DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-31
УДК 004.056.55:004.738.5
Розломій Інна Олександрівна[1], к.т.н., доцент
https://orcid.org/0000-0001-5065-9004
Науменко Сергій Васильович[2], аспірант
https://orcid.org/0000-0002-6337-1605
Ковтюх Віталій Анатолійович[1], аспірант
https://orcid.org/0009-0009-5301-7045
[1]Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна
[2]Черкаський державний технологічний університет, м. Черкаси, Україна

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛІЙ У ДОСТУПІ ДО ДАНИХ У ХМАРНИХ СУБД НА ОСНОВІ ПОВЕДІНКОВОЇ АНАЛІТИКИ

Розломій І.О., Науменко С.В., Ковтюх В.А. Система виявлення аномалій у доступі до даних у хмарних СУБД на основі поведінкової аналітики. У статті розглянуто проблему забезпечення безпеки доступу до даних у хмарних системах управління базами даних в умовах динамічної поведінки користувачів та зростання складності сучасних інформаційних систем. Обгрунтовано доцільність використання поведінкової аналітики як основи для виявлення неочевидних загроз, зокрема внутрішніх зловживань і компрометації облікових записів, які не можуть бути ефективно ідентифіковані традиційними механізмами контролю доступу. Запропоновано архітектуру системи виявлення аномалій, що включає модулі збору подій доступу, профілювання поведінки користувачів, аналізу відхилень та реагування на виявлені загрози. Сформовано модель поведінки користувача на основі агрегованих ознак доступу до хмарної СУБД, зокрема часових характеристик, частоти та типів SQL-запитів, мережевих і геолокаційних параметрів. Для виявлення аномалій застосовано нейронний автоенкодер, який дозволяє визначати відхилення від нормального простору поведінки за величиною помилки реконструкції. Наведено математичне представлення моделі та обгрунтовано вибір порогового значення для класифікації поведінкових сесій. Проведено експериментальну перевірку ефективності запропонованого підходу та порівняльний аналіз із класичними методами, що підтвердило його переваги за показниками точності, повноти та адаптивності. Показано практичну придатність системи для використання у хмарних і мультиорендних середовищах, а також окреслено перспективи подальших досліджень, пов'язані з потоковим навчанням, масштабуванням і інтеграцією з системами управління інцидентами інформаційної безпеки.
Ключові слова: аномалії доступу, хмарні СУБД, поведінкова аналітика, автоенкодер, інформаційна безпека, профіль користувача.

Rozlomii I., Naumenko S., Kovtiukh V. A system for detecting anomalies in data access in cloud DBMSs based on behavioral analytics. This paper presents a user behavior-based anomaly detection system designed for cloud database management systems (DBMS). The proposed solution addresses the growing need for proactive security mechanisms in cloud environments, where traditional access control models often fail to detect context-dependent or insider threats. The system architecture comprises four key modules: access event collection, user behavior profiling, anomaly detection, and automated response. A behavioral profile is generated for each user by aggregating multiple features such as access time, query frequency, operation types, IP addresses, and SQL query structure. The core of the anomaly detection model is an autoencoder – a neural network capable of reconstructing input vectors with high accuracy for normal behavior and exhibiting elevated reconstruction error in anomalous sessions. The anomaly score is computed using mean squared error, and a threshold is empirically defined to classify behaviors as normal or anomalous. Comparative analysis demonstrates that the autoencoder-based model outperforms classical methods such as statistical thresholding, k-means clustering, and One-Class SVM in terms of accuracy, recall, and adaptability. The proposed approach also shows lower false-positive rates and better suitability for high-dimensional behavior vectors, typical of cloud access logs. The system was implemented using Python and PostgreSQL on the AWS platform. Integration with DBMS logs was achieved using built-in audit extensions, while real-time behavior analysis was supported through the automatic profiling and classification modules. A test dataset confirmed the model's capability to detect unusual behavior such as abnormal access times, query bursts, or login from unexpected geolocations. The practical applicability of this system lies in its suitability for dynamic and multi-tenant cloud architectures. It enables security teams to continuously monitor user behavior and react to emerging threats without manual reconfiguration of access rules. Future work will focus on the inclusion of session-level activity parameters, streaming data learning methods, and seamless integration with incident management systems.
Key words: access anomalies, cloud DBMS, behavioral analytics, autoencoder, information security, user profile.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. У сучасних умовах стрімкого зростання обсягів даних та поширення хмарних технологій зберігання й обробки інформації, забезпечення безпеки доступу до даних у хмарних системах управління базами даних (СУБД) набуває особливої актуальності [1]. Класичні підходи до контролю доступу, зокрема рольовий або політико-орієнтований контроль, мають низку обмежень. Вони неспроможні виявляти неочевидні, контекстуально-зумовлені загрози, які виникають унаслідок компрометації користувацьких облікових записів або внутрішніх зловживань [2].

