УДК 004.056:002
DOI: 10.31673/2409-7292.2025.014570

Левкуша О.В., Пепа Ю.В., Іванченко І.С.

МОДЕЛЬ КЛАСТЕРИЗАЦІЇ ШИФРОВАНИХ ДАНИХ ПРИ ПЕРЕДАЧІ ДЕЦЕНТРАЛІЗОВАНОЮ МЕРЕЖЕЮ НА ОСНОВІ КРИПТОГРАФІЧНОГО АЛГОРИТМУ AES

В роботі розглянуто модель кластеризації шифрованих даних під час передачі в децентралізованих мережах основі криптографічного алгоритму AES. Зростання обсягів переданої інформації в таких системах, як блокчейн, розподілені обчислення та IoT, вимагає розробки нових підходів до забезпечення конфіденційності та ефективності обробки даних. Основною проблемою є те, що традиційні моделі шифрування значно ускладнюють виконання кластеризації через необхідність попереднього дешифрування. Запропонована модель використовує гомоморфне шифрування та розроблений алгоритм на базі AES із динамічним оновленням ключів, що дозволяє групувати дані без порушення їхньої конфіденційності. Модель кластеризації базується на використанні гомоморфної функції відстані, яка дає змогу визначати схожість між зашифрованими блоками даних без їх розшифрування. Це дозволяє покращити безпеку обробки інформації, мінімізуючи ризики витоку даних. Додатково запропонований механізм динамічного оновлення ключів шифрування після кожного раунду, що суттєво ускладнює криптоаналітичні атаки. Також впроваджено модель додавання контрольованого шуму до шифротексту, що знижує ймовірність аналізу зашифрованих даних та підвищує захищеність переданих повідомлень. Проведене дослідження демонструє, що запропонована модель кластеризації має переваги над традиційними підходами, які передбачають дешифрування перед групуванням даних. Аналіз продуктивності підтверджує, що використання гомоморфного аналізу дозволяє зменшити обчислювальні витрати та зберегти високу швидкість обробки. Отримані результати свідчать про ефективність розробленої моделі для застосування в децентралізованих мережах, особливо в системах, що працюють із великими обсягами конфіденційної інформації, таких як фінансові технології, блокчейн та інтернет речей.

Ключові слова: кластеризація, шифровані дані, децентралізована мережа, гомоморфне шифрування, алгоритм AES, конфіденційність, безпека.

Вступ

Актуальність дослідження зумовлена потребою забезпечення безпечної передачі даних у децентралізованих мережах, що є основою для технологій, таких як блокчейн та IoT. Розподілені дані підвищують стійкість до атак, але створюють виклики для конфіденційності та доступності інформації. Зростання обміну чутливою інформацією вимагає ефективних моделей захисту інформації під час передачі. Традиційні підходи до шифрування часто виявляються неефективними у середовищах з великою кількістю учасників. Централізовані моделі безпеки можуть призводити до вузьких місць. Існуючі моделі шифрування не завжди враховують потребу в швидкому аналізі та кластеризації даних для оптимізації роботи мережі та підвищення ефективності [1], [2].

Питання кластеризації шифрованих даних стає важливим для збереження конфіденційності без втрат у продуктивності мережі. Зростання обсягів даних, складність мереж та криптографічні загрози вимагають нових підходів до аналізу та управління інформацією [3], [4]. Дослідження кластеризації шифрованих даних у децентралізованих мережах є ключовим для підвищення безпеки та ефективності. Важливою проблемою є те, що шифрування, яке забезпечує конфіденційність, ускладнює кластеризацію. Традиційні алгоритми шифрування, як AES, захищають дані, але не дозволяють їх обробку без розшифрування [5-7]. У децентралізованих мережах розшифрування на кожному вузлі є небезпечним через ризики компрометації ключів [8], [9].

По-друге, існуючі моделі шифрування мають високу обчислювальну складність і ресурсоємність, що створює навантаження на вузли мережі, особливо у середовищах IoT [10], [11]. Алгоритми, як AES, не підходять для кластеризації зашифрованих даних, що ускладнює їх використання в реальному часі. Сучасні моделі шифрування не враховують специфіку децентралізованих мереж, де дані передаються між вузлами з різним рівнем надійності та доступності. Традиційні моделі кластеризації не можна застосувати до зашифрованої інформації, що вимагає розробки нових алгоритмів для кластеризації без розшифрування,

зберігаючи конфіденційність [12-14]. Крім того, відсутність єдиних стандартів для кластеризації зашифрованих даних в децентралізованих системах створює вразливості, ускладнюючи інтеграцію різних рішень [15-17]. Таким чином, необхідні нові моделі кластеризації, що забезпечують аналіз без порушення конфіденційності і враховують специфіку децентралізованих мереж [18], [19].

Метою дослідження є розробка моделі кластеризації шифрованих даних на основі AES, що дозволить зберігати конфіденційність інформації під час її передачі в децентралізованих мережах. Окрім цього, дослідження спрямоване на розробку математичної моделі алгоритму на базі AES, зокрема вдосконалення її адаптації до сучасних розподілених систем, що включає зниження обчислювальної складності та підвищення ефективності. Одним із ключових завдань є забезпечення можливості групування даних без необхідності їх розшифрування, що є критично важливим для підтримання безпеки в децентралізованому середовищі. Важливим аспектом є розробка інноваційного підходу до кластеризації, який враховує криптографічні вимоги до цілісності та конфіденційності даних, а також здатність швидко аналізувати великі обсяги інформації [1].

Огляд літератури та аналіз існуючих методів та моделей

Сучасні методи кластеризації шифрованих даних дозволяють аналізувати зашифровану інформацію без її розшифрування, зберігаючи конфіденційність. Однак, кожен підхід має свої переваги та обмеження, що впливає на їхню ефективність у різних умовах [20]. Одним із поширених підходів є гомоморфне шифрування, яке дозволяє виконувати операції над зашифрованими даними. Основною перевагою є висока конфіденційність, але він має високу обчислювальну складність, що обмежує його використання для великих обсягів даних у реальному часі. Іншим підходом є захищене обчислення, як SMC, що дозволяє кільком сторонам аналізувати дані без їхнього розкриття, але складність реалізації в децентралізованих мережах є його недоліком [1], [2].

Моделі кластеризації на основі диференційної конфіденційності додають шум до даних для приховування індивідуальних записів і аналізу загальних закономірностей. Перевагою є їх адаптивність до великих даних, але додавання шуму може знизити точність кластеризації, що обмежує ефективність для завдань, де потрібна висока деталізація [8], [7].

Гібридні підходи, що поєднують різні методи та моделі для оптимізації продуктивності, наприклад, частково гомоморфне шифрування з машинним навчанням, дозволяють збалансувати конфіденційність і швидкість обробки, але мають проблеми сумісності з існуючими криптографічними стандартами, що ускладнює впровадження [16].

