними даними в умовах недовіри до хмарного середовища.

Ключові слова: хмарні обчислення; Trusted Execution Environment; enclave; конфіденційні обчислення; IoT; ізольована обробка даних.

ВСТУП

В умовах активного впровадження хмарних технологій та зростання кількості пристроїв Інтернету речей (IoT) постає необхідність у надійних механізмах захисту конфіденційних даних [1, с. 5]. Особливої актуальності це набуває у випадках, коли обробка даних здійснюється у хмарних середовищах, що перебувають поза межами повного контролю користувача. Відсутність прозорості в адмініструванні хмарної інфраструктури та потенційна вразливість гіпервізорів, операційних систем і програмного забезпечення створюють загрози несанкціонованого доступу до чутливої інформації [2, с. 73].

Одним із перспективних підходів до подолання цих викликів є використання технологій довірених ізольованих середовищ виконання (Trusted Execution Environment, TEE), що реалізуються апаратними засобами сучасних процесорів [3, с. 105]. Завдяки підтримці механізмів SGX (Intel), SEV (AMD), TrustZone (ARM) можливо створювати захищені області пам'яті (enclaves), недоступні для інших процесів системи, у тому числі для гіпервізора та адміністратора хмари [4, с. 33], [5, с. 330]. Це дозволяє забезпечити ізольовану обробку конфіденційних даних, навіть якщо інші компоненти обчислювального середовища скомпрометовані.

Постановка проблеми. У традиційних хмарних архітектурах обробка даних відбувається у середовищі з широкими правами доступу, що унеможливлює гарантування конфіденційності за умов потенційної компрометації інфраструктури. Це створює серйозні ризики для галузей, де обробляється критично важлива інформація: охорони здоров'я, промисловості, енергетики, оборони. Створення моделі ізольованої обробки даних із використанням TEE у хмарному середовищі дає змогу зберегти контроль над критичними обчисленнями, зменшити обсяг довіри до хмарного провайдера та підвищити рівень захисту даних, що передаються з IoT-пристроїв.

Аналіз останніх досліджень і публікацій. Останніми роками спостерігається стрімке зростання наукового інтересу до концепцій безпечного обчислення у хмарних середовищах, особливо із застосуванням апаратних механізмів захисту, таких як Trusted Execution Environment (TEE) [6, с. 105], [7, с. 325]. Широке впровадження IoT-пристроїв, які генерують великі обсяги чутливої інформації (зокрема, медичної, промислової, енергетичної), потребує нових парадигм ізолювання обробки даних. Це спричинило появу нових підходів до створення enclave-архітектур та інтеграції TEE у контексти хмарної безпеки.

Зокрема, в працях [8, с. 15], [9, с. 205] запропоновано архітектури enclave-заснованих сервісів, реалізованих за допомогою технології Intel SGX. Автори демонструють приклади захищеного виконання обчислень у медицині, де збереження конфіденційності даних пацієнтів є критично важливим. У цих роботах доведено можливість ізольованої обробки навіть за умов скомпрометованого програмного забезпечення, що розширює область застосування хмарних сервісів для критично важливих сфер.

Водночас у роботах [10, с. 583], [11, с. 66] акцент зроблено на обмеженнях TEE з погляду масштабованості, сумісності з контейнеризованими інфраструктурами та складності інтеграції в мультиарендні хмарні середовища. Підкреслено, що хоча enclave-модулі забезпечують високу ізоляцію, вони обмежені обсягом доступної пам'яті, що ускладнює обробку великих масивів даних. Крім того, деякі сценарії обчислень із попередньою обробкою та агрегацією даних потребують складної логіки розмежування між enclave і незахищеними частинами середовища.

У роботі [12, с. 258] запропоновано ефективний протокол формування довірених каналів передачі зашифрованих даних до enclave-модуля, з використанням попередньо обчислених ключів і обміну токенами автентифікації. Незважаючи на переваги цього підходу, автори не охопили питання організації потоку даних між компонентами IoT-системи, не представили логіку розмежування доступу та не сформували повноцінну модель ізольованої обробки в умовах IoT.

Дослідження в [13, с. 6613], [14, с. 4] фокусуються на формалізації моделей безпеки у розподілених хмарних обчисленнях, проте основну увагу приділяють класичним програмним підходам до криптографії, нехтуючи апаратною ізоляцією. Аналогічно, у [15, с. 92740] розглядаються гібридні моделі з елементами довіреної обчислювальної бази, однак відсутнє обґрунтування щодо оптимального розподілу обчислень між enclave та хмарними мікросервісами.