© Розломій І.О., Науменко С.В., Ковтюх В.А.

Особливої складності набуває ситуація в хмарних середовищах, де множинність користувачів, гнучка модель доступу, динамічні зміни у поведінці системи й користувачів створюють додаткові виклики для систем захисту. Зокрема, типові атаки можуть не порушувати явні політики доступу, але все ж бути шкідливими, якщо враховувати атиповість дій у конкретному контексті. Виявлення подібних загроз потребує переходу від традиційних моделей до поведінкової аналітики, що дозволяє фіксувати відхилення у шаблонах використання системи, які потенційно свідчать про несанкціонований або зловмисний доступ.

Поведінкова аналітика ґрунтується на дослідженні активності користувачів, побудові моделей «нормальної» поведінки та виявленні аномалій шляхом зіставлення поточних дій із очікуваними [3]. У цьому контексті виникає потреба в розробці ефективної системи виявлення аномалій, яка б у режимі реального часу аналізувала поведінку суб'єктів доступу до хмарної СУБД, своєчасно виявляла потенційні загрози та реагувала на них.

Особливого значення набуває забезпечення високої точності виявлення аномалій при мінімальній кількості хибнопозитивних спрацювань, що вимагає створення моделей, адаптованих до особливостей хмарних архітектур, змінної природи навантаження та гетерогенності даних. Наукове завдання також полягає в обґрунтуванні вибору метрик, підходів до попередньої обробки даних, формування профілів поведінки користувачів та механізмів машинного навчання для ідентифікації аномалій у доступі до даних.

Практичне значення дослідження визначається потребами організацій у проактивному моніторингу безпеки доступу до інформаційних активів у хмарних середовищах, де традиційні засоби журналювання та контролю вже не забезпечують належного рівня захищеності.

Метою дослідження є розробка системи виявлення аномалій у доступі до даних у хмарних СУБД на основі поведінкової аналітики користувачів.

Аналіз останніх досліджень та публікацій. Упродовж останнього десятиліття спостерігається активне зростання інтересу до виявлення аномальної активності в інформаційних системах, зокрема в контексті хмарних обчислень та систем управління базами даних [4]. Значна кількість досліджень присвячена використанню методів машинного навчання для виявлення нестандартних шаблонів поведінки користувачів. Такі шаблони можуть свідчити про зловмисну активність, втрату контролю над обліковими записами або порушення внутрішньої політики безпеки.

Серед основних напрямів, які розробляються науковцями, можна виокремити моделі на основі класифікації дій користувачів. Зокрема застосовуються алгоритми Support Vector Machines, Random Forest та K-Nearest Neighbors [5-7]. Окремий напрям становлять методи глибокого навчання, включаючи рекурентні нейронні мережі та автоенкодери [8]. У працях багатьох авторів запропоновано застосування безнаглядних методів кластеризації для виявлення відхилень у поведінці користувачів, які не потрапляють у межі заздалегідь визначених класів, що особливо актуально для виявлення нових типів атак [9].

Поряд з цим зростає кількість досліджень, орієнтованих на адаптацію поведінкової аналітики до специфіки хмарних СУБД [10]. У таких роботах враховуються фактори розподіленості даних, багатокористувацького доступу, еластичності інфраструктури та складності побудови профілів поведінки в умовах змінного навантаження. Зокрема, аналізуються часові характеристики запитів до бази даних, геолокаційні ознаки, послідовності виконаних транзакцій, параметри підключення та інші сигнатурні маркери [11].

