https://doi.org/10.31891/2219-9365-2026-85-27
УДК 004.056.55:004.652.2:004.738.5

РОЗЛОМІЙ Інна
Черкаський державний технологічний університет
https://orcid.org/0000-0001-5065-9004
inna-roz@ukr.net
НАУМЕНКО Сергій
Черкаський національний університет імені Богдана Хмельницького
https://orcid.org/0000-0002-6337-1605
naumenko.serhii1122@vu.cdu.edu.ua
КОВТЮХ Віталій
Черкаський державний технологічний університет
https://orcid.org/0009-0009-5301-7045
granvitalik@gmail.com

МОДЕЛЬ ЗАХИЩЕНОГО ЗБЕРІГАННЯ ДАНИХ У РОЗПОДІЛЕНИХ БАЗАХ ДАНИХ НА ОСНОВІ АТРИБУТНОГО ШИФРУВАННЯ ДЛЯ КРИТИЧНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

У статті запропоновано модель захищеного зберігання даних у розподілених базах даних на основі атрибутивного шифрування, орієнтовану на потреби критичних інформаційно-комунікаційних систем. Розроблена архітектура передбачає фрагментацію даних, гібридне шифрування з використанням CP-ABE для ключів доступу та симетричних алгоритмів для повідомлень, а також інтеграцію політик доступу у СУБД. Проведене моделювання демонструє ефективність підходу за показниками часу розшифрування, стійкості до атак та рівномірного розподілу навантаження між вузлами. Особливу увагу приділено практичним аспектам реалізації – зокрема, використанню PostgreSQL з політиками RLS, формалізації політик доступу у вигляді логічних виразів та перевірці цілісності фрагментів. Запропонована модель забезпечує децентралізоване керування доступом, зменшує ризики витоку даних та адаптується до змінних контекстів. У перспективі планується підтримка атрибутів із динамічними значеннями, відкликання доступу та інтеграція з блокчейн-реєстрами для фіксації дій.

Ключові слова: атрибутивне шифрування, розподілені бази даних, контроль доступу, фрагментація даних, CP-ABE, інформаційно-комунікаційні системи.

ROZLOMII Inna
Cherkasy State Technological University
NAUMENKO Serhii
Bohdan Khmelnytskyi National University of Cherkasy
KOVTIUKH Vitalii
Cherkasy State Technological University

MODEL OF PROTECTED DATA STORAGE IN DISTRIBUTED DATABASES BASED ON ATTRIBUTE ENCRYPTION FOR CRITICAL INFORMATION AND COMMUNICATION SYSTEMS

This paper presents a secure data storage model for distributed databases based on attribute-based encryption (ABE), specifically tailored for critical information and communication systems (ICS). The proposed architecture incorporates data fragmentation, hybrid encryption using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for access keys and symmetric algorithms for message encryption, along with the integration of access control policies within the database management system (DBMS). The model introduces a decentralized access mechanism where access rules are embedded into the ciphertext and verified solely on the client side, eliminating the need for full trust in nodes or centralized authorization servers.

An experimental evaluation in a virtual distributed environment demonstrates the model's effectiveness in terms of decryption time, ciphertext size, resistance to unauthorized access, and balanced node load. The use of PostgreSQL with Row-Level Security (RLS) policies and the formalization of access control through logical expressions in policy tables ensures end-to-end data protection. Notably, the hybrid scheme reduces computational load by encrypting only the keys, making the model suitable for real-time systems and resource-constrained environments.

The novelty lies in the combination of CP-ABE mechanisms with data fragmentation, dynamic fragment placement, and embedded policy verification within the DBMS. Future research directions include support for dynamically changing attributes (such as situational roles or context), attribute revocation, optimization of fragment distribution based on network topology and load balancing, and blockchain integration to ensure tamper-proof access logging. This work advances secure, scalable, and adaptable data protection in distributed critical infrastructures.

Keywords: attribute encryption, distributed databases, access control, data fragmentation, CP-ABE, information and communication systems.