Отже, попри наявність значної кількості робіт, які досліджують потенціал TEE для безпечної обробки даних, досі залишаються нерозв'язаними такі важливі аспекти:

- формалізація моделі ізольованої обробки конфіденційної інформації у хмарному середовищі з урахуванням архітектури IoT;
- побудова потоків обміну даними із чітким розмежуванням доступу на enclave/не-enclave-рівнях;
- забезпечення ефективності й масштабованості при мінімізації втрат продуктивності.

Таким чином, існує необхідність у створенні узагальненої моделі, що враховує особливості обробки чутливих даних в умовах недовіри до провайдера хмари, адаптованої до обмежень типових IoT-інфраструктур.

Метою статті є формалізація моделі ізольованої обробки конфіденційних даних у хмарному середовищі із застосуванням TEE-технологій (SGX, SEV), орієнтованої на підтримку IoT-архітектур з високими вимогами до конфіденційності та збереження цілісності даних в умовах недовіри до хмарного провайдера.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У цьому розділі приводяться концепції, підходи, принципи, методи та інші положення, на яких безпосередньо базується дослідження. Зазначаються основні терміни, поняття та категорії, що лежать в основі дослідження.

Концепція ізольованої обробки даних ґрунтується на принципах нульової довіри (Zero Trust) та апаратної ізоляції, згідно з якими будь-які компоненти інфраструктури, що не є частиною довіреного середовища, розглядаються як потенційно небезпечні. У межах цієї парадигми забезпечення конфіденційності даних можливе лише за умови гарантування цілісності середовища виконання, незалежно від стану хмарної інфраструктури.

Ключовим терміном у даному контексті є довірене ізольоване середовище виконання (Trusted Execution Environment, TEE) – це обчислювальне середовище з підвищеним рівнем захисту, яке забезпечує апаратну ізоляцію процесів, даних і пам’яті. TEE гарантує, що код та дані всередині enclave не можуть бути зчитані або модифіковані жодними зовнішніми процесами, навіть у разі повного контролю над гостьовою операційною системою або гіпервізором.

Найбільш поширені реалізації TEE включають:

- Intel SGX (Software Guard Extensions) – дозволяє створювати enclave в оперативній пам’яті, у межах яких відбувається захищене виконання коду [16, с. 184];
- AMD SEV (Secure Encrypted Virtualization) – забезпечує повне шифрування віртуальних машин та їх ізоляцію на рівні гіпервізора [17, с. 87];
- ARM TrustZone – ділить процесорну архітектуру на захищене (Secure World) та звичайне (Normal World) середовище з розмежуванням доступу до ресурсів [18, с. 160].

На основі цих технологій формується контейнер ізоляції – базовий елемент запропонованої моделі, який є віртуальною захищеною областю для виконання критичних обчислень. Контейнер обробляє лише вузькоспеціалізовані задачі, що вимагають абсолютної конфіденційності: декодування вхідних потоків, валідація, зберігання тимчасових ключів, підпис або обробка даних у форматі plaintext до шифрування. Решта функціоналу – фільтрація, агрегація, зберігання в базах даних, візуалізація – виконується поза enclave, у менш привілейованому середовищі [19, с. 455].

Важливим поняттям для опису архітектури є модель потоків даних. У ній передбачено наявність захищених логічних каналів обміну, де enclave отримує зашифровані вхідні дані, проводить внутрішню дешифрацію та обчислення, а потім повертає лише дозволені результати. Таким чином, забезпечується повне розмежування доступу до змісту повідомлень і пов’язаних з ними метаданих. Незахищені компоненти системи взаємодіють виключно із зашифрованими формами даних, що унеможливлює аналіз вмісту навіть у разі витоку.

Дослідження базується також на концепції конфіденційних обчислень, яка передбачає створення довіреного середовища на всіх етапах життєвого циклу даних: у стані зберігання, передачі та обробки. Відомі моделі безпеки (наприклад, Bell-LaPadula, Clark-Wilson) у класичному вигляді не пристосовані до умов IoT- і хмарної взаємодії, а тому адаптація принципів ізоляції і потокового контролю є необхідною [20, с. 6], [21, с. 3].

У цілому, розробка моделі ізольованої обробки даних у хмарі спирається на поєднання апаратного захисту, контейнерних обчислень та криптографічного контролю доступу, що дозволяє створити ізольовану і масштабовану архітектуру без необхідності довіри до зовнішніх компонентів інфраструктури.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження моделі ізольованої обробки конфіденційних даних у хмарному середовищі здійснювалося шляхом концептуального моделювання, побудови архітектурних схем, аналізу протоколів взаємодії між enclave-модулями та хмарними компонентами, а також емпіричної валідації запропонованих рішень на базі емуляції типових сценаріїв IoT.