Разом із тим, незважаючи на помітні здобутки, дослідження демонструють, що для досягнення високої точності та оперативності виявлення аномалій у доступі до даних у хмарному середовищі досі необхідна подальша оптимізація підходів. Складність полягає в досягненні балансу між точністю виявлення та обчислювальними витратами, мінімізацією хибнопозитивних результатів та забезпеченням масштабованості в умовах великої кількості користувачів і запитів.

Більшість існуючих рішень залишаються або надто загальними, або вузько спеціалізованими й не враховують у повній мірі динаміку поведінки користувачів саме в хмарних СУБД. Також часто не приділяється достатньої уваги адаптивності моделей до змін у поведінкових патернах, що виникають унаслідок змін ролей, задач або зовнішніх умов функціонування системи.

Таким чином, актуальним науковим завданням є створення універсальної, адаптивної системи виявлення аномалій у поведінці користувачів хмарних СУБД, здатної працювати в умовах високого навантаження, мінімальних обчислювальних ресурсів та змінного середовища доступу.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.

© Розломій І.О., Науменко С.В., Ковтюх В.А.

Запропонована система виявлення аномалій у доступі до даних у хмарних СУБД базується на принципах поведінкової аналітики та має модульну архітектуру, що дозволяє забезпечити гнучкість, масштабованість і ефективність обробки великого обсягу подій. Основу архітектури складають чотири ключові компоненти: модуль збору подій доступу, модуль профілювання поведінки користувачів, модуль виявлення аномалій та модуль реагування.

Модуль збору подій доступу відповідає за фіксацію активності користувачів у хмарній СУБД. До подій, що аналізуються, належать SQL-запити, підключення до системи, спроби читання, запису, зміни або видалення даних. Дані збираються у вигляді логів або телеметрії за допомогою вбудованих засобів моніторингу бази даних або через проксі-сервери доступу.

Модуль профілювання поведінки користувачів формує унікальні поведенкові профілі на основі історичних даних активності. Цей компонент агрегує події, визначає статистичні характеристики поведінки користувачів і генерує вектори поведінки, які використовуються як еталонні шаблони для подальшого порівняння.

Модуль виявлення аномалій виконує аналіз поточних дій користувачів та їхнє порівняння з попередньо побудованими профілями. У разі виявлення значних відхилень поведінки, які можуть свідчити про потенційне порушення безпеки, генерується сигнал про аномалію.

Модуль реагування відповідає за подальші дії у разі виявлення аномалій. Це може бути сповіщення адміністратора, автоматичне припинення сесії користувача або ініціація додаткової автентифікації.

Взаємозв'язок між модулями системи представлено на рис. 1.