Стаття надійшла до редакції / Received 03.01.2026
Прийнята до друку / Accepted 04.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Одна з ключових проблем сучасних критичних інформаційно-комунікаційних систем – необхідність забезпечення захищеного зберігання даних у середовищах з підвищеними вимогами до конфіденційності, доступності та цілісності інформації [1]. Розподілені бази даних активно використовуються в таких системах для підвищення відмовостійкості, масштабованості та продуктивності, але водночас створюють нові виклики у сфері інформаційної безпеки [2]. В умовах розподіленого середовища дані зберігаються на кількох вузлах, що підвищує ризики несанкціонованого доступу, модифікації або компрометації даних на окремих вузлах або під час передачі між ними.

Традиційні методи шифрування часто не забезпечують достатньої гнучкості щодо управління правами доступу, що є критичним для систем з динамічно змінними ролями користувачів та складною політикою безпеки [3]. Особливо це актуально для галузей, де рішення щодо доступу повинні прийматися на основі множини атрибутів, таких як роль, місце розташування, рівень секретності чи контекст дії. У таких випадках атрибутивне шифрування дає потенціал для побудови системи, в якій доступ до зашифрованих даних визначається не ідентифікатором користувача, а набором атрибутів, що узгоджується з політикою безпеки.

Наукова та практична актуальність проблеми полягає в тому, що незважаючи на наявність окремих рішень для шифрування та розподіленого зберігання, відсутня цілісна модель, яка б дозволяла реалізувати керований, адаптивний доступ до чутливої інформації у розподілених середовищах саме з використанням атрибутивного шифрування. Крім того, існуючі рішення часто не враховують обмеження, притаманні критичним ІК-системам, як-от вимоги до низької затримки, підвищеної надійності, обмеженого часу відповіді та можливості інтеграції з уже розгорнутими інфраструктурами.

Метою дослідження є розробка моделі захищеного зберігання даних у розподілених базах даних на основі атрибутивного шифрування з урахуванням специфіки критичних інформаційно-комунікаційних систем.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Атрибутивне шифрування (Attribute-Based Encryption, ABE) вже тривалий час розглядається як перспективний механізм для забезпечення гнучкого та контекстно-залежного контролю доступу до даних [4]. Починаючи з базових моделей Key-Policy ABE (KP-ABE) та Ciphertext-Policy ABE (CP-ABE), наукова спільнота досліджує шляхи покращення ефективності, стійкості до атак, масштабованості та практичного впровадження таких схем у системах з високими вимогами до безпеки [5]. Зокрема, у роботах [6, 7] було вперше запропоновано концепцію CP-ABE, яка дозволяє визначати політику доступу безпосередньо у шифротексті, що є критично важливим для систем зі складною ієрархією ролей і обмеженнями.

Подальші дослідження зосереджувалися на оптимізації ABE-схем для обмежених обчислювальних середовищ, таких як IoT, мобільні платформи або розподілені системи з динамічним складом вузлів. Запропоновано гібридні підходи, в яких атрибутивне шифрування поєднується з симетричними алгоритмами, аби зменшити обчислювальне навантаження. У деяких роботах також розглядається питання відкликання атрибутів, делегування повноважень, а також шифрування з підтримкою атрибутів часу або місцезнаходження [8]. Поряд із цим, з'явилися численні реалізації бібліотек ABE на основі Pairing-Based Cryptography, зокрема у проєктах CP-ABE Toolkit, Charm та інших, які дозволяють оцінювати продуктивність різних реалізацій на практиці [9].

Проблематика захищеного зберігання даних у розподілених базах даних досліджується в контексті безпечного хмарного зберігання, Big Data платформ, блокчейн-інфраструктур, а також критичних ІК-систем, де необхідно забезпечити доступ за умов часткової довіри до вузлів. У публікаціях розглядаються як централізовані, так і децентралізовані підходи, що використовують шифрування на стороні клієнта, розділення даних на фрагменти, контроль доступу через проксі-сервери або шлюзи, та реалізацію атестації вузлів [10]. Значна увага приділяється стійкості до атак типу «man-in-the-middle», атак через зловмисні вузли, а також питанню довіри до сховища.

Водночас більшість існуючих моделей або обмежуються централізованою архітектурою, або не враховують повною мірою гнучкі політики доступу на основі атрибутів. Недостатньо розробленими залишаються також питання інтеграції атрибутивного шифрування у структури розподілених баз даних, де присутні вимоги до реплікації, узгодженості даних, захисту метаданих та збереження продуктивності в умовах підвищеного навантаження.