В основу розробки моделі покладено метод структурного розподілу обчислень, який дозволяє виокремити критичні для конфіденційності операції та віднести їх до enclave-контейнера, тоді як неконфіденційна обробка виконується у загальнодоступному середовищі. Такий підхід знижує загальне навантаження на TEE-платформу та підвищує масштабованість рішення.

Для верифікації архітектурної моделі було створено узагальнену схему взаємодії між IoT-пристроями, enclave-модулем та іншими сервісами хмарного середовища. Як основу для моделювання використано:

- Intel SGX SDK – для моделювання enclave;
- Open Enclave SDK – як кросплатформену абстракцію для розробки захищених застосунків;
- Azure Confidential Computing Emulator – для відтворення поведінки хмарної інфраструктури з підтримкою TEE.

Під час дослідження змодельовано обробку чутливих даних, що надходять із сенсорів IoT-пристроїв, з подальшою маршрутизацією до enclave. Було реалізовано захищений канал з автентифікацією та шифруванням на основі TLS, а також механізм дешифрування, валідації та формування відповіді всередині enclave.

Серед основних критеріїв оцінювання ефективності моделі використовувалися:

- обсяг ізольованих обчислень;
- ступінь розмежування доступу до даних;
- мінімізація часу переходу між enclave/non-enclave середовищем;
- узгодженість з концепцією Zero Trust;
- рівень масштабованості в умовах зростання кількості пристроїв.

Під час оцінювання моделі проводилось порівняння із класичними підходами до обробки даних у хмарі, що не передбачають TEE, із метою визначення переваг ізоляції на рівні обчислювального середовища.

Результати були частково апробовані в рамках виконання НДР №0125U000637 – «Розробка завадозахищеної енергоефективної системи контролю та управління віддаленими безпілотними об'єктами на основі факторіального кодування даних».

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Запропонована модель ізольованої обробки даних передбачає поділ хмарного середовища на два функціональні домени: довірене середовище enclave та загальнодоступні (незахищені) сервіси. Джерелом конфіденційних даних виступають IoT-пристрої, які передають зашифровану інформацію до хмари через захищений канал. У межах хмарної інфраструктури enclave-модуль приймає зашифровані дані, проводить їх валідацію, розшифрування, критичну обробку та формує відповідь, яка може бути повторно зашифрована або передана у незахищену частину системи.

Незахищені сервіси, такі як бази даних, сервіси аналітики, інтерфейси візуалізації або зовнішні API, не мають доступу до відкритого змісту даних. Вони оперують лише зашифрованими результатами або агрегованими показниками, підготовленими enclave-контейнером. Таким чином досягається функціональна ізоляція критичної логіки без необхідності повної перебудови хмарної архітектури.

Основним елементом довіреної зони є enclave-контейнер, який реалізовано на базі апаратної підтримки TEE (наприклад, Intel SGX або AMD SEV). Він відповідає за виконання обчислень, зберігання тимчасових ключів, криптографічну обробку, автентифікацію джерела та контроль відповідності вхідних даних. У той час як решта сервісів зберігають масштабованість і не залежать від обмежень enclave, завдяки чіткому поділу повноважень і потоків обробки, рис. 1.

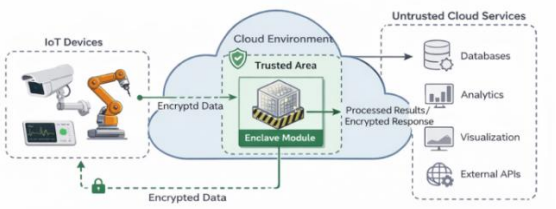

Рис. 1. Узагальнена архітектура ізольованої обробки даних у хмарі з TEE

На рис. 1 зображено логічну структуру взаємодії між IoT-пристроями, enclave-модулем та хмарною інфраструктурою. Стрілками позначено напрямок передачі зашифрованих і оброблених даних.

Enclave-модуль виступає як центральний вузол обробки, тоді як інші компоненти залишаються функціонально відокремленими.

Модель потоків даних у хмарі, що використовує TEE, формує два ключові логічні канали: захищений канал обробки та незахищений канал допоміжних операцій. Дані від IoT-пристрою надходять у зашифрованому вигляді до enclave, де проходять дешифрування, первинну обробку та формування довіреного результату. Важливо, що доступ до enclave можливий лише за автентифікованим запитом, а вся комунікація здійснюється через TLS або інші криптографічно захищені протоколи.