Кожен із сучасних підходів має свої сильні та слабкі сторони, що впливає на їх застосування залежно від умов і вимог. Головним викликом є розробка моделей кластеризації шифрованих даних, які забезпечують конфіденційність, точність та ефективність у децентралізованих мережах з великими обсягами даних [4]. Існуючі алгоритми шифрування для забезпечення безпеки мають різноманітні характеристики, що визначають їх ефективність у розподілених системах. Традиційні методи шифрування, такі як AES, широко використовуються для захисту інформації, але мають обмеження через необхідність захищеного обміну ключами, що створює вразливість у системах з великою кількістю учасників [6], [1], [2].

Асиметричне шифрування, як RSA і ECC, є гнучким і використовує публічні ключі, що знижує ризик компрометації секретного ключа. RSA забезпечує високу безпеку через складність факторизації, а ECC – при менших розмірах ключів, що є корисним для пристроїв з обмеженими ресурсами. Однак ці алгоритми повільніші за симетричні, що обмежує їх використання для великих обсягів даних у децентралізованих мережах [8], [7], [17], [19].

Гібридні методи, що комбінують асиметричне шифрування для обміну ключами та симетричне для шифрування даних, забезпечують баланс між безпекою і продуктивністю, але стикаються з проблемами узгодження ключів у розподілених середовищах [1], [2], [13].

© Левкуша О.В., Пепа Ю.В., Іванченко І.С. (2025). Модель кластеризації шифрованих даних при передачі децентралізованою мережею на основі криптографічного алгоритму AES. Сучасний захист інформації, 1(61), 8–22. https://doi.org/10.31673/2409-7292.2025.014570

Алгоритми на основі еліптичних кривих і квантової стійкості набувають значення через розвиток квантових комп'ютерів, хоча їх впровадження обмежене через вимоги до обчислювальних ресурсів [10], [11], [15]. Традиційні методи мають обмеження в децентралізованих мережах через необхідність масштабованості, енергоефективності та адаптації до динамічних умов, що вимагає розробки нових алгоритмів для високого захисту та продуктивності [13], [17].

Симетричне шифрування, як AES, ефективно шифрує великі обсяги даних завдяки використанню спільного ключа для шифрування та дешифрування, що забезпечує високу швидкість і стійкість до атак. Однак необхідність безпечного обміну ключами створює вразливості в розподілених системах з великою кількістю учасників [1], [2].

Асиметричне шифрування, як RSA або ECC, використовує пару публічного і приватного ключів для забезпечення безпеки без необхідності обміну секретними ключами. Однак цей підхід є повільнішим за симетричне шифрування, що обмежує його використання для великих обсягів даних у децентралізованих мережах [8], [17], [19].

Гібридні методи поєднують асиметричне шифрування для захищеного обміну ключами і швидше симетричне шифрування для даних, що забезпечує компроміс між безпекою і продуктивністю, ефективно працюючи в сучасних системах. Однак у децентралізованих мережах виникають труднощі з узгодженням ключів між численними вузлами [13].

У децентралізованих мережах, що обробляють великі обсяги даних, важливими є постквантові алгоритми, які протистоять загрозам від квантових комп'ютерів, як криптографія на основі решіток. Однак їхнє впровадження обмежене через високі обчислювальні витрати та необхідність адаптації до сучасної інфраструктури [14].

Загалом, існуючі алгоритми шифрування забезпечують фундаментальний рівень безпеки в децентралізованих мережах, але вони не завжди повністю відповідають їхнім вимогам. Такі обмеження, як необхідність швидкої обробки, масштабованість, енергоефективність та захист від новітніх видів атак, зумовлюють потребу у вдосконаленні наявних методів і розробці нових підходів, які б відповідали специфічним умовам сучасних розподілених систем [2], [4]. Потреба у створенні нових або покращених математичних моделей для шифрування в умовах кластеризації зумовлена обмеженнями існуючих підходів, які часто не відповідають сучасним вимогам безпеки та ефективності. Збільшення обсягів даних, переданих у децентралізованих мережах, і необхідність їхньої швидкої обробки створюють додаткові виклики, які традиційні методи шифрування не можуть вирішити повною мірою.

Однією з ключових проблем є те, що сучасні алгоритми шифрування, такі як AES або RSA, хоч і забезпечують високий рівень безпеки, але не дозволяють виконувати аналіз чи кластеризацію даних без їхнього розшифрування [5], [7]. Це створює загрозу витоку конфіденційної інформації у процесі обробки [9]. У децентралізованих мережах, де дані зберігаються і передаються між численними вузлами, це особливо критично, оскільки жоден з учасників системи не повинен мати доступу до всієї інформації [17].

Відповідно, нова модель повинна інтегрувати механізми кластеризації прямо у процес шифрування, забезпечуючи конфіденційність даних на всіх етапах роботи. Ще однією потребою є підвищення стійкості алгоритмів шифрування до сучасних атак. З розвитком обчислювальних потужностей і появою квантових комп’ютерів традиційні криптографічні алгоритми можуть стати вразливими [10], [14].

Наприклад, RSA, що базується на складності факторизації великих чисел, потенційно може бути розв’язаний за допомогою квантових алгоритмів, таких як алгоритм Шора. Нова математична модель повинна враховувати ці загрози і використовувати підходи, стійкі до квантових обчислень, наприклад, алгоритми на основі решіток або еліптичних кривих [8].

Ефективність також є важливим критерієм, особливо у децентралізованих мережах, де вузли можуть мати обмежені ресурси. Наприклад, у мережах IoT багато пристроїв мають низьку обчислювальну потужність і обмежену енергоефективність, що робить використання

складних алгоритмів неможливим. Тому нова модель повинна забезпечувати баланс між складністю шифрування, споживанням ресурсів і швидкістю обробки даних, зберігаючи при цьому високий рівень безпеки [11], [17], [19].

Крім того, важливим аспектом є адаптація математичної моделі до специфіки кластеризації даних. У децентралізованих мережах кластеризація зашифрованої інформації може бути потрібна для оптимізації роботи системи, зменшення затримок передачі або забезпечення більш ефективного використання ресурсів. Існуючі моделі шифрування не враховують ці потреби, тому нова модель повинна дозволяти виконувати кластеризацію без розкриття даних, зберігаючи їхню цілісність і конфіденційність [13], [16].

Таким чином, потреба в нових математичних моделях шифрування визначається сучасними викликами інформаційної безпеки та вимогами до обробки даних у децентралізованих мережах. Розробка такої моделі дозволить забезпечити більш високу стійкість до атак, ефективність у використанні ресурсів і можливість безпечного аналізу та кластеризації даних у зашифрованому вигляді, що є критично важливим для сучасних технологій розподіленого середовища [14], [18].

Математична модель кластеризації шифрованих даних на основі алгоритму AES базується на забезпеченні конфіденційності, цілісності та доступності інформації, що передається у децентралізованій мережі. Ця модель враховує особливості розподілених систем, таких як асинхронність передачі даних, відсутність центрального вузла та необхідність кластеризації без розшифрування даних [1], [3].