Таким чином, попри значну кількість теоретичних досліджень і прототипів, залишається відкритим питання створення цілісної моделі захищеного зберігання даних у розподілених базах даних, яка б інтегрувала переваги атрибутивного шифрування, відповідала специфіці критичних ІК-систем та враховувала практичні вимоги до надійності, масштабованості і гнучкого управління доступом.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У критичних інформаційно-комунікаційних системах розподілені бази даних використовуються для забезпечення високої доступності, надійності та відмовостійкості. Типова архітектура такої системи включає декілька вузлів зберігання, об'єднаних у мережу, де дані реплікуються та розподіляються відповідно до заданої політики. Кожен вузол виконує роль часткового сховища, що забезпечує обробку запитів, верифікацію доступу та обмін зашифрованими фрагментами. Дані на вузлах зберігаються у зашифрованому вигляді з використанням атрибутивного шифрування, яке дозволяє застосовувати гнучкі політики доступу на основі множини атрибутів, а не конкретних ідентифікаторів користувачів.

У системі визначаються кілька типових ролей користувачів: адміністратор безпеки, системний користувач, зовнішній аудитор, оператор моніторингу, службовець з обмеженим доступом. Кожна роль описується набором атрибутів, які можуть включати рівень доступу (наприклад, «секретно», «конфіденційно»), географічне розташування, приналежність до підрозділу, контекст використання (перегляд, редагування, експортування), час активності та інші. Ці атрибути стають основою для визначення політик доступу до шифрованих даних.

На рис. 1 зображено архітектуру захищеного середовища із застосуванням атрибутивного шифрування, в якій джерело даних, шифрувальний модуль, модуль управління політиками доступу, вузли розподіленого зберігання та модулі автентифікації формують інтегровану систему захищеного зберігання.

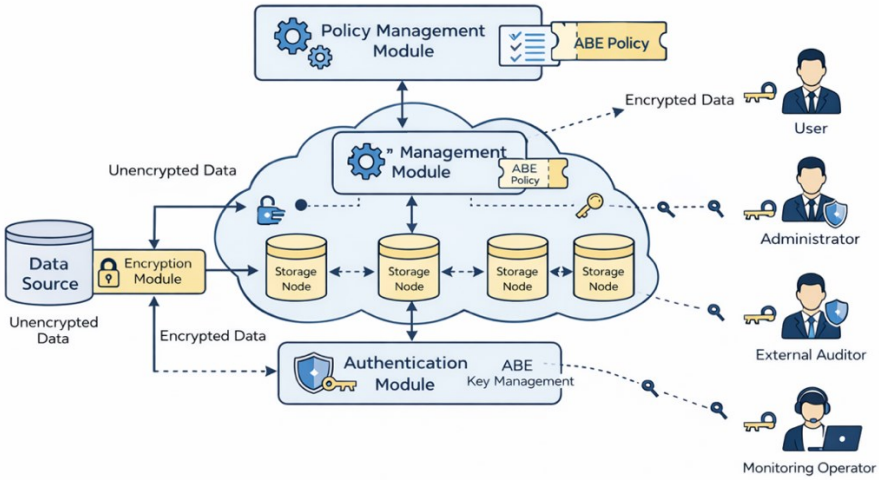

Рис. 1. Архітектура розподіленої системи захищеного зберігання даних на основі атрибутивного шифрування

Як засіб реалізації контролю доступу у даній роботі розглядається Ciphertext-Policy Attribute-Based Encryption (CP-ABE), що надає можливість формулювати політику доступу безпосередньо у шифротексті. Це дозволяє гнучко задавати правила доступу на основі логічного поєднання атрибутів, якими володіє користувач. Наприклад, політика може мати вигляд: («роль = аналітик» AND «рівень доступу = секретно») OR («підрозділ = моніторинг» AND «локація = штаб»), що задається у формі дерева доступу з логічними вузлами AND/OR.

Математична модель CP-ABE визначається множиною атрибутів $A = \{a_1, a_2, \dots, a_n\}$, політикою доступу $P(A)$, функцією шифрування $E(m, P)$, яка створює шифротекст C, та функцією розшифрування $D(C, K)$, де K – приватний ключ користувача з відповідними атрибутами. Функція $D(C, K)$ успішно розшифрує повідомлення m лише тоді, коли атрибути користувача задовольняють політику P.