Після завершення обробки enclave повертає результат, який може бути переданий у вигляді:

– зашифрованого повідомлення до зовнішнього сервісу;
– агрегованої метаінформації для зберігання в базі даних;
– відповіді без конфіденційних складових – у випадку відкритої взаємодії.

Незахищені частини інфраструктури мають доступ лише до закритих форматів, і не можуть ініціювати обчислення у enclave без авторизації. Така логіка мінімізує вірогідність витоку або стороннього впливу на процеси критичної обробки, рис. 2.

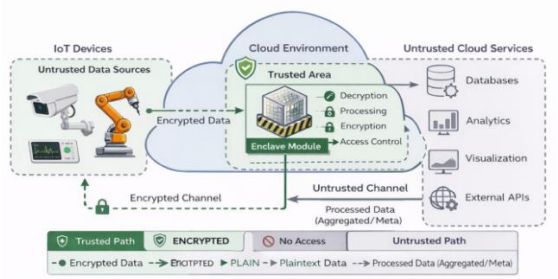

Рис. 2. Модель потоків даних з enclave та розмежування доступу

На рис. 2 представлено потоки даних між IoT-пристроями, enclave-модулем і зовнішніми хмарними сервісами. Виділено зони доступу, типи інформації (зашифрована, plaintext, оброблена) та напрями переміщення. Модель ілюструє, що enclave є єдиною точкою розшифрування, тоді як решта системи ніколи не має доступу до відкритих даних.

Формалізована модель ізольованої обробки конфіденційних даних ґрунтується на уявленні обчислювального маршруту як послідовності перетворень у межах enclave-модуля та зовнішніх (недовірених) компонентів. Нехай, D_{enc} – вхідні зашифровані дані, отримані від IoT-пристрою; D_{TEE} – розшифровані дані у середовищі enclave; $f(D)$ – функція обробки даних у довіреному середовищі (наприклад, фільтрація, підпис, обрахунок параметрів); R_{enc} – результат обробки у зашифрованому або агрегованому вигляді, що повертається в незахищене середовище.

Загальна модель обробки формалізується як (1).

$$D_{enc} \rightarrow D_{TEE} \rightarrow f(D) \rightarrow R_{enc} \quad (1)$$

Кожен етап моделі супроводжується застосуванням відповідного контролю доступу та механізмів захисту. На етапі D_{TEE} виконується автентифікація джерела, перевірка цілісності та обмеження обсягу доступної пам'яті. Функція D_{TEE} виконується в межах enclave з повною ізоляцією процесу.

Політика доступу реалізується у вигляді правил:

– тільки enclave має право дешифрувати вхідні дані;
– лише оброблені результати можуть бути передані назовні;
– зовнішні сервіси не мають доступу до жодного з етапів D_{TEE} або D_{TEE}.

Це забезпечує дотримання принципу мінімального розкриття інформації (least disclosure) та відокремлення привілеїв (privilege separation).

Таблиця 1

Ключові функціональні етапи enclave-обробки

Етап	Опис операції	Вихідні дані
Denc	Прийом зашифрованих даних	Зашифроване повідомлення
DTEE	Дешифрування та перевірка цілісності	Дані у plaintext
f(D)	Критична обробка у enclave	Оброблений результат
Renc	Шифрування або агрегація результату	Вихідні зашифровані дані

У рамках перевірки працездатності запропонованої моделі було реалізовано прототип на базі Intel SGX, із використанням Intel SGX SDK та бібліотеки Open Enclave [22, с. 4123]. Емуляція хмарного середовища проводилася у Docker-середовищі з поділом на окремі контейнери для enclave-компонента та допоміжних сервісів.

Прототип реалізовано у вигляді багатокомпонентної системи, що включає симульоване джерело даних (IoT-пристрій), enclave-сервіс, допоміжні хмарні компоненти та візуалізаційний модуль. Модель розгорнуто в середовищі контейнеризації Docker, де enclave-модуль працює у вигляді ізольованого мікросервісу з обмеженим доступом до системних ресурсів. Комунікація між компонентами здійснюється через захищені канали з автентифікацією на основі TLS. Загальна структура прототипу, розробленого для перевірки працездатності запропонованої архітектури, наведена на рис. 3.