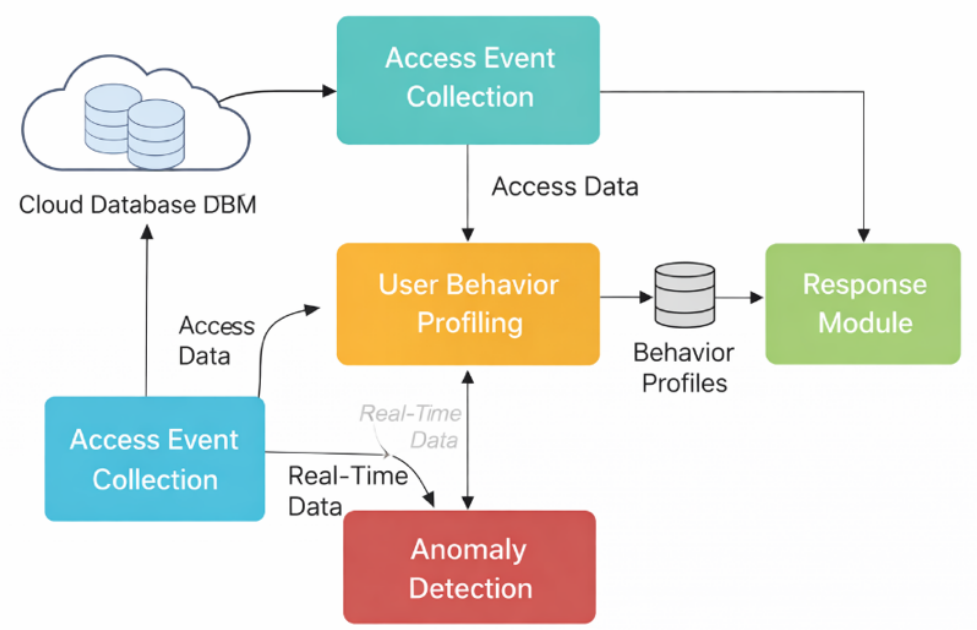

Рис. 1. Архітектура системи виявлення аномалій у хмарній СУБД

На рисунку зображено, як події з хмарної СУБД надходять до модуля збору, проходять обробку та аналіз, формують поведінкові профілі, порівнюються з новими подіями і в разі виявлення аномалії ініціюють реакцію.

Профіль поведінки користувача формується на основі ряду ключових ознак, що є найбільш інформативними для виявлення аномальної активності. До них належать час доступу до СУБД (з урахуванням робочого графіку та вихідних), частота запитів за певний період, тип виконуваних SQL-операцій (читання, запис, оновлення, видалення), IP-адреса користувача та її стабільність, геолокаційні маркери та структура самих SQL-запитів.

Зібрані дані піддаються попередній обробці. Зокрема, часові характеристики нормалізуються до уніфікованого формату, текстові значення (типів операцій або IP) переводяться у числові представлення з використанням one-hot або label-encoding, а також проводиться усереднення частот та агрегація по часових вікнах. Це дозволяє зменшити шум і підвищити чутливість моделі до відхилень.

Після нормалізації для кожного користувача формується вектор поведінки – числове представлення його типових дій за обраний період. Ці вектори зберігаються у базі профілів і

© Розломій І.О., Науменко С.В., Ковтюх В.А.

використовуються як референс при поточному аналізі подій.

Для забезпечення стійкості поведінкових профілів до короткочасних коливань активності користувачів формування ознак здійснюється на основі ковзних часових вікон фіксованої або адаптивної довжини. Такий підхід дозволяє враховувати природні варіації у поведінці, зумовлені змінами робочого навантаження, часовими поясами або специфікою виконуваних завдань, та водночас зменшити вплив одиничних нетипових подій. Агрегування ознак у межах часових вікон забезпечує стабільність векторів поведінки та підвищує точність подальшої класифікації.

Крім того, для кожної ознаки визначаються базові статистичні характеристики, зокрема середнє значення, дисперсія та допустимі інтервали варіації, що дозволяє формувати узагальнений опис типової активності користувача. Такий підхід забезпечує універсальність моделі та її адаптацію до різних ролей користувачів у хмарній СУБД, зокрема адміністраторів, аналітиків або прикладних сервісів. Сформований набір агрегованих характеристик використовується як еталон нормальної поведінки під час аналізу нових сесій доступу.

У табл. 1 представлено приклад поведінкового профілю користувача, який демонструє основні агреговані характеристики.

Таблиця 1. Приклад побудованого профілю користувача

Ознака	Значення
Середній час підключення	10:15
Стандартне відхилення часу	25 хв
Частота запитів/год	12
Переважний тип запитів	SELECT
Середній обсяг даних (MB)	3,2
Середня довжина SQL-запиту	48 символів
Типові IP-адреси	192.168.1.12, 192.168.1.14
Геолокація	Київ, Україна

Цей профіль буде використовуватись як шаблон «нормальної» поведінки, з яким порівнюються поточні дії користувача в системі. Відхилення від даних показників будуть класифікуватись як потенційно аномальні.

В основі математичної моделі системи виявлення аномалій лежить ідея визначення нормального простору поведінки користувачів та виявлення точок, що значно від нього відхиляються. Формально, кожна поведінкова сесія користувача описується вектором ознак $x \in R^n$, сформованим на основі агрегованих даних доступу до хмарної СУБД. Мета моделі – визначити, чи належить новий вектор x' до простору нормальної поведінки, чи є він аномальним.