Оцінка складності системи включає наступні формули:

1. Складність шифрування – $T_{enc} = O(k \times |P|)$ де k – розмір групи, $|P|$ – кількість вузлів у дереві політики.
2. Складність розшифрування – $T_{dec} = O(k \times d)$ де d – глибина дерева політики, що відповідає успішному набору атрибутів.
3. Обсяг шифротексту – $|C| = O(k \times |P| + |m|)$, де $|m|$ – розмір повідомлення.

Для критичних систем особливо важливо забезпечити баланс між гнучкістю управління доступом, ефективністю обробки запитів і мінімізацією затримок при шифруванні та розшифруванні. Саме тому CP-ABE розглядається як базовий механізм, що дозволяє точно визначати правила доступу у шифротексті та забезпечує масштабованість у розподілених середовищах. Водночас складність шифрування і розшифрування, яка зростає із кількістю атрибутів і глибиною політики доступу, вимагає адаптації при реалізації у практичних системах. Одним із рішень виступає використання гібридних схем, де безпосереднє повідомлення шифрується швидким симетричним алгоритмом, а атрибутивне шифрування застосовується лише для ключів доступу. Такий підхід дозволяє зберігати переваги CP-ABE в частині контролю доступу та водночас знижувати навантаження на систему при роботі з великими обсягами даних у розподілених базах.

У запропонованій моделі захищеного зберігання даних у розподіленій базі використовується принцип фрагментованого розміщення зашифрованих даних. Кожне повідомлення перед записом у базу ділиться на кілька фрагментів, які незалежно шифруються відповідно до заданої політики доступу за допомогою CP-ABE. Після шифрування фрагменти розподіляються між кількома вузлами зберігання згідно з політикою реплікації, що враховує навантаження на вузли, їхню доступність та довірений статус.

Кожен зашифрований фрагмент супроводжується метаданими, які містять хеш-контрольну суму, сигнатуру відправника, мітку часу та ідентифікатор політики доступу. Хеші використовуються для перевірки цілісності при зчитуванні, а сигнатури дозволяють підтвердити справжність джерела даних. Мітки часу забезпечують механізм контролю актуальності, що особливо важливо у сценаріях з часовими обмеженнями доступу.

Алгоритм збереження та шифрування складається з таких основних етапів: користувач передає дані до модуля шифрування, де вони діляться на фрагменти; до кожного фрагмента застосовується шифрування згідно з політикою CP-ABE; створюються метадані та формується структура збереження; зашифровані фрагменти розміщуються на вузлах зберігання; до глобального каталогу записується інформація про місцезнаходження фрагментів і політику доступу. Під час запиту на отримання даних користувач проходить автентифікацію, отримує ключ на основі своїх атрибутів, і якщо вони відповідають політиці, фрагменти розшифровуються, перевіряється цілісність, і дані відновлюються.

На рис. 2 представлено схему, що відображає повну послідовність операцій збереження та отримання даних у розподіленій системі з атрибутивним шифруванням.

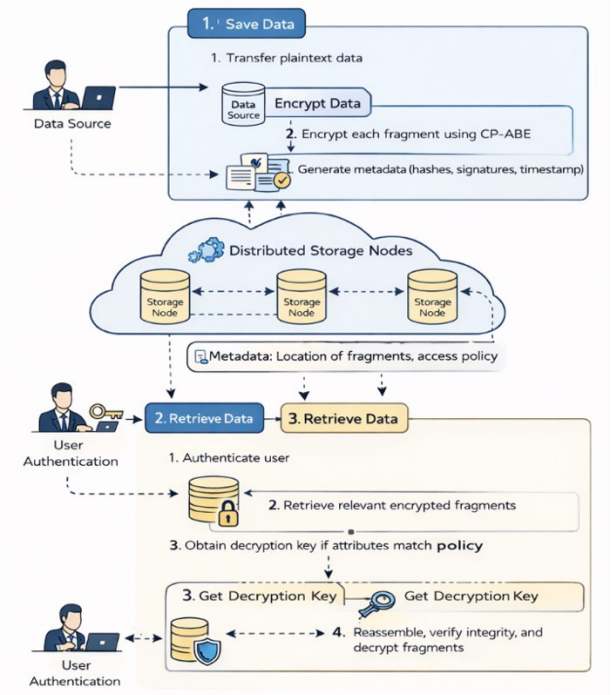

Рис. 2. Послідовність операцій збереження та отримання даних у моделі з атрибутивним шифруванням