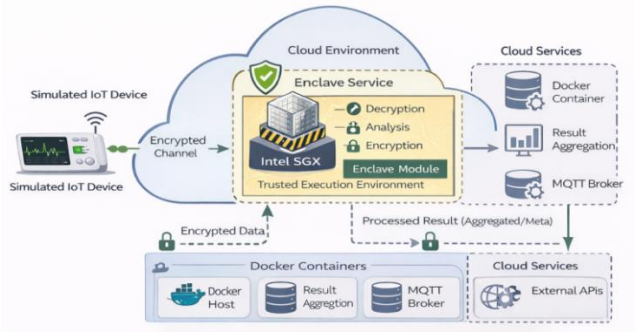

Рис. 3. Прототип системи ізольованої обробки конфіденційних даних

На схемі зображено компоненти розгорнутої моделі, включаючи генератор даних (IoT-симулятор), enclave-модуль, модуль збору результатів та підсистему візуалізації. Виділено типи каналів, через які передається інформація (зашифровані, відкриті), а також операції, які виконуються в enclave (дешифрування, аналіз, шифрування результату). Сценарій взаємодії охоплює повний цикл: від генерації даних до представлення результатів, що дозволяє оцінити ізоляцію, контроль доступу та цілісність даних у процесі обробки.

Такий сценарій дозволив перевірити поведінку enclave в умовах потоку реальних даних і показав зменшення ризику витоку інформації за відсутності довіри до середовища виконання.

Для оцінки ефективності запропонованої моделі проведено порівняння з типовими схемами хмарної обробки, які не використовують механізми ізольованого виконання. Основними критеріями вибрано рівень ізоляції даних, продуктивність обробки та масштабованість системи.

Таблиця 2

Модель TEE vs традиційна хмарна обробка

Критерій	Традиційна хмарна обробка	Модель з використанням TEE
Ізоляція даних	Логічна, програмна	Апаратна, гарантована на рівні CPU
Контроль доступу	Залежить від ОС та гіпервізора	Вбудований у enclave, незалежний від ОС
Довіра до хмари	Повна або часткова	Мінімальна, обмежена enclave
Продуктивність	Вища у загальному випадку	Нижча при повній ізоляції, оптимізується за рахунок розподілу обчислень
Масштабованість	Висока	Висока за умови оптимального розподілу навантаження
Захист у разі атаки	Залежить від засобів моніторингу	Дані недоступні навіть при компрометації ОС/гіпервізора

Запропонована модель забезпечує вищий рівень ізоляції завдяки апаратним механізмам, що мінімізує ризики витоку навіть у разі атак на хмарну інфраструктуру. Хоча enclave-технології мають певні обмеження щодо обсягу пам’яті та часу перемикання контексту, оптимізація через часткове розвантаження обчислень поза enclave дозволяє досягти прийнятного балансу між безпекою та продуктивністю [23, с. 1880]. Масштабованість моделі підтверджена сценарієм використання enclave лише для критичних функцій, що дає змогу підтримувати обробку даних від великої кількості IoT-пристроїв.

Наукова новизна запропонованої моделі полягає у поєднанні ізольованого оброблення в enclave з потоковим маршрутизуванням даних у хмарному середовищі. Завдяки впровадженню логіки

розмежування потоків на enclave- і non-enclave-рівнях забезпечується контроль доступу на рівні каналів передачі, а не лише на рівні обчислювальних процесів. Такий підхід дозволяє створити динамічну та адаптивну модель, у якій enclave виконує лише критично важливі операції, а решта обробки здійснюється у незахищеному, але ізольованому контексті.

Запропонована модель універсальна щодо типів застосування і може бути використана в різних галузях. У сфері охорони здоров'я вона дозволяє обробляти дані пацієнтів без доступу медичного персоналу до сирих значень. У промисловості – забезпечити захист конфіденційних технологічних параметрів. В енергетиці – убезпечити дані про споживання, балансування навантаження та контроль доступу до систем диспетчеризації.

На відміну від відомих моделей enclave-сервісів, які переважно реалізуються як ізольовані мікросервіси або довірені функції без обліку контексту потоків, запропоноване рішення описує повноцінну модель маршрутизації й обробки із чітко вираженою формальною структурою та критеріями адаптації. Це дозволяє інтегрувати її як шаблон архітектури в системах, що потребують високої конфіденційності без повного контролю над хмарним середовищем.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано модель ізольованої обробки конфіденційних даних у хмарному середовищі з використанням технологій Trusted Execution Environment (TEE), яка забезпечує апаратну ізоляцію критичних обчислень навіть у разі компрометації гіпервізора, операційної системи або хмарного провайдера. Побудовано архітектуру моделі з enclave-модулем як основним елементом довіреного середовища, формалізовано процес обробки даних, визначено політики доступу та сформовано логіку потоків обміну.