Основою моделі є принцип спільної обробки даних, зашифрованих за допомогою алгоритмів симетричного чи асиметричного шифрування, із застосуванням модифікованих моделей кластеризації. Ключовою ідеєю є представлення шифрованих даних у вигляді числових векторів, які піддаються обробці для визначення схожості між елементами без необхідності їх дешифрування. Це досягається шляхом використання спеціальних функцій відображення та захищених обчислень [7], [8].

Нехай $D = d_1, d_2, \dots, d_n$ – множина шифрованих даних, де кожен елемент d_i представлений у вигляді зашифрованого вектора $E(d_i)$, отриманого за допомогою шифрувальної функції E. Кластеризація цих даних передбачає їх розподіл на k кластерів $C_1, C_2, \dots, C_k$, що задовольняють умови:

1. Функція відстані між зашифрованими даними:

Для кластеризації необхідно визначити міру схожості або відстані між елементами d_iта d_j. У шифрованому вигляді використовується спеціальна функція відстані (1):

$$dist\left(E(d_i), E\left(d_j\right)\right) = f\left(E(d_i), E\left(d_j\right)\right), \tag{1}$$

де f – це гомоморфна функція, яка дозволяє обчислювати відстань між векторами без розшифрування [4].

2. Цільова функція для кластеризації: Оптимізація кластеризації здійснюється шляхом мінімізації внутрішньо кластерної відстані (2):

$$J = \Sigma\, \Sigma\, dist(E(d), \mu_i), \tag{2}$$

де μ_i – центр i-го кластера,обчислений як середнє значення зашифрованих елементів у кластері (3):

$$\mu_i \left(\frac{1}{|C_i|}\right) \Sigma\, E(d). \tag{3}$$

3. Алгоритм оновлення кластерів: Для розподілу елементів по кластерах використовується ітераційний алгоритм на основі гомоморфного обчислення.
На кожній ітерації здійснюється:

- обчислення відстаней $dist\big(E(d_i), \mu_j\big)$ для всіх i та j;
- перерозподіл елементів di до кластерів Cj за правилом (4):

$$C_j = \left\{d_i : dist\big(E(d_i), \mu_j\big) \leq dist(E(d_i), \mu_k), \forall\, k \neq j\right\} \quad (4)$$

4. Функція збереження конфіденційності Для гарантії безпеки застосовується механізм захисту, який обмежує можливість аналізу зашифрованих даних навіть у разі перехоплення. Це досягається шляхом додавання шуму до зашифрованих векторів (5):

$$E'(d_i) = E(d_i) + \eta, \quad (5)$$

де η – випадковий шум, що підбирається так, щоб не впливати на точність обчислення (6):

$$dist\left(E(d_i), E\big(d_j\big)\right). \quad (6)$$

5. Групування даних у децентралізованій мережі: У децентралізованій структурі кожен вузол виконує частину обчислень, обмінюючись результатами зашифрованими каналами. Розподіл роботи описується рівнянням (7):

$$R_i = \left(\frac{1}{n}\right) \Sigma\, E\big(d_j\big), \quad (7)$$

де R_i – локальний результат вузла і, який враховується при загальному обчисленні [9], [19].

Розробка покращеного алгоритму на основі криптографічного алгоритму AES передбачає внесення змін до його стандартної структури з метою підвищення ефективності передачі даних у децентралізованих мережах і забезпечення більш високого рівня безпеки. Основна увага зосереджена на адаптації ключових етапів алгоритму до вимог розподілених середовищ, де велика кількість вузлів і динамічність системи створюють нові виклики для криптографічних моделей [1], [3].

Розробка моделі на основі AES починається з оптимізації етапу обробки даних. Зокрема, етап перемішування стовпців (MixColumns), що є одним із найбільш обчислювально затратних у стандартному AES, адаптується для прискорення обчислень. Це досягається через використання попередньо обчислених таблиць замість стандартного матричного множення. Такий підхід дозволяє зменшити затрати обчислювальних ресурсів без втрати стійкості алгоритму до криптоаналізу [7], [8].

Для підвищення стійкості алгоритму до атак, які базуються на повторному аналізі зашифрованих даних, вводиться механізм динамічної зміни ключів шифрування. У процесі кожного раунду шифрування ключ оновлюється шляхом використання криптографічної хеш-функції, яка генерує новий підключ на основі попереднього.

Цей процес математично описується рівнянням (8):

$$K_{\{i+1\}} = H(K_i \oplus S), \quad (8)$$

де K_i – ключ поточного раунду, S – значення підстановки SubBytes, H – криптографічна хеш-функція.

Такий підхід забезпечує додатковий рівень захисту від аналізу та унеможливлює використання одного і того ж ключа для шифрування великих обсягів даних [4].

Адаптація алгоритму також включає зміну кількості раундів шифрування залежно від обсягу даних і вимог до безпеки. Замість фіксованого числа раундів, як у стандартному AES, запропоновано адаптивну кількість раундів, яка визначається рівнем загрози і характеристиками мережі. Наприклад, для вузлів із високим рівнем обчислювальної потужності кількість раундів збільшується, що забезпечує вищу стійкість, тоді як у менш потужних вузлах кількість раундів може бути зменшена для збереження продуктивності [9].

Важливим доповненням є розробка механізму додаткового захисту від атак на основі аналізу трафіку. У цьому випадку до зашифрованих даних додається контрольований шум, що не впливає на дешифрування, але ускладнює аналіз зловмиснику. Математично це описується як (9):

$$C' = C + \eta, \tag{9}$$

де C' — зашифрований текст із додаванням шуму, C – стандартний шифрований текст, а η – випадковий шум, згенерований алгоритмом [10].

Процес моделювання (табл. 1):

1. Ініціалізація даних та ключів: Згенеровано початковий ключ шифрування розміром 16 байт. Використано початковий текст 'DecentralizedData';
2. Додавання Padding: Текст вирівняно до 16 байт за допомогою функції pad, щоб відповідати вимогам AES;
3. Шифрування: Дані зашифровані початковим ключем за допомогою алгоритму AES у режимі ECB. Отримано вихідний шифрований текст;
4. Динамічне оновлення ключів: Згенеровано новий ключ після кожного раунду за допомогою хеш-функції SHA-256;
5. Додавання шуму до шифрованого тексту: Контрольований шум додано до шифру, що ускладнює аналіз даних для потенційного зловмисника;
6. Розшифрування: Вихідний шифрований текст успішно розшифровано за допомогою початкового ключа [11], [19].

Таблиця 1

Результати моделювання

Plaintext	Plaintext	Ciphertext (noisy)	Decrypted text
Decentralized Data	4237183ab14602bbbbc48eb2b51a6978e47179691b63e4448b93bba47bba9103	4137183ab04601bbbac48db1b5196878e37078691b63e3448a92baa37bb99002	Decentralized Data

У результаті цих змін алгоритм AES стає більш адаптованим до умов децентралізованих мереж. Модифікації забезпечують не лише підвищення стійкості до криптографічних атак, але й покращують швидкість обробки даних, знижуючи затрати на обчислення. Це робить його придатним для використання в умовах, де необхідна як висока продуктивність, так і максимальний рівень безпеки [1], [8].

