Метод Захисту Баз Даних Шляхом Багатошарового Користувацького Доступу

Олеся Войтович
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
voytovych.olesya@vntu.edu.ua

Іван Микитюк
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
mikityukchanel@gmail.com

Database Protection by Multilayer User Access

Olesia Voitovych
dept. of Cybersecurity
Vinnytsia National Technical University
Vinnytsia, Ukraine
voytovych.olesya@vntu.edu.ua

Ivan Mikityuk
dept. of Cybersecurity
Vinnytsia National Technical University
Vinnytsia, Ukraine
mikityukchanel@gmail.com

***Анотація*—У статті запропоновано підхід та метод захисту інформації, що зберігається у базах даних шляхом створення багатошарової структури користувацького доступу до функцій СКБД. На основі запропонованого підходу та використання аналізу захищеності сучасних СКБД розроблено модульну систему захисту інформації у базах даних.**

***Abstract*—The analysis of modern DBMS and developing new method of databases security is described in the article. The analysis allows highlighting the main shortcomings of modern DBMS - poor protection against loss of user access data and the use of discretionary access control mechanism to the management function. Based on analyzing, multilayer approach to the user's access to the functions of the DBMS as the main stage of protection is proposed. The proposed approach help to design the modular system of data base protection. The modular system of information protection divides in 3 layers. Every layer uses crypto-algorithms and hash-functions, which can help creator of database to protect his DB from unpredictable access and make system more flexible and secure. First layer is getting access to the user rights which can give user simple access to read DB information. Second layer is getting access to the redactor rights. This layer requires the input of user information and selection correct hash algorithm. Third layer is getting personal administrator access to the all rights in database. It can be creator access or simple administrator or moderator access. This layer requires availability of personal flash-card or any user-selected authentication data which can checked by a DBMS when user make a request to get personal access to all DBMS functions. Additional mechanism is blockchain database validation, which help user to protect integrity of his information. The developed modular database protection system allows users to pay attention to the state of the modern authentication algorithm and adds a contribution to the development of protection of modern DBMS in general.**

Ключові слова—база даних; захист баз даних; багатошаровий захист; шифрування; гешування; blockchain.

Keywords—database; database protection; multilayer protection; cryptographic algorithms; hash; blockchain.

I. Вступ

Бази даних – найпопулярніший спосіб збереження та маніпулювання користувацькою інформацією. Використання систем керування базами даних набуло широкого використання у сучасному, швидкому суспільстві і з розвитком інформаційних технологій механізми захисту СКБД втрачають свою потужність та актуальність і відповідно потребують доопрацювань [1]. Серед сучасних засобів керування базами даних важко зустріти представника, який би надавав користувачу додатковий, специфічний захист його інформації. В додаток до розвитку інформаційних технологій та потреб користувачів йде розвиток методів та технологій, які використовуються зловмисником, і спричиняють зростання ризиків втрати автентифікаційних даних користувачів у СКБД.

У ході дослідження стану сучасних СКБД [2-4], було виявлено, що в більшості з них використовується дискреційна модель надання доступу користувачам та адміністраторам, що збільшує ризик компрометації автентифікаційних даних (підглядування чи підбір паролю).

У зв’язку з цим постає задача – реалізувати підхід захисту баз даних, який має додатковий механізм, що дозволяє розділяти доступ до функцій СКБД на різних функціональних рівнях.

II. Аналіз проблем захищеності сучасних СКБД

Сучасні СКБД можуть бути охарактеризовані, як програмні засоби з високим ступенем захищеності інформації, яка зберігається в базах даних під їх управлінням, проте під час їх аналізу було виявлено один з недоліків [6], а саме використання одного бар'єру (дискреційної, рольової, моделі доступу).

При аналізі проблеми було виявлено, що на сьогодні СКБД надають користувачам певні ролі, які мають свій набір привілеїв [6], основні з них зображені у таблиці 1 [7].

ТАБЛИЦЯ І. Ролі користувачів у сучасних СКБД

Роль	Можливості	Загрози
Власник	Усі дії по налаштуванню та обслуговуванню БД та видалення	Втрата даних у зв'язку з некомпетентністю чи халатністю,
Адміністратор	Адміністрування бази даних, надання привілеїв.	Цілісність даних, ненавмисне надання прав іншим користувачам.
Редактор	Редагування та видалення даних у таблицях	Цілісність та конфіденційність даних
Читач	Зчитування даних	Конфіденційність даних
Користувач без прав	Не може виконувати дії з БД	-

Для аналізу та висування пропозицій слід перелічити деякі з реалізацій загроз, наведених у таблиці 1.

Загрози отримання зловмисником автентифікаційних даних відповідної ролі такі:

- читач бази даних дасть змогу зловмиснику вкрасти інформацію;
- редактор дасть змогу відредагувати інформацію у БД;
- адміністратор дасть змогу приховано надати права користувачам, що не мають відповідного рангу;
- власник ставить під загрозу існування бази даних в цілому.