Проведене порівняння з традиційними підходами до хмарної обробки показало переваги запропонованої моделі за критеріями ізоляції, контролю доступу та гнучкості інтеграції в IoT-архітектури. Практична реалізація на основі Intel SGX підтвердила можливість застосування моделі для обробки чутливих даних у медичних сценаріях.

Наукова новизна роботи полягає в поєднанні enclave-технологій із потоково орієнтованим підходом до маршрутизації даних, що дозволяє адаптувати модель до різних типів навантаження, зберігаючи високий рівень конфіденційності.

У подальших дослідженнях передбачається:

- розширення моделі із підтримкою динамічної ротації enclave-контейнерів у мультихмарних середовищах;
- оптимізація продуктивності за рахунок гібридного розподілу обчислень між enclave та периферійними обчислювальними вузлами;
- розробка інструментів моніторингу та верифікації цілісності enclave під час виконання;
- дослідження інтеграції з blockchain- або DLT-платформами для забезпечення прозорості взаємодії та трасування доступів до даних.

Запропонована модель може стати основою для побудови типових архітектур у системах критичного призначення, які потребують одночасно високого рівня безпеки, масштабованості та незалежності від довіри до хмарного провайдера.

ПОДЯКА

Дослідження виконано за сприяння науково-дослідної роботи, що фінансується за кошти державного бюджету України: НДР №0125U000637 – «Розробка завадозахищеної енергоефективної системи контролю та управління віддаленими безпілотними об'єктами на основі факторіального кодування даних».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rozlomii, I., Naumenko, S., Myhailovskyi, P., & Lishchuk, R. (2025, October). Methodology for selecting the protection strategy in IoT environments based on the device resource profile. In *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek)* (pp. 1-5). IEEE.
2. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, May). The role of encryption in information protection for cloud computing. In *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 70-75). IEEE.

3. Ménétrey, J., Göttel, C., Khurshid, A., Pasin, M., Felber, P., Schiavoni, V., & Raza, S. (2022, June). Attestation mechanisms for trusted execution environments demystified. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 95-113). Springer.
4. Will, N. C., & Maziero, C. A. (2023). Intel software guard extensions applications: A survey. *ACM Computing Surveys, 55*(14s), 1-38.
5. Zhao, S., Li, M., Zhang, Y., & Lin, Z. (2022, May). vSGX: Virtualizing SGX enclaves on AMD SEV. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 321-336). IEEE.
6. Anasuri, S. (2023). Confidential computing using trusted execution environments. *International Journal of AI, Big Data, Computational and Management Studies, 4*(2), 97-110.
7. Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2023). TEBDS: A trusted execution environment-and-blockchain-supported IoT data sharing system. *Future Generation Computer Systems, 140*, 321-330.
8. Park, J., Kang, S.,Lee, S.,Kim, T.,Park, J.,Kwon, Y.,Huh, J.(2024).Hardware-hardened sandbox enclaves for trusted serverless computing.*ACM Transactions on Architecture and Code Optimization, 21* (1), 1-25.
9. Will, N. C., & Maziero, C. A. (2023, February). Efficient management models for SGX enclaves. In *International Conference on Information Systems Security and Privacy* (pp. 195-224). Springer.
10. Eboseremen, B. O., Ogedengbe, A. O., Obuse, E., Oladimeji, O., Ajayi, J. O., Akindemowo, A. O., & Erigha, E. D. (2022). Secure data integration in multi-tenant cloud environments: Architecture for financial services providers. *Journal of Frontiers in Multidisciplinary Research, 3*(1), 579-592.
11. Voievodin, Y. V., & Rozlomii, I. O. (2024, April). Advanced software framework for comparing balancing strategies in container orchestration systems. In *Proceedings of the conference* (pp. 60-69).
12. Hamidy, G. M., Yulianti, S., Philippaerts, P., & Joosen, W. (2023, November). TC4SE: A high-performance trusted channel mechanism for secure enclave-based trusted execution environments. In *International Conference on Information Security* (pp. 246-264). Springer.
13. Pradhan, G., & Priyadarsini, M. (2024). A trusted computing framework for cloud data security using role-based access and pattern recognition. *Cluster Computing, 27*(5), 6609-6622.
14. Vuppala, N. S. M., Hebbar, K. S., Gupta, D., Sharma, V., & Roy, V. (2025, December). Advanced security framework for threat mitigation in cloud computing environments. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.
15. Modaber, M., Hendriks, M., Geilen, M., Basten, T., Voeten, J.(2024). A method for building trustworthy hybrid performance models for cyber-physical systems of systems. *IEEE Access, 12*, 92733-92752.
16. Kang, D. M., Faahym, H., Meftah, S., Keoh, S. L., & Khin, M. M. A. (2023, March). Practical deep neural network protection for unmodified applications in Intel software guard extension environments. In *International Conference on Critical Infrastructure Protection* (pp. 177-192). Springer.
17. Tara, A., & Khan, T. U. (2025, April). A comparative study of hardware-based and software-based secure virtualization technologies. In *Computer Science On-line Conference* (pp. 69-95). Springer.
18. Islam, M. S., Zamani, M., Kim, C. H., Khan, L., & Hamlen, K. W. (2023, April). Confidential execution of deep learning inference at the untrusted edge with ARM TrustZone. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy* (pp. 153-164). ACM.
19. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2023). Analysis of information security issues in balancing multiple independent containers on a single server. In *Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems* (pp. 450-461).
20. Ayamga, D., Nanda, P., & Mohanty, M. (2024, December). The Bell-LaPadula (BLP) enterprise security architecture model vs inference attacks. In *2024 17th International Conference on Security of Information and Networks (SIN)* (pp. 1-8). IEEE.
21. Haloua, F., Abbas, M., Djerbi, R., & Bouhamed, M. M. (2024, April). Formal modelling and implementation of Clark–Wilson security policy with FoCaLiZe. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)* (pp. 1-5). IEEE.
22. Yu, J. Z., Shinde, S., Carlson, T. E., & Saxena, P. (2022).Elasticlave:An efficient memory model for enclaves.In *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)* (pp. 4111-4128).
23. Lee, D., Cheang, K., Thomas, A., Lu, C., Gaddamadugu, P., Vahldiek-Oberwagner, A., & Asanović, K. (2022, November). Cerberus: A formal approach to secure and efficient enclave memory sharing. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1871-1885). ACM.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Serhiy Naumenko
PhD student
Bohdan Khmelnytskyi Cherkasy National University, Cherkasy, Ukraine
ORCID: 0000-0002-6337-1605
naumenko.serhii1122@vu.cdu.edu.ua