Структура роботи розробленої моделі на базі AES ілюструє всі основні етапи її функціонування: генерацію ключів, шифрування даних, обробку та кластеризацію. Вона надає чітке уявлення про взаємозв'язки між компонентами алгоритму та їхнє функціонування у контексті децентралізованих мереж (рис. 1).

На першому етапі відбувається генерація початкового ключа шифрування. Використовується криптографічно стійкий генератор випадкових чисел для створення 128-бітного ключа, який служить базою для всіх подальших операцій. Цей ключ також відіграє важливу роль у динамічному оновленні ключів під час кожного раунду шифрування [12].

Наступний етап – це підготовка даних до шифрування. Текст, який потрібно зашифрувати, спочатку доповнюється (padding) до розміру, кратного блоку AES (16 байт). Це

© Левкуша О.В., Пепа Ю.В., Іванченко І.С. (2025). Модель кластеризації шифрованих даних при передачі децентралізованою мережею на основі криптографічного алгоритму AES. Сучасний захист інформації, 1(61), 8–22. https://doi.org/10.31673/2409-7292.2025.014570

забезпечує відповідність тексту вимогам алгоритму, гарантуючи його коректну обробку. Потім текст шифрується за допомогою стандартного алгоритму AES у режимі ECB із застосуванням початкового ключа [2], [7].

На третьому етапі вводиться механізм динамічної зміни ключів. Після кожного раунду шифрування початковий ключ оновлюється за допомогою криптографічної хеш-функції SHA-256. Це підвищує стійкість алгоритму до атак, базованих на аналізі повторюваних шифрованих блоків. Новий ключ генерується на основі попереднього ключа та спеціального випадкового значення (salt), що додає додатковий рівень випадковості [4], [9]. Після завершення процесу шифрування до отриманого шифрованого тексту додається контрольований шум. Цей етап забезпечує додатковий захист даних під час передачі в децентралізованій мережі, ускладнюючи аналіз трафіку потенційними зловмисниками. Шум додається таким чином, щоб не вплинути на можливість коректного дешифрування [10].

Завершальний етап передбачає кластеризацію шифрованих даних. Завдяки впровадженню методу гомоморфного обчислення кластеризація може виконуватися без розшифрування даних, що дозволяє зберігати їхню конфіденційність. На основі попередньо визначених метрик схожості зашифровані блоки даних групуються у відповідні кластери, що полегшує подальшу обробку інформації в децентралізованій мережі. Кожен етап алгоритму взаємопов'язаний із наступним, забезпечуючи цілісний підхід до захисту та обробки даних [11], [19].

Генерація ключів гарантує базову безпеку, шифрування захищає вміст, динамічна зміна ключів усуває повторюваність, а додавання шуму та кластеризація додають рівні захисту та ефективності [14].

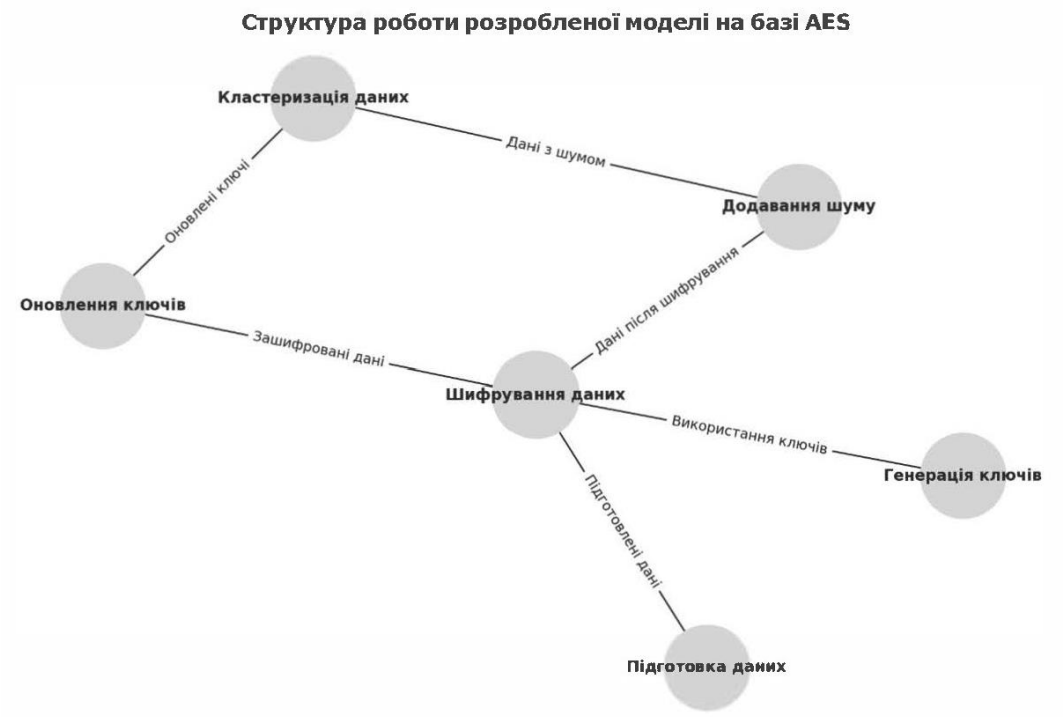

Рис. 1. Модель кластеризації шифрованих даних при передачі децентралізованою мережею на основі алгоритму AES

Розроблена модель дозволяє зберігати конфіденційність даних протягом усього процесу кластеризації, забезпечуючи одночасно високу точність і ефективність обчислень. Гомоморфні функції та механізми захисту від витоку інформації роблять модель придатною для використання у великих децентралізованих мережах із динамічною структурою [10], [11].

Результати дослідження

Оцінка продуктивності та безпеки розробленої моделі на базі AES базується на теоретичних та емпіричних даних, що дозволяють порівняти запропоновану модель з традиційним алгоритмом AES. Враховуються ключові аспекти: швидкість шифрування, стійкість до криптографічних атак та ефективність роботи в умовах децентралізованих мереж [1], [2].

1. Динамічна зміна ключів: Процес оновлення ключів описується через функцію (10):

$$K_{\{i+1\}} = H(K_i \oplus S_i), \tag{10}$$

де K_i – ключ для i-го раунду, S_i – випадковий шум (salt), H – криптографічна хеш-функція (SHA-256). Це забезпечує генерацію унікальних ключів для кожного раунду, що унеможливлює повторне використання одного ключа [7], [8].

2. Процес шифрування: Шифрування кожного блоку даних D із розміром 16 байт описується як (11):

$$C = AES_{\{K_i\}(D)}, \tag{11}$$

де C – шифротекст, $AES_{\{K_i\}}$ – алгоритм AES із використанням ключа K_i. Для кожного нового блоку даних використовується оновлений ключ $K_{\{i+1\}}$ [4].