Інтеграція атрибутивного шифрування в систему управління базами даних передбачає використання атрибутів користувача як частини механізму авторизації при виконанні SQL-запитів. У СУБД, таких як PostgreSQL або MongoDB, це можливо шляхом розширення механізму ролей, коли кожному користувачу призначається не лише роль, а й набір атрибутів, що зберігаються в окремій таблиці політик або у вигляді JSON-документів.

Прикладом є додавання до таблиці користувачів атрибутів, таких як «department», «clearance_level», «location», а також запис відповідних політик доступу у вигляді логічних виразів. При спробі доступу до захищених даних перевіряється відповідність атрибутів користувача політиці, що була застосована під час шифрування. У PostgreSQL така перевірка може реалізовуватись за допомогою тригерів, представлень (views) або політик на основі RLS (Row-Level Security). У MongoDB – через middleware-шари, що перевіряють відповідність політик у запитах до колекцій.

У таблиці 1 наведено приклади зіставлення поширених атрибутів з відповідними політиками доступу в СУБД.

Цей підхід дозволяє реалізувати єдину логіку політик як у шифруванні, так і при зверненні до бази даних, що забезпечує наскрізний контроль доступу до інформації незалежно від фізичного розташування фрагментів.

Для оцінки ефективності запропонованої моделі було проведено експериментальну перевірку у віртуальному тестовому середовищі, що імітує розподілену систему з п'ятьма вузлами зберігання, окремим сервером аутентифікації та клієнтами з різними наборами атрибутів. У якості програмної реалізації використано модуль CP-ABE, розроблений на основі бібліотеки Charm Crypto, а також модуль симетричного шифрування AES-256 для гібридної реалізації. База даних реалізована на платформі PostgreSQL з увімкненою політикою RLS.

Таблиця 1

Зіставлення атрибутів з політиками доступу в СУБД

Атрибут користувача	Приклад значення	Умова доступу у політиці	Приклад реалізації в СУБД
department	analytics	department = 'analytics'	WHERE department = 'analytics'
clearance_level	high	clearance_level = 'high'	USING clearance_level = 'high'
location	Kyiv	location = 'Kyiv'	JSON->>'location' = 'Kyiv'
access_time_range	08:00–18:00	time BETWEEN 08:00 AND 18:00	FUNCTION check_access_time()

Серед ключових параметрів експерименту – розмір повідомлення (від 1 до 50 КБ), кількість атрибутів у політиці доступу (від 2 до 15), кількість атрибутів у користувача (від 2 до 10), глибина дерева доступу, а також кількість одночасних запитів. Вимірювалися середній час розшифрування, затримка доступу, розмір шифротексту, навантаження на вузли та стійкість до спроб несанкціонованого доступу.

Результати засвідчили, що середній час розшифрування зростає майже лінійно із кількістю атрибутів у політиці, проте залишається у межах прийнятного для систем реального часу. Так, при політиці з 5 атрибутів середній час розшифрування становив 57 мс, а при 10 – 111 мс. У гібридному варіанті час обробки зменшувався в середньому на 43% за рахунок того, що дешифрувався лише ключ, а не весь фрагмент. Обсяг шифротексту збільшувався пропорційно до кількості атрибутів, але завдяки фрагментації навантаження рівномірно розподілялося між вузлами. Система успішно блокувала доступ користувачів із неповним набором атрибутів, що підтверджує її стійкість до атак на основі підміни ідентичності або запиту.

На рис. 3 показано залежність часу розшифрування від кількості атрибутів у політиці доступу. Графік демонструє, що зі збільшенням кількості атрибутів час розшифрування зростає майже лінійно. Гібридна схема забезпечує значно нижчий час розшифрування, що особливо помітно при складніших політиках.