Pavlo Mykhailovskyi
PhD student
Bohdan Khmelnytskyi Cherkasy National University, Cherkasy, Ukraine
ORCID: 0009-0008-4324-1724
mykhailovskyi.pavlo1123@vu.cdu.edu.ua

Inna Rozlomii
PhD, Associate Professor
Associate Professor of the Department of Information Security and Computer Engineering
Cherkasy State Technological University, Cherkasy, Ukraine
ORCID: 0000-0001-5065-9004
inna-roz@ukr.net

MODEL OF ISOLATED PROCESSING OF CONFIDENTIAL DATA IN A CLOUD ENVIRONMENT

Abstract. The article focuses on the development of a model for isolated processing of confidential data in cloud environments, with particular emphasis on Internet of Things use cases. The relevance of the study is driven by the growing volume of sensitive data transferred to cloud platforms under conditions of limited trust in cloud service providers. The proposed approach relies on Trusted Execution Environment technologies that provide hardware-based isolation for critical data processing tasks. The developed model introduces a clear separation of cloud infrastructure components, where an enclave container acts as the only trusted entity allowed to access plaintext data. All sensitive operations, including decryption, validation, computation, and result generation, are executed exclusively within the trusted environment. Untrusted cloud services operate only on encrypted or aggregated data, ensuring confidentiality even in the event of operating system or hypervisor compromise. A data flow model is proposed to describe secure routing between IoT devices, the enclave module, and external cloud services, taking into account data types and access levels. The data processing pipeline is formalized as a sequence of transformations performed within the trusted environment, followed by controlled output delivery. Access control policies and result transmission rules are defined in accordance with the principles of zero trust and minimal information disclosure. The practical applicability of the model is demonstrated through a prototype implementation based on Intel SGX technology, targeting the processing of medical data collected from IoT devices. A comparative analysis with traditional cloud processing architectures confirms the advantages of the proposed solution in terms of isolation strength and access control while preserving scalability. The results indicate that the proposed model is suitable for deployment in systems requiring high levels of confidentiality without full reliance on cloud provider trust.

Keywords: cloud computing; Trusted Execution Environment; enclave; confidential computing; IoT; isolated data processing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Rozlomii, I., Naumenko, S., Myhailovskyi, P., & Lishchuk, R. (2025, October). Methodology for selecting the protection strategy in IoT environments based on the device resource profile. In *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek)* (pp. 1-5). IEEE.
2. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, May). The role of encryption in information protection for cloud computing. In *2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST)* (pp. 70-75). IEEE.
3. Ménétrey, J., Göttel, C., Khurshid, A., Pasin, M., Felber, P., Schiavoni, V., & Raza, S. (2022, June). Attestation mechanisms for trusted execution environments demystified. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 95-113). Springer.
4. Will, N. C., & Maziero, C. A. (2023). Intel software guard extensions applications: A survey. *ACM Computing Surveys*, *55*(14s), 1-38.