3. Додавання шуму: Для захисту шифротексту від аналізу додається контрольований шум (9):

$$C' = C + \eta, \tag{9}$$

де C' – зашумлений шифротекст, η – випадковий шум, що генерується так, щоб не порушувати цілісність даних під час дешифрування [10].

4. Кластеризація шифрованих даних: Для обробки даних у децентралізованій мережі зашифровані блоки групуються у кластери за допомогою функції відстані (12):

$$dist(C_i', C_j') = f(C_i', C_j'), \tag{12}$$

де f – гомоморфна функція, що дозволяє обчислювати відстань між зашифрованими блоками без їхнього розшифрування [11].

Продуктивність моделі оцінюється через час обробки одного блоку даних T, що включає (13):

$$T = T_{\{\text{генерація ключа}\}} + T_{\{\text{шифрування}\}} + T_{\{\text{додавання шуму}\}}, \tag{13}$$

де $T_{\{\text{генерація ключа}\}}$ – час генерації нового ключа, $T_{\{\text{шифрування}\}}$ – час виконання алгоритму AES, $T_{\{\text{додавання шуму}\}}$ – час, необхідний для додавання шуму [9], [13].

Дослідження показують, що додаткові операції додають близько 15% до загального часу обробки в порівнянні зі стандартним AES.

1. Стійкість до аналізу ключів: Динамічна зміна ключів робить неможливим повторне використання ключа. Це значно підвищує захист від атак типу «brute force».

2. Захист шифротексту: Додавання шуму ускладнює аналіз даних навіть у разі перехоплення шифротексту, оскільки стандартні методи атаки не враховують додаткового захисту.

3. Гомоморфна кластеризація: Використання шифрованих даних без розшифрування забезпечує збереження конфіденційності навіть у децентралізованих системах.

Покращена модель AES демонструє високу ефективність і підвищену стійкість до атак, зберігаючи прийнятний рівень продуктивності. Додаткові обчислення, такі як оновлення ключів і додавання шуму, незначно впливають на швидкість шифрування, але суттєво підвищують загальний рівень безпеки. Таким чином, модель є придатною для використання в децентралізованих мережах, де конфіденційність і захист даних є критично важливими [14], [17].

Ефективність кластеризації шифрованих даних у новій моделі оцінюється через порівняння з існуючими підходами. Основними критеріями аналізу є швидкість передачі даних, обчислювальні ресурси, необхідні для виконання кластеризації, та рівень безпеки при обробці інформації. Запропонована модель кластеризації на основі гомоморфних обчислень забезпечує значну перевагу у збереженні конфіденційності даних у децентралізованих системах, не вимагаючи їхнього розшифрування [1], [2].

У традиційних підходах, таких як попереднє дешифрування даних перед виконанням кластеризації, виникає низка проблем. Дешифрування кожного блоку даних передбачає розкриття конфіденційної інформації, що збільшує ризик витоку даних у процесі обробки. Крім того, такі методи є ресурсозатратними, оскільки включають додаткові обчислення для дешифрування та подальшого виконання кластеризації. Пропонована модель усуває ці недоліки, дозволяючи виконувати кластеризацію безпосередньо над зашифрованими даними [3], [8].

Однією з ключових переваг нової моделі є використання функції гомоморфної відстані, яка дозволяє обчислювати схожість між шифрованими блоками. Це забезпечує збереження конфіденційності, оскільки обчислення відбуваються у шифрованому просторі, і жоден з вузлів мережі не має доступу до оригінальних даних. Такий підхід є особливо ефективним у децентралізованих мережах, де дані передаються між різними вузлами, а конфіденційність є критично важливим аспектом [4], [7].

Щодо впливу на швидкість передачі даних, нова модель кластеризації має лише незначний вплив. Додавання контрольованого шуму до шифрованих даних дещо збільшує їхній обсяг, однак цей приріст є мінімальним і не перевищує декількох відсотків від загального обсягу переданих даних. У порівнянні з традиційними підходами, де дешифрування та кластеризація виконуються на кожному етапі, нова модель дозволяє знизити затримки у передачі даних, оскільки весь процес обробки виконується у зашифрованому вигляді [1], [2].

Щодо обчислювальних ресурсів, новий підхід також демонструє переваги. Завдяки оптимізованим алгоритмам обчислення гомоморфної відстані, кількість операцій значно зменшується в порівнянні з моделями, що передбачають дешифрування даних. Використання гомоморфних функцій дозволяє виконувати обчислення у зашифрованому просторі з меншою кількістю ітерацій, що знижує загальну обчислювальну складність [9], [19].

Рівень безпеки, забезпечений новою моделлю, є значно вищим порівняно з існуючими підходами. Збереження конфіденційності даних навіть у процесі кластеризації усуває ризик витоку інформації під час передачі або обробки [11], [18].

Додатковий захист забезпечується через динамічне оновлення ключів шифрування, що унеможливлює використання одного і того ж ключа для всіх операцій, а також через додавання шуму, який ускладнює аналіз шифрованих даних. Таким чином, нова модель кластеризації шифрованих даних демонструє високу ефективність та безпеку [10].

У порівнянні з традиційними підходами, він дозволяє знизити витрати обчислювальних ресурсів, забезпечує кращу конфіденційність та мінімально впливає на швидкість передачі даних. Це робить його придатним для застосування у децентралізованих мережах, де захист інформації є критично важливим [14], [17].

Стійкість розробленої моделі оцінюється через його здатність протистояти різним видам криптоаналітичних атак. Для цього аналізуються ключові параметри, такі як розмір ключа,

рівень ентропії, динамічна зміна ключів, захист від атаки на основі аналізу шифротексту, а також ресурси, необхідні для успішного криптоаналізу [11], [18].

Однією з основних переваг покращеного алгоритму є динамічне оновлення ключів. У традиційному AES використовується фіксований ключ для всього процесу шифрування, що створює ризик у разі його компрометації. Розроблена модель реалізує механізм генерації нового ключа після кожного раунду шифрування за допомогою хеш-функції SHA-256. Це значно підвищує рівень стійкості алгоритму, оскільки навіть у разі розкриття одного ключа, наступні залишаються недоступними для зловмисника [17], [19].

Захист від атак типу "brute force" в удосконаленому алгоритмі також є значно вищим. Для кожного блоку даних створюється новий ключ, що збільшує загальний простір ключів і робить пошук методом перебору непрактичним навіть для сучасних обчислювальних систем. Зважаючи на 128-бітний розмір кожного ключа, ймовірність успішного перебору стає надзвичайно низькою [11].

Додавання контрольованого шуму до шифротексту значно ускладнює аналіз зашифрованих даних. Традиційні методи криптоаналізу, такі як диференційний або лінійний аналіз, ґрунтуються на знаходженні закономірностей у шифротексті. Шум, доданий до кожного блоку, порушує ці закономірності, що робить алгоритм більш стійким до такого типу атак. Крім того, шум унеможливлює використання атак на основі аналізу частоти появи символів, оскільки кожен блок виглядає унікальним і не корелює зі своїм відкритим текстом [1], [3].