Запропонована модель відрізняється від традиційних централізованих систем або систем з жорсткою авторизацією тим, що не вимагає повної довіри до окремих вузлів або центрального контролера. Політика доступу вбудовується у сам шифротекст і перевіряється лише на стороні користувача, що забезпечує децентралізований контроль доступу. На відміну від систем, які покладаються на статичні ролі чи ACL-таблиці, атрибутивне шифрування дозволяє створювати політики, гнучко адаптовані до контексту, середовища, часу або функціональної ролі.

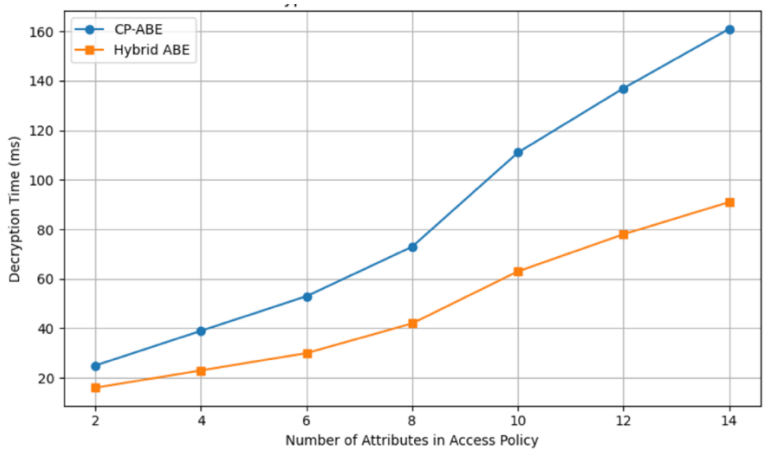

Рис. 3. Залежність часу розшифрування від кількості атрибутів у політиці доступу

Наукова новизна моделі полягає у поєднанні механізмів CP-ABE із фрагментацією даних, динамічним розміщенням фрагментів та вбудованою перевіркою політик у середовищі СУБД. Завдяки цьому досягається наскрізна інтеграція захисту як на рівні шифрування, так і на рівні бази даних. Практична значущість моделі полягає у можливості її застосування у критичних інформаційно-комунікаційних системах, де потрібен не лише захист даних, а й обмеження доступу з урахуванням багатьох динамічних параметрів. Це дозволяє зменшити ризики витоку даних, покращити контроль за їх використанням, забезпечити стійкість до компрометації окремих вузлів і адаптувати систему до нових загроз без повного перешифрування всієї інформації.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті представлено модель захищеного зберігання даних у розподілених базах даних на основі атрибутивного шифрування, орієнтовану на використання у критичних інформаційно-комунікаційних системах. Запропонований підхід поєднує механізми CP-ABE з фрагментацією даних, динамічним розподілом фрагментів між вузлами та інтеграцією контролю політик доступу на рівні СУБД. Це дозволяє забезпечити гнучке, масштабоване та децентралізоване керування доступом без необхідності повної довіри до окремих вузлів або централізованих авторизаційних служб.

Проведене експериментальне моделювання підтвердило ефективність запропонованої моделі з погляду часу розшифрування, обсягу шифрованих даних та стійкості до несанкціонованого доступу. Зокрема, гібридна реалізація на основі симетричного шифрування ключа показала значне зниження обчислювального навантаження, що є критично важливим для систем реального часу та середовищ із обмеженими ресурсами.

До перспектив подальших досліджень належить розширення моделі з урахуванням багаторівневого доступу, атрибутів, що змінюються динамічно (наприклад, контексту використання або ситуаційної ролі), та впровадження механізмів відкликання атрибутів. Окрему увагу планується приділити оптимізації розподілу фрагментів з урахуванням навантаження на мережу та топології розміщення вузлів. Також перспективним напрямом є дослідження можливостей інтеграції з блокчейн-платформами для забезпечення незаперечності операцій доступу.