5. Zhao, S., Li, M., Zhang, Y., & Lin, Z. (2022, May). vSGX: Virtualizing SGX enclaves on AMD SEV. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 321-336). IEEE.
6. Anasuri, S. (2023). Confidential computing using trusted execution environments. *International Journal of AI, Big Data, Computational and Management Studies*, *4*(2), 97-110.
7. Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2023). TEBDS: A trusted execution environment-and-blockchain-supported IoT data sharing system. *Future Generation Computer Systems*, *140*, 321-330.
8. Park, J., Kang, S.,Lee, S.,Kim, T.,Park, J.,Kwon, Y.,Huh, J.(2024).Hardware-hardened sandbox enclaves for trusted serverless computing.*ACM Transactions on Architecture and Code Optimization*, *21* (1), 1-25.
9. Will, N. C., & Maziero, C. A. (2023, February). Efficient management models for SGX enclaves. In *International Conference on Information Systems Security and Privacy* (pp. 195-224). Springer.
10. Eboseremen, B. O., Ogedengbe, A. O., Obuse, E., Oladimeji, O., Ajayi, J. O., Akindemowo, A. O., & Erigha, E. D. (2022). Secure data integration in multi-tenant cloud environments: Architecture for financial services providers. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 579-592.
11. Voievodin, Y. V., & Rozlomii, I. O. (2024, April). Advanced software framework for comparing balancing strategies in container orchestration systems. In *Proceedings of the conference* (pp. 60-69).
12. Hamidy, G. M., Yulianti, S., Philippaerts, P., & Joosen, W. (2023, November). TC4SE: A high-performance trusted channel mechanism for secure enclave-based trusted execution environments. In *International Conference on Information Security* (pp. 246-264). Springer.
13. Pradhan, G., & Priyadarsini, M. (2024). A trusted computing framework for cloud data security using role-based access and pattern recognition. *Cluster Computing*, *27*(5), 6609-6622.
14. Vuppala, N. S. M., Hebbar, K. S., Gupta, D., Sharma, V., & Roy, V. (2025, December). Advanced security framework for threat mitigation in cloud computing environments. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.
15. Modaber, M., Hendriks, M., Geilen, M., Basten, T., Voeten, J.(2024). A method for building trustworthy hybrid performance models for cyber-physical systems of systems. *IEEE Access*, *12*, 92733-92752.
16. Kang, D. M., Faahym, H., Meftah, S., Keoh, S. L., & Khin, M. M. A. (2023, March). Practical deep neural network protection for unmodified applications in Intel software guard extension environments. In *International Conference on Critical Infrastructure Protection* (pp. 177-192). Springer.
17. Tara, A., & Khan, T. U. (2025, April). A comparative study of hardware-based and software-based secure virtualization technologies. In *Computer Science On-line Conference* (pp. 69-95). Springer.
18. Islam, M. S., Zamani, M., Kim, C. H., Khan, L., & Hamlen, K. W. (2023, April). Confidential execution of deep learning inference at the untrusted edge with ARM TrustZone. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy* (pp. 153-164). ACM.
19. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2023). Analysis of information security issues in balancing multiple independent containers on a single server. In *Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems* (pp. 450-461).
20. Ayamga, D., Nanda, P., & Mohanty, M. (2024, December). The Bell-LaPadula (BLP) enterprise security architecture model vs inference attacks. In *2024 17th International Conference on Security of Information and Networks (SIN)* (pp. 1-8). IEEE.
21. Haloua, F., Abbas, M., Djerbi, R., & Bouhamed, M. M. (2024, April). Formal modelling and implementation of Clark–Wilson security policy with FoCaLiZe. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)* (pp. 1-5). IEEE.
22. Yu, J. Z., Shinde, S., Carlson, T. E., & Saxena, P. (2022).Elasticlave:An efficient memory model for enclaves.In *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)* (pp. 4111-4128).
23. Lee, D., Cheang, K., Thomas, A., Lu, C., Gaddamadugu, P., Vahldiek-Oberwagner, A., & Asanović, K. (2022, November). Cerberus: A formal approach to secure and efficient enclave memory sharing. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1871-1885). ACM.

Отримано редакцією журналу / Received: 30.01.26
Прорецензовано / Revised: 12.02.26
Схвалено до друку / Accepted: 25.06.26