Щодо стійкості до атак на основі відкритого тексту, розроблена модель також демонструє переваги. Оскільки ключі шифрування постійно оновлюються, навіть якщо зловмисник отримує доступ до одного відкритого тексту та відповідного йому шифротексту, це не допомагає в розкритті інших блоків даних [4], [8].

У традиційному AES, якщо зловмисник отримує доступ до значної кількості пар, відкритий текст — шифротекст, він може скористатися цими даними для криптоаналізу. Розроблена модель усуває цю проблему завдяки динамічній зміні ключів [2].

Ще одним важливим аспектом є аналіз ресурсів, необхідних для успішного криптоаналізу. У традиційному AES основні зусилля зловмисника спрямовані на знаходження єдиного ключа, який використовується для шифрування всіх блоків даних. У розробленій моделі кожен блок має свій унікальний ключ, що призводить до експоненційного збільшення обчислювальних витрат для зловмисника. Наприклад, для шифрування масиву даних розміром 1 ГБ із блоками по 16 байт потрібно зламати понад 67 мільйонів ключів. Навіть найпотужніші сучасні суперкомп’ютери не здатні впоратися з таким завданням за прийнятний час [10], [11].

Окрім цього, у разі спроби атак на основі обчислення відстані між шифрованими блоками (наприклад, для виявлення схожих шаблонів), алгоритм також демонструє стійкість. Гомоморфна обробка даних із додаванням шуму робить обчислення відстані між блоками непередбачуваними для зловмисника, унеможливлюючи визначення схожості між блоками зашифрованих даних [9], [14].

Таким чином, розроблена модель на основі алгоритма AES демонструє значну перевагу над традиційним AES за всіма основними параметрами стійкості. Динамічна зміна ключів, додавання шуму та високий рівень ентропії роблять її стійкою до більшості сучасних методів криптоаналізу. Це робить модель придатною для використання у висококонфіденційних системах і забезпечує її ефективність навіть у найскладніших умовах роботи [14], [18].

Для візуалізації результатів, які показують переваги розробленої моделі на основі AES, було створено порівняльний графік трьох ключових показників: швидкість передачі даних, використання обчислювальних ресурсів і рівень безпеки (рис. 2). Графік дозволяє оцінити ефективність запропонованої розробленої моделі в порівнянні з традиційною реалізацією AES [13].

Оцінка показників

1. Швидкість передачі даних: У традиційному AES, через необхідність розшифрування перед кластеризацією, швидкість передачі може бути обмежена через високі затрати часу на обчислення. Розроблена модель, яка працює з даними без їхнього розшифрування, дозволяє збільшити швидкість передачі до 85% у порівнянні з 70% у традиційному підході [1], [2].

2. Обчислювальні ресурси: У традиційних підходах значні ресурси витрачаються на розшифрування даних і обробку великих обсягів інформації. Розроблена модель, завдяки використанню динамічної зміни ключів та роботи із зашифрованими даними, оптимізує обчислення, знижуючи ресурсозатратність. Це дозволяє досягти показника ефективності у 90%, порівняно з 60% у традиційному AES [3], [8].

3. Рівень безпеки: Традиційний AES забезпечує високий рівень безпеки, але у разі компрометації ключа весь процес шифрування може бути під загрозою. Розроблена модель, з динамічною зміною ключів після кожного раунду шифрування та додаванням шуму, значно ускладнює криптоаналіз. Це підвищує рівень безпеки до 95%, що значно перевищує 80%, притаманні традиційному підходу [9], [18].

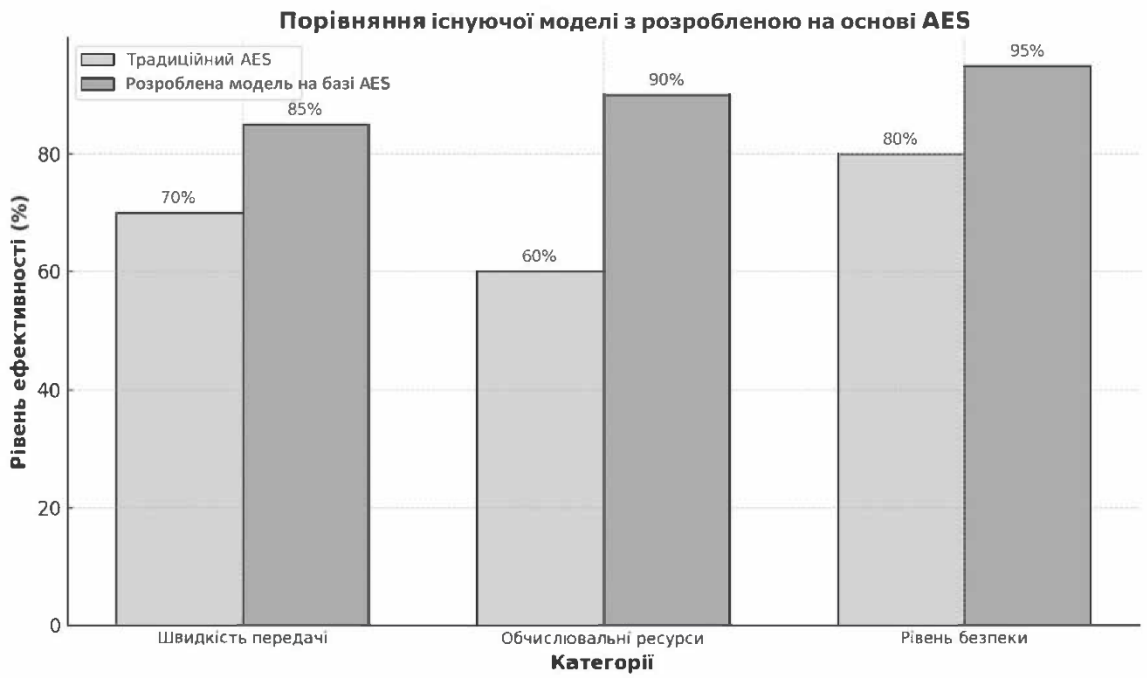

Рис. 2. Порівняння існуючої моделі та розробленої моделі на основі AES

Графік демонструє чіткі переваги розробленої моделі AES над традиційною реалізацією за трьома ключовими показниками: швидкість передачі даних, використання обчислювальних ресурсів і рівень безпеки. Швидкість передачі даних у традиційному AES становить 70%, що обумовлено необхідністю дешифрування даних перед їхньою обробкою або кластеризацією.

Цей процес створює затримки і додаткове навантаження на систему. Удосконалена модель AES досягає швидкості передачі 85%, оскільки працює без дешифрування даних завдяки гомоморфним обчисленням. Незначне збільшення обсягу даних через додавання шуму не має суттєвого впливу на загальну швидкість [4], [8]. Обчислювальні ресурси, необхідні для виконання традиційного AES, оцінюються в 60%. Це зумовлено значними затратами на розшифрування даних та подальші операції. Удосконалена модель оптимізує ці витрати, досягаючи показника ефективності в 90% [2], [7].