Література

1. Farid, G., Warraich, N. F., & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 51(4), 1000–1014. https://doi.org/10.1177/01655515231174370
2. Rozlomii, I. O., & Naumenko, S. V. (2025). Архітектура та функціональні особливості захищених систем керування базами даних нового покоління з підтримкою serverless та edge-обчислень. *Systems and Technologies*, 69(1), 130–137.
3. Rozlomii, I., Koseniuk, G., & Naumenko, S. (2025). Механізми криптографічного контролю автентичності коду у сенсорних вузлах з обмеженими обчислювальними ресурсами. *Computer-integrated technologies: education, science, production*, (61), 193–198. https://doi.org/10.36910/6775-2524-0560-2025-61-24
4. Hohenberger, S., Lu, G., Waters, B., & Wu, D. J. (2023). Registered attribute-based encryption. In *EUROCRYPT 2023* (pp. 511–542). Springer. https://doi.org/10.1007/978-3-031-30620-4_18
5. Delerablée, C., Gouriou, L., & Pointcheval, D. (2022). Key-policy ABE with switchable attributes. In *Security and Cryptography for Networks* (pp. 147–171). Springer. https://doi.org/10.1007/978-3-031-14791-3_8
6. Das, S., & Namasudra, S. (2022). Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. *IEEE Transactions on Industrial Informatics*, 19(1), 821–829. https://doi.org/10.1109/TII.2022.3159046
7. Wee, H. (2022). Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In *EUROCRYPT 2022* (pp. 217–241). Springer. https://doi.org/10.1007/978-3-031-06944-4_8
8. Shruti, Rani, S., Sah, D. K., & Gianini, G. (2023). Attribute-based encryption schemes for next generation wireless IoT networks: a comprehensive survey. *Sensors*, 23(13), 5921. https://doi.org/10.3390/s23135921
9. Bhaskar, S., Parmar, K., & Jinwala, D. C. (2025). Comparative evaluation of pairing-free and pairing-based CP-ABE schemes for resource constrained environments. *Cluster Computing*, 28(7), 431. https://doi.org/10.1007/s10586-025-05319-8
10. Ha, G., Jia, C., Chen, Y., Chen, H., & Li, M. (2023). A secure client-side deduplication scheme based on updatable server-aided encryption. *IEEE Transactions on Cloud Computing*, 11(4), 3672–3684. https://doi.org/10.1109/TCC.2022.3192225

References

1. Farid, G., Warraich, N. F., & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 51(4), 1000–1014. https://doi.org/10.1177/01655515231174370
2. Rozlomii, I. O., & Naumenko, S. V. (2025). Architecture and functional features of next-generation secure database management systems with support for serverless and edge computing. *Systems and Technologies*, *69*(1), 130-137.
3. Rozlomii, I., Koseniuk, G., & Naumenko, S. (2025). Механізми криптографічного контролю автентичності коду у сенсорних вузлах з обмеженими обчислювальними ресурсами. *Computer-integrated technologies: education, science, production*, (61), 193–198. https://doi.org/10.36910/6775-2524-0560-2025-61-24
4. Hohenberger, S., Lu, G., Waters, B., & Wu, D. J. (2023). Registered attribute-based encryption. In *EUROCRYPT 2023* (pp. 511–542). Springer. https://doi.org/10.1007/978-3-031-30620-4_18
5. Delerablée, C., Gouriou, L., & Pointcheval, D. (2022). Key-policy ABE with switchable attributes. In *Security and Cryptography for Networks* (pp. 147–171). Springer. https://doi.org/10.1007/978-3-031-14791-3_8
6. Das, S., & Namasudra, S. (2022). Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure. *IEEE Transactions on Industrial Informatics*, 19(1), 821–829. https://doi.org/10.1109/TII.2022.3159046
7. Wee, H. (2022). Optimal broadcast encryption and CP-ABE from evasive lattice assumptions. In *EUROCRYPT 2022* (pp. 217–241). Springer. https://doi.org/10.1007/978-3-031-06944-4_8
8. Shruti, Rani, S., Sah, D. K., & Gianini, G. (2023). Attribute-based encryption schemes for next generation wireless IoT networks: a comprehensive survey. *Sensors*, 23(13), 5921. https://doi.org/10.3390/s23135921
9. Bhaskar, S., Parmar, K., & Jinwala, D. C. (2025). Comparative evaluation of pairing-free and pairing-based CP-ABE schemes for resource constrained environments. *Cluster Computing*, 28(7), 431. https://doi.org/10.1007/s10586-025-05319-8
10. Ha, G., Jia, C., Chen, Y., Chen, H., & Li, M. (2023). A secure client-side deduplication scheme based on updatable server-aided encryption. *IEEE Transactions on Cloud Computing*, 11(4), 3672–3684. https://doi.org/10.1109/TCC.2022.3192225