У межах цього дослідження як основний метод було обрано автоенкодер – нейронну мережу, що навчається відтворювати вхідні дані, мінімізуючи функцію помилки реконструкції. При цьому нормальні шаблони поведінки відтворюються з малою помилкою, тоді як аномальні – із великою. Нехай $\hat{x} = AE(x)$ – результат реконструкції автоенкодером, тоді відхилення обчислюється як середньоквадратична помилка (1).

$$\delta(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2 \quad (1)$$

Порогове значення θ визначається емпірично або за допомогою статистичних методів (наприклад, 95-й процентиль значень помилки на навчальній множині). Якщо $\delta(x') > 0$, сесія класифікується як аномальна.

Для оцінювання здатності моделі відокремлювати нормальні поведінкові сесії від аномальних було проаналізовано розподіл значень помилки реконструкції e для двох підмножин даних: нормальної активності та штучно змодельованих відхилень. Нехай e_n – середнє значення помилки для множини нормальних сесій, e_a – середнє значення для аномальних.

Величина розділення між цими множинами визначалась як $\Delta = e_a - e_n$. Чим більшим є значення Δ, тим чіткіше модель відокремлює нормальний простір поведінки від аномального.

© Розломій І.О., Науменко С.В., Ковтюх В.А.

Додатково було оцінено відносну стабільність реконструкції для нормальних даних через коефіцієнт варіації $v = \frac{\sigma_n}{e_n}$, де σ_n – стандартне відхилення помилки реконструкції для нормальних сесій.

Невеликі значення v свідчать про стабільність поведінкової моделі користувача та високу узгодженість реконструкції нормальних шаблонів активності. У випадку появи нетипових дій значення помилки реконструкції різко зростає, що призводить до значного збільшення показника Δ і дозволяє впевнено ідентифікувати аномальні події.

Альтернативно, у випадках обмежених обчислювальних ресурсів або коли нейромережеві моделі є недоцільними, може бути використано One-Class SVM або Isolation Forest. Перший створює межу навколо нормальних даних, другий – ізолює точки, які легко відокремити від інших, що часто відповідає аномаліям.

Запропонована система була реалізована з використанням Python та бібліотек TensorFlow/Keras для побудови нейронної мережі автоенкодера. Для зберігання логів подій та профілів поведінки застосовувалась СУБД PostgreSQL. Хмарну інфраструктуру було розгорнуто на платформі AWS, де використовувались сервіси EC2 для обчислень і RDS для бази даних. Збір логів реалізовано за допомогою PostgreSQL Audit Extension, що дозволяє отримувати дані про кожну SQL-операцію користувача.

Інтеграція здійснювалась за допомогою регулярного експорту логів у форматі CSV, що надходили до модуля збору подій, після чого вектори ознак формувались у режимі реального часу. Обробка та класифікація виконувались у рамках модуля аномалій, а результати виводились у вигляді таблиць і графіків для подальшого аналізу.

Для перевірки працездатності системи було сформовано тестовий набір даних, що включав як нормальні, так і модифіковані сесії з аномаліями: незвичний час доступу, зміну IP-адреси, нетипову частоту запитів та нові типи операцій. Виявлені аномалії позначались червоними маркерами на графіку розсіювання.

Для оцінки ефективності запропонованої системи було здійснено експериментальне тестування з використанням згенерованого набору поведінкових сесій, що включав як типові (нормальні), так і модифіковані з аномаліями. Змодельовані відхилення включали зміну звичних параметрів доступу, таких як геолокація, IP-адреса, типи запитів і час підключення. Після обробки даних нейронною моделлю автоенкодера було здійснено класифікацію сесій на нормальні та аномальні, що дало змогу наочно оцінити розподіл поведінки користувачів у просторі ознак. Графік результатів класифікації представлено на рис. 2.