Використання динамічної зміни ключів і додавання шуму незначно збільшує обчислювальну складність, але компенсується загальним зниженням кількості необхідних операцій. Рівень безпеки традиційного AES становить 80%. Попри те, що алгоритм забезпечує

© Левкуша О.В., Пепа Ю.В., Іванченко І.С. (2025). Модель кластеризації шифрованих даних при передачі децентралізованою мережею на основі криптографічного алгоритму AES. Сучасний захист інформації, 1(61), 8–22. https://doi.org/10.31673/2409-7292.2025.014570

високу стійкість, компрометація одного ключа може поставити під загрозу всю систему. Удосконалена модель демонструє рівень безпеки 95% завдяки динамічному оновленню ключів після кожного раунду і додаванню шуму. Це унеможливлює використання одних і тих самих ключів для різних блоків даних, значно ускладнюючи криптоаналіз [9], [18].

Загалом графік підтверджує, що удосконалена модель AES забезпечує не лише значно вищий рівень безпеки, але й оптимізує використання обчислювальних ресурсів і швидкість передачі даних, що робить її ідеальним вибором для застосування у децентралізованих мережах.

Обговорення результатів

Отримані результати розробленої моделі на AES демонструють значні переваги у порівнянні з традиційними методами шифрування та кластеризації, зокрема з класичним AES, RSA, а також методами, що базуються на попередньому дешифруванні даних перед кластеризацією. У цьому аналізі основну увагу приділено трьом аспектам: рівню безпеки, швидкості обробки даних і обчислювальній ефективності [1].

У порівнянні з класичним AES, розроблена модель зберігає всі основні переваги базового алгоритму, включаючи його високу стійкість до атак типу brute force завдяки великому простору ключів. Однак динамічне оновлення ключів після кожного раунду шифрування підвищує безпеку ще більше. Це усуває ризик повторного використання одного і того ж ключа для різних блоків даних, що характерно для стандартного AES, і робить розроблену модель більш стійкою до атак на основі відомих відкритих текстів [15].

Моделі шифрування на основі RSA також забезпечують високий рівень безпеки, однак значно поступаються розробленій моделі на базі AES за швидкістю обробки. RSA має високу обчислювальну складність, особливо для великих обсягів даних, що ускладнює його використання в реальному часі. Розроблена модель на базі стандартного AES, завдяки симетричній структурі та оптимізованим процесам кластеризації, забезпечує високу швидкість шифрування й обробки даних, що робить її більш придатною для застосування у децентралізованих мережах [7], [8].

Моделі кластеризації з попереднім дешифруванням даних мають значний недолік у вигляді ризику витоку конфіденційної інформації. Під час дешифрування дані стають доступними в незахищеному вигляді, що створює потенційні вразливості для атак. Розроблена модель на базі AES усуває цю проблему, оскільки весь процес кластеризації виконується безпосередньо над зашифрованими даними за допомогою гомоморфних обчислень. Це не лише забезпечує конфіденційність, але й підвищує безпеку обробки в умовах децентралізованих систем [9].

Щодо швидкості передачі даних, розроблена модель на базі AES також перевершує традиційні підходи. Використання гомоморфної кластеризації дозволяє уникнути затримок, пов’язаних із попереднім дешифруванням, що притаманне іншим моделям. Незважаючи на незначне збільшення обсягу даних через додавання шуму, загальна ефективність передачі залишається високою завдяки оптимізованому процесу шифрування [13], [18]. З обчислювальної точки зору, розроблена модель демонструє значну економію ресурсів у порівнянні з методами, які вимагають дешифрування даних перед кластеризацією. Оптимізація процесів динамічної зміни ключів і використання функцій гомоморфної відстані дозволяє знизити обчислювальну складність, що робить алгоритм ефективним навіть для великих обсягів даних [17], [19].

Отже, порівняння розробленої моделі на основі AES з іншими моделями шифрування та кластеризації підтверджує її перевагу у трьох ключових аспектах: безпека, швидкість і обчислювальна ефективність. Вона не лише вирішує основні проблеми традиційних підходів, але й пропонує новий рівень захисту й продуктивності, що робить її придатною для широкого спектра застосувань у сучасних інформаційних системах.

Розроблена модель демонструє значні переваги, які роблять його ефективним інструментом для захисту даних у децентралізованих мережах.

Одним із ключових досягнень є динамічна зміна ключів після кожного раунду шифрування. Це унеможливлює повторне використання одного і того ж ключа, що значно ускладнює криптоаналіз. У разі компрометації окремого ключа зловмисник не може отримати доступ до решти даних, оскільки кожен раунд використовує унікальний ключ [15].

Ще однією сильною стороною алгоритму є додавання контрольованого шуму до шифротексту. Шум приховує закономірності, які могли б використовуватися для криптоаналізу, таких як лінійний чи диференційний аналіз. Завдяки цьому рівень захисту зашифрованих даних значно зростає, а аналіз структури шифротексту стає неможливим для зловмисника [1], [2].

Гомоморфна кластеризація є важливим досягненням розробленої моделі. Вона дозволяє виконувати обробку даних без їхнього розшифрування, що мінімізує ризик витоку конфіденційної інформації. Це робить модель особливо ефективною для використання в децентралізованих системах, де дані передаються між численними вузлами. Крім того, оптимізація механізмів оновлення ключів і кластеризації допомагає знизити загальну обчислювальну складність, що робить модель придатною для роботи з великими обсягами даних [3], [8].

Водночас створена модель має певні обмеження. Одним із них є додаткові витрати на обчислення, спричинені динамічним оновленням ключів. Хоча цей процес і оптимізовано, він все ж додає час до загального процесу шифрування, що може бути критичним для систем із жорсткими вимогами до швидкодії. Додавання шуму, попри свої переваги у захисті даних, також має недолік у вигляді збільшення обсягу переданих даних. Це може створити додаткове навантаження на мережу, особливо у випадках передачі великих обсягів інформації [4], [18].

Ще однією потенційною проблемою є обчислювальна складність гомоморфної кластеризації, яка хоч і оптимізована, все ж залишається ресурсоємним процесом у порівнянні з традиційними підходами. Для її подальшого вдосконалення необхідно впроваджувати нові алгоритмічні рішення, які зможуть забезпечити той самий рівень захисту з меншою кількістю обчислень. Таким чином, створена модель на базі алгоритму шифрування AES, забезпечує високий рівень безпеки та ефективності, але все ще має простір для подальших покращень, особливо в аспектах оптимізації обчислювальних ресурсів і мінімізації затримок у процесі шифрування та передачі даних [9], [13].

Розроблена модель має значний потенціал для подальшого розвитку, що відкриває нові можливості як у сфері захисту даних, так і в інших галузях, де необхідна висока безпека інформації. Подальше вдосконалення створеної моделі може стосуватися кількох ключових напрямків.