Проаналізувавши загрози (табл. 1) було виявлено ті, що можуть бути реалізовані відповідними користувачами. Сучасні СКБД надають права щодо користування базою даних після автентифікації користувача з необхідним рівнем доступу, тобто зловмиснику стає доступним рівень доступу користувача, в якого він міг отримати автентифікаційні дані. Даних підхід, як і будь-яка дискреційна (рольова) модель доступу, відкриває багато можливостей для несанкціонованого доступу до даних через перехоплення автентифікаційних даних та зловживання повноваженнями. З цього можна зробити висновок, що однорівневий захист є проблемою, яку необхідно вирішити.

В реальних умовах при роботі з СКБД створюється достатня кількість проблем з точки зору безпеки, які зв'язані з користувацькою авторизацією. Це можуть бути, як проблеми звичайного підглядання паролю з боку працівників, що сидять поруч, так і проблеми крадіжок необхідних даних шляхом використання власних користувацьких автентифікаційних даних з невідповідною високою користувацькою роллю. З цього можна зробити висновок, що сучасні СКБД, які мають слабкий парольний захист, чи потребують більшого рівня захисту [8], потребують покращення системи авторизації.

Після проведення досліджень можна зробити висновок, що досліджені СКБД мають низку переваг у вигляді можливості дуже гнучко налаштовувати власний функціонал. Проте з аналізу можна виділити основні недоліки сучасних СКБД – слабкий захист від втрати користувацького доступу та використання слабких моделей розмежування користувацького доступу до функції з управління.

Відповідно до переваг відомих СКБД запропоновано використовувати криптографічні функції, зокрема гешування [9] та шифрування [10], використовуючи сучасні та стійкі криптоалгоритми, проте на прикладі поточної розробки вони будуть використовуватись дещо іншим способом. Отже до процесу отримання та аналізу інформації про сучасні СКБД було виділено два модулі, які необхідно реалізувати: гешування та шифрування.

III. Побудова та впровадження багатошарової системи захисту інформації

Для покращення ситуації запропоновано розшарування доступу до різних функціональних рівнів СКБД шляхом ускладнення доступу користувачів до функцій СКБД залежно від привілеїв, що їм надаються (рис. 1).

Для забезпечення належного захисту інформації необхідно комбінувати найкращі існуючі напрацювання та розбивати їх використання на «рівні захисту». Це дасть деякі переваги: користувач, який не володіє необхідним набором автентифікаційних даних отримає доступ тільки до відповідного рівня взаємодії з базою даних .

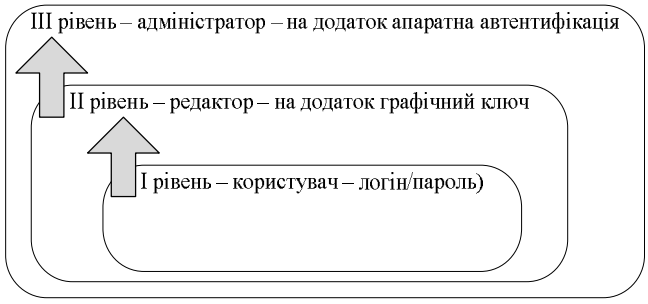

Рис. 1. Схема користувацького доступу до функцій СКБД у відповідності до рівнів захисту

Для того щоб реалізувати відповідні функції шарів отримання доступу до функцій СКБД передбачено реалізацію геш-функцій та основних криптографічних алгоритмів, які будуть використовуватись для гешування атрибутів та шифрування інформації, проте ці функції будуть реалізовані на різних «шарах» проходження користувацької автентифікації.

Першим і початковим рівнем є автентифікація користувача, яка дозволяє зловмиснику отримати *перший*

рівень доступу до інформації у БД, прикладом якого може бути реалізація алгоритму авторизації за допомогою введення комбінації логіну та паролю.

Отримавши перший рівень користувач, який хоче відредагувати інформацію має підтвердити свої права редактора для отримання доступу до функцій, які знаходяться на *другому рівні доступу*.

Прикладом реалізації автентифікації при отриманні прав другого рівня (функціонального рівня редактора) може бути сутність, яка використовує алгоритми гешування і зберігає геш-значення з таблицею, до якої хоче отримати доступ, особа з правами користувача. Для переходу на другий рівень користувачеві пропонується ввести графічний пароль, та вибрати геш-функцію, яка повинна до нього примінитись. Після введення, автентифікаційні дані зіставляються з даними, які прив'язані до БД, і, після підтвердження, надається доступ.

Третій рівень доступу реалізується підтвердженням доступу з другого рівня (рівня редактора), наприклад шляхом наявності флешки-ключа. При запиті на отримання найвищих прав користувачеві виводиться повідомлення, яке пропонує йому вставити флешку з файлом, який містить необхідне для підтвердження прав геш-значення, яке було згенероване під час створення БД і відвантажене на флешку. При наявності необхідного файлу його дані скануються та зіставляються з наявними даними у БД. Також можлива реалізація з використанням технології одноразових пароль, що генеруються на основі отриманого геш-значення.