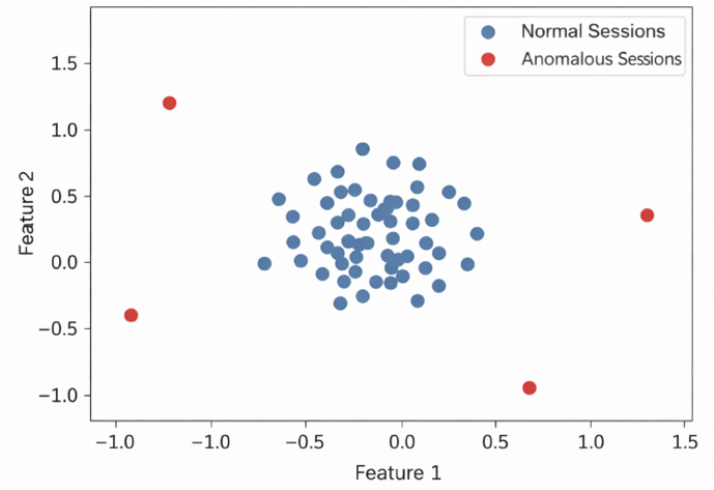

Рис. 2. Розподіл нормальної та аномальної поведінки користувачів

На рисунку 2 продемонстровано результати класифікації подій доступу: нормальні дії розміщені у щільному кластері, тоді як аномальні – виявляються на периферії простору ознак, що підтверджує ефективність застосованої моделі.

Запропонована система була проаналізована порівняно з низкою існуючих підходів до виявлення аномальної активності у доступі до даних. У якості критеріїв оцінювання було обрано точність (accuracy), повноту (recall), швидкість виявлення (latency) та здатність адаптуватися до нових шаблонів поведінки без ручного втручання (adaptability). Для порівняння обрано чотири

© Розломій І.О., Науменко С.В., Ковтюх В.А.

підходи: статистичний метод порогового аналізу, кластеризацію k-means, One-Class SVM та запропоновану модель на основі автоенкодера.

Таблиця 2. Порівняння ефективності методів виявлення аномалій у поведінці користувачів

Метод	Accuracy	Recall	Latency (ms)	Adaptability
Статистичний поріг	0.82	0.64	15	Низька
K-means кластеризація	0.86	0.71	48	Середня
One-Class SVM	0.89	0.77	130	Висока
Autoencoder (запропон.)	0.92	0.85	95	Висока

Для кількісної оцінки ефективності моделі було проведено серію експериментів на тестовому наборі поведінкових сесій, що включав як типові сценарії доступу, так і штучно змодельовані відхилення. Загальний обсяг вибірки становив 500 сесій, серед яких 120 містили аномальні характеристики (зміну геолокації, нетипову частоту запитів, аномальний час доступу або нетипові SQL-операції).

Середнє значення помилки реконструкції для нормальної поведінки становило $e_n = 0.021$, тоді як для аномальних сесій $e_a = 0.147$. Відповідно різниця між цими значеннями $\Delta = 0.126$ свідчить про значний рівень відокремлення аномальних поведінкових шаблонів від нормального простору даних. Стандартне відхилення помилки реконструкції для нормальних сесій становило $\sigma_n = 0.006$, що відповідає коефіцієнту варіації $v = 0.29$.

Отримані значення демонструють стабільність реконструкції нормальної поведінки та значне зростання помилки у випадку аномальної активності. Такий контраст між значеннями e_n та e_a забезпечує надійність класифікації поведінкових сесій і підтверджує ефективність запропонованої моделі у задачі виявлення відхилень у доступі до даних.

Згідно з результатами, модель на основі автоенкодера продемонструвала найкраще поєднання точності та повноти при помірному рівні затримки. Найбільшу адаптивність до нових шаблонів поведінки також виявлено саме в нейронної моделі, яка має здатність навчатися на потокових даних та автоматично оновлювати профілі без ручної участі адміністратора. У порівнянні з One-Class SVM, автоенкодер краще справляється з високовимірними просторами ознак, що є типовим для поведінкових даних у хмарних СУБД.

Практична цінність запропонованого рішення полягає в його застосовності до сучасних хмарних середовищ, де поведінка користувачів є нестабільною та може швидко змінюватися в залежності від задач, змін у штаті або віддаленого доступу з різних регіонів. На відміну від класичних підходів із фіксованими політиками або ручним налаштуванням правил, система здатна автоматично адаптуватися до змін, формуючи нові поведінкові шаблони.

Крім того, запропонована модель підтримує інтеграцію у CI/CD-процеси безпеки, що дозволяє вбудовувати її в сучасні хмарні архітектури, оновлювати поведінкові профілі без зупинки сервісу та реагувати на аномалії в режимі реального часу. Це забезпечує безперервний моніторинг активності та швидке реагування на загрози без втручання оператора.