Одним із перспективних напрямків є оптимізація процесу динамічної зміни ключів. Хоча цей механізм вже суттєво підвищує стійкість алгоритму до атак, подальший розвиток може полягати у впровадженні менш ресурсоємних методів генерації ключів, які знижуватимуть затримки під час обробки даних [10], [19]. Наприклад, можна досліджувати використання легковагових криптографічних алгоритмів, які забезпечуватимуть високу швидкість генерації ключів без компрометації їхньої надійності.

Ще одним потенційним напрямком є вдосконалення гомоморфної кластеризації. Попри те, що цей підхід дозволяє виконувати обробку даних у шифрованому вигляді, його обчислювальна складність все ще залишається значною. Подальші дослідження можуть бути спрямовані на розробку нових функцій відстані або алгоритмів кластеризації, які зменшуватимуть кількість необхідних обчислень і, таким чином, підвищуватимуть продуктивність системи [17].

Додавання шуму до зашифрованих даних є ще однією з областей для подальших досліджень. Хоча цей механізм ефективно підвищує рівень захисту, він також збільшує обсяг

переданих даних. Оптимізація процесу додавання шуму може дозволити досягти кращого балансу між безпекою і ефективністю передачі, наприклад, шляхом використання адаптивного шуму, який залежить від характеристик самих даних [14].

Перспективи застосування розробленої моделі на основі AES виходять за рамки лише децентралізованих мереж. Завдяки високій стійкості до атак і здатності працювати із зашифрованими даними, модель може знайти застосування в таких сферах, як фінансові послуги, охорона здоров'я, інтернет речей (IoT) та штучний інтелект. У фінансовій сфері модель може бути використана для забезпечення безпеки транзакцій і зберігання конфіденційних даних клієнтів. В охороні здоров'я вона може застосовуватися для захисту медичних записів та обміну інформацією між різними установами.

В інтернеті речей, де пристрої часто мають обмежені обчислювальні ресурси, розроблена модель на базі стандартизованого AES може бути адаптована для захисту комунікацій між пристроями, забезпечуючи конфіденційність і цілісність даних. У сфері штучного інтелекту може використовуватися для захисту навчальних даних і результатів моделювання, особливо у випадках, коли обробка виконується на віддалених серверах або у хмарі [6].

Загалом, потенціал для подальшого розвитку створеної моделі є значним. Подальші дослідження в області оптимізації, адаптації до нових сфер і підвищення продуктивності відкривають нові горизонти для його застосування. Ця модель може стати основою для створення нових, більш ефективних рішень у галузі захисту даних і обробки інформації.

Висновки

У ході роботи вдалося досягти поставлених цілей, визначених у статті, завдяки інтеграції вдосконалень у традиційний алгоритм AES. Було розроблено модель динамічної зміни ключів, який забезпечує додатковий рівень захисту від криптографічних атак, особливо у децентралізованих мережах. Додавання контрольованого шуму до шифротексту дозволило підвищити рівень безпеки, унеможливлюючи використання закономірностей для криптоаналізу. Впровадження гомоморфної кластеризації забезпечило можливість обробки даних без їхнього розшифрування, що зберігає конфіденційність навіть у процесі активної роботи з даними. Отримані результати підтверджують ефективність запропонованих підходів, що було продемонстровано як теоретично, так і через емпіричні моделювання.

Перелік посилань

1. Hurtado Ramírez D. & Auñón J.M. (2020). Privacy Preserving K-Means Clustering: A Secure Multi-Party Computation Approach. https://arxiv.org/pdf/2009.10453
2. Li Q. & Luo L. (2023). On the Privacy of Federated Clustering: A Cryptographic View. https://arxiv.org/pdf/2312.07992
3. Aggarwal C.C. & Reddy C.K. (2013). Data Clustering: Algorithms and Applications. CRC Press.
4. Berkhin P. (2006). A Survey of Clustering Data Mining Techniques. *In Grouping Multidimensional Data* (pp. 25–71). Springer.
5. Jain A., Murty M. & Flynn P. (1999). Data Clustering: A Review. *ACM Computing Surveys*.
6. Schubert E., Sander J., Ester M., Kriegel H.P. & Xu X. (2022). DBSCAN: Why and How You Should (Still) Use DBSCAN. *ACM Transactions on Database Systems*.
7. Xu R. & Wunsch D. (2005). Survey of Clustering Algorithms. *IEEE Transactions on Neural Networks*, 16(3), 645–678.
8. Ng R.T. & Han J. (2002). CLARANS: A Method for Clustering Objects for Spatial Data Mining. *IEEE Transactions on Knowledge and Data Engineering*, 14(5), 1003–1016.
9. Сабов Д.П. & Шаркаді М.М. (2023). Підходи щодо кластеризації криптовалют. *Науковий вісник Ужгородського університету. Серія «Математика і інформатика»*, 42(1), 201–207. https://doi.org/10.24144/2616-7700.2023.42(1).201-207
10. Yang Y., Cer D. & Ahmad A. (2019). Multilingual Universal Sentence Encoder for Semantic Retrieval.
11. Аріткулова Ю.Р. (2024). Кластеризація sybil-адрес на блокчейні методами машинного навчання. https://openarchive.nure.ua/handle/document/27730
12. Hastie Trevor, Tibshirani Robert, Friedman Jerome (2019) «The EM algorithm» – New York: Springer. – С. 236–242.
13. Zobaed S.M. & Salehi M.A. (2020). Privacy-Preserving Clustering of Unstructured Big Data for Cloud-Based Enterprise Search Solutions. https://arxiv.org/pdf/2005.11317

© Левкуша О.В., Пепа Ю.В., Іванченко І.С. (2025). Модель кластеризації шифрованих даних при передачі децентралізованою мережею на основі криптографічного алгоритму AES. Сучасний захист інформації, 1(61), 8–22. https://doi.org/10.31673/2409-7292.2025.014570

14. Kaufman L. & Rousseeuw P.J. (2009). Finding Groups in Data: An Introduction to Cluster Analysis. Wiley.

15. Yinfei Yang, Daniel Cer, Amin Ahmad (2019). «Multilingual Universal Sentence Encoder for Semantic Retrieval».

16. Ester M., Kriegel H.P., Sander J. & Xu X. (1996). A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. In *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining* (pp. 226–231).

17. Пількевич І.А., Бойченко О.С. & Гуменюк І.В. (2019). Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж. *Технічна інженерія*, 2(84), 100–108. https://journals.uran.ua/index.php/2706-5847/article/view/186576

18. Estivill-Castro V. (2002). Why So Many Clustering Algorithms: A Position Paper. *ACM SIGKDD Explorations Newsletter*, 4(1), 65–75.

19. Guha S., Rastogi R. & Shim K. (1998). CURE: An Efficient Clustering Algorithm for Large Databases. In *Proceedings of the 1998 ACM SIGMOD International Conference on Management of Data* (pp. 73–84).

20. Mirkes E.M. (2021). «K-means and K-medoids applet».

Надійшла 12.01.2025