Узагальнена схема отримання доступу відповідно до рівнів захисту показана на рис.2.

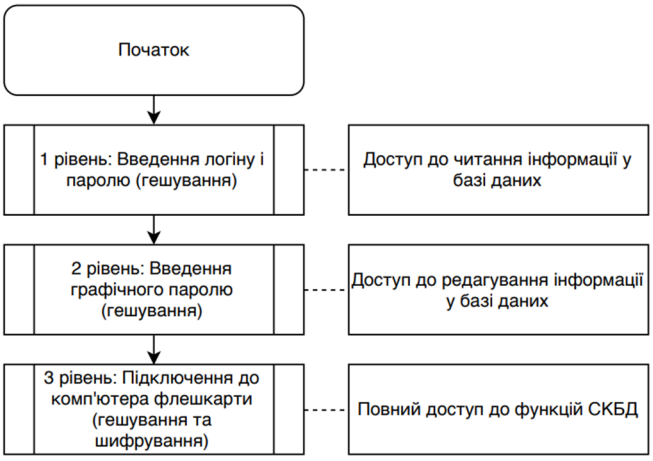

Рис. 2. Вигляд рівнів захисту з криптографічнми функціями, які на них використовуються

У зв'язку з цим час, потрачений на процес отримання необхідних користувачеві привілеїв збільшиться, але дозволить відслідковувати та керувати доступом користувачів і захищати цілісність та конфіденційність бази даних. Крім того, доступ з правами третього рівня потрібен тільки у виключних ситуаціях, і затримка не сильно впливає на нормальну роботу з базою даних.

Такі три шари захисту дозволяють обмежити можливості зловмиснику, який хоче, наприклад, видалити БД. Зламавши пароль він зупиниться на шарі захисту, який пропонує вибір геш-функції та введення графічного паролю, до якого вона буде застосовуватись. Після цього, зловмиснику необхідно подолати наступний шар – наявність носія з електронним-ключем, і наприкінці співставлення отриманих автентифікаційних даних зі списком ролей та відповідним йому списком користувачів. Таким чином, зловмисник, який отримав автентифікаційні дані одного користувача, графічний пароль та геш-функцію другого користувача, а носій в третього користувача, не зможе отримати доступ.

В доповнення до багатошарової моделі доступу до користувацької інформації у базі даних, використано порівняно нову технологію, а саме blockchain [11]. Дана технологія дозволить базі даних мати додатковий рівень захисту інформації щодо забезпечення цілісності інформації, яка у ній зберігається та структури бази даних в цілому. Дана технологія дозволить зв'язати усю важливу інформацію в один ланцюг даних, які залежатимуть один від одного, і, при неправомірній зміні інформації зловмисником, відразу ж буде відображення помилки та мутації при використанні БД іншими користувачами, і, цим самим, дозволить користувачам розпізнати можливі ситуації, коли базу було змінено без відома інших.

IV. Реалізації методу багатошарової системи захисту інформації

Для проведення експериментальних дослідження та перевірки моделі багатошарової системи захисту інформації з розділення користувацького доступу на необхідні адміністратору БД рівні було прийнято рішення реалізувати запропоновану систему у вигляді програмного засобу. Загальна схема запропонованих для реалізації механізмів захисту показана на рис.3.

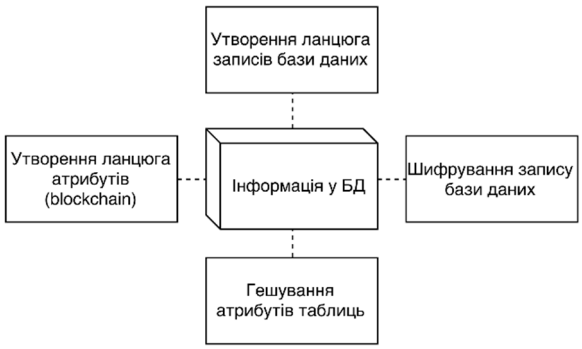

Рис. 3. Загальна схема запропонованих механізмів захисту бази даних

Відповідно до рівнів та використання криптографічних функцій було виділено два шляхи:

- використання криптографічних функцій для захисту користувацької автентифікаційної інформації

- використання криптографічних функцій для безпосереднього захисту інформації у базах даних.

Алгоритм гешування користувацької інформації передбачає збереження будь-яких автентифікаційних даних у загешованому вигляді, що захищає їх від зламу таким чином, що зловмисник, отримавши до них доступ, не може їх використати у своїх цілях при подальшому зламі СКБД. Кожен користувач на етапі автентифікації на одному з рівнів вводить автентифікаційні дані, після чого вони геруються, і, в загешованому вигляді, порівнюються з даними, які відповідають цьому користувачеві на даному рівні захисту.

Для забезпечення цілісності інформації, яка зберігається у базі даних, застосовується технологія blockchain, яка є аналогом ланцюга, дані в якому накопичуються і формують постійно зростаючу базу даних [11]. Однією з головних особливостей даної технології є те, що дані, які зберігаються у