Наукова новизна полягає у поєднанні кількох підходів: використанні ознак поведінки, специфічних для хмарних СУБД, застосуванні нейронного автоенкодера для відтворення поведінки та обчислення відхилення, а також впровадженні циклічного оновлення профілів користувачів. Запропонована модель має потенціал для подальшого розвитку, зокрема шляхом розширення ознак, інтеграції з потоковими обчисленнями та масштабування на багатоарендні хмарні платформи.

Висновки та перспективи подальшого дослідження. У статті запропоновано архітектуру та математичну модель системи виявлення аномалій у доступі до даних у хмарних СУБД на основі поведінкової аналітики. Обґрунтовано вибір ключових ознак, що формують профілі користувачів, а також використання автоенкодера як ефективного методу виявлення відхилень у поведінці. Проведено порівняльний аналіз із альтернативними підходами, який підтвердив переваги запропонованого рішення за критеріями точності, повноти та адаптивності. Система показала здатність до виявлення нестандартних дій у реальному часі, що робить її придатною для інтеграції

© Розломій І.О., Науменко С.В., Ковтюх В.А.

в сучасні хмарні середовища.

Практична реалізація довела застосовність моделі для моніторингу доступу в умовах динамічного навантаження та множинних точок підключення. Формування поведінкових профілів дозволяє не лише фіксувати порушення, але й будувати контекстуальне розуміння взаємодії користувача із системою, що підвищує загальний рівень безпеки.

Кількісна оцінка роботи моделі показала значне розділення між простором нормальної та аномальної поведінки користувачів. Середнє значення помилки реконструкції для нормальних сесій становило $e_n = 0.021$, тоді як для аномальних – $e_a = 0.147$. Різниця між цими значеннями $\Delta = 0.126$ підтверджує здатність автоенкодера формувати компактний простір нормальної поведінки та ефективно виявляти відхилення. Низьке значення коефіцієнта варіації $v = 0.29$ додатково свідчить про стабільність реконструкції поведінкових шаблонів. Отримані результати підтверджують практичну ефективність запропонованої математичної моделі для задач моніторингу доступу до даних у хмарних СУБД.

Перспективи подальших досліджень полягають у розширенні набору поведінкових ознак, включенні параметрів сеансової активності, використанні методів потокового навчання та адаптації моделі до багатокористувацьких і мультиорендних хмарних архітектур. Окрему увагу планується приділити інтеграції з системами управління інцидентами, формалізації оцінки ризику на основі поведінкових змін і забезпеченню масштабованості рішення в умовах великого обсягу даних.

Список бібліографічного опису

1. Omotunde, H., Ahmed, M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity. 2023. Vol. 2023. P. 115–133. https://doi.org/10.58496/MJCSC/2023/016
2. Zabolotnii, S., Rozlomii, I., Yarmilko, A., Naumenko, S. Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2025. Vol. 15. No. 4. P. 164–169. https://doi.org/10.35784/iapgos.7782
3. Rozlomii, I. O., Naumenko, S. V. Архітектура та функціональні особливості захищених систем керування базами даних нового покоління з підтримкою serverless та edge-обчислень. Systems and Technologies. 2025. Vol. 69. No. 1. P. 130–137. https://doi.org/10.32782/2521-6643-2025-1-69.16
4. Gadde, H. AI-augmented database management systems for real-time data analytics. Revista de Inteligencia Artificial en Medicina. 2024. Vol. 15. No. 1. P. 616–649.
5. Pan, J. J., Wang, J., Li, G. Survey of vector database management systems. The VLDB Journal. 2024. Vol. 33. No. 5. P. 1591–1615. https://doi.org/10.1007/s00778-024-00864-x
6. Halder, R. K., Uddin, M. N., Uddin, M. A., Aryal, S., Khraisat, A. Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications. Journal of Big Data. 2024. Vol. 11. No. 1. P. 113. https://doi.org/10.1186/s40537-024-00973-y
7. Khan, S. M., Shafi, I., Butt, W. H., Diez, I. D. L. T., Flores, M. A. L., Galán, J. C., Ashraf, I. A systematic review of disaster management systems: Approaches, challenges, and future directions. Land. 2023. Vol. 12. No. 8. P. 1514. https://doi.org/10.3390/land12081514
8. Mustafa, A., Huma, Z. Neural networks for database anomaly detection in SQL Server. Pioneer Research Journal of Computing Science. 2024. Vol. 1. No. 3. P. 13–22.
9. Chaudhry, M., Shafi, I., Mahnoor, M., Vargas, D. L. R., Thompson, E. B., Ashraf, I. A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. Symmetry. 2023. Vol. 15. No. 9. P. 1679. https://doi.org/10.3390/sym15091679
10. Vashishth, T. K., Sharma, V., Kumar, B., Sharma, K. K. Cloud-based data management for behavior analytics in business and finance sectors. Data-Driven Modelling and Predictive Analytics in Business and Finance. 2024. P. 133–155. Auerbach Publications.
11. Wang, Y., Bourhis, P., Rouvoy, R., Royer, P. Challenges and opportunities in automating DBMS: A qualitative study. Proceedings of the 39th IEEE ACM International Conference on Automated Software Engineering. 2024. P. 2013–2023. https://doi.org/10.1145/3691620.3695264

References

1. Omotunde, H., Ahmed, M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity. 2023. Vol. 2023. P. 115–133. https://doi.org/10.58496/MJCSC/2023/016
2. Zabolotnii, S., Rozlomii, I., Yarmilko, A., Naumenko, S. Reconfigured CoARX architecture for implementing ARX hashing in microcontrollers of IoT systems with limited resources. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2025. Vol. 15. No. 4. P. 164–169. https://doi.org/10.35784/iapgos.7782
3. Rozlomii, I. O., Naumenko, S. V. Architecture and functional features of next-generation secure database management systems with support for serverless and edge computing. Systems and Technologies. 2025. Vol. 69. No. 1. P. 130–137. https://doi.org/10.32782/2521-6643-2025-1-69.16
4. Gadde, H. AI-augmented database management systems for real-time data analytics. Revista de Inteligencia Artificial en Medicina. 2024. Vol. 15. No. 1. P. 616–649.

© Розломій І.О., Науменко С.В., Ковтюх В.А.

5. Pan, J. J., Wang, J., Li, G. Survey of vector database management systems. The VLDB Journal. 2024. Vol. 33. No. 5. P. 1591–1615. https://doi.org/10.1007/s00778-024-00864-x
6. Halder, R. K., Uddin, M. N., Uddin, M. A., Aryal, S., Khraisat, A. Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications. Journal of Big Data. 2024. Vol. 11. No. 1. P. 113. https://doi.org/10.1186/s40537-024-00973-y
7. Khan, S. M., Shafi, I., Butt, W. H., Diez, I. D. L. T., Flores, M. A. L., Galán, J. C., Ashraf, I. A systematic review of disaster management systems: Approaches, challenges, and future directions. Land. 2023. Vol. 12. No. 8. P. 1514. https://doi.org/10.3390/land12081514
8. Mustafa, A., Huma, Z. Neural networks for database anomaly detection in SQL Server. Pioneer Research Journal of Computing Science. 2024. Vol. 1. No. 3. P. 13–22.
9. Chaudhry, M., Shafi, I., Mahnoor, M., Vargas, D. L. R., Thompson, E. B., Ashraf, I. A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. Symmetry. 2023. Vol. 15. No. 9. P. 1679. https://doi.org/10.3390/sym15091679
10. Vashishth, T. K., Sharma, V., Kumar, B., Sharma, K. K. Cloud-based data management for behavior analytics in business and finance sectors. Data-Driven Modelling and Predictive Analytics in Business and Finance. 2024. P. 133–155. Auerbach Publications.
11. Wang, Y., Bourhis, P., Rouvoy, R., Royer, P. Challenges and opportunities in automating DBMS: A qualitative study. Proceedings of the 39th IEEE ACM International Conference on Automated Software Engineering. 2024. P. 2013–2023. https://doi.org/10.1145/3691620.3695264

Історія статті:
Отримано: 18.02.2026 Доопрацьовано: 04.03.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026

© Розломій І.О., Науменко С.В., Ковтюх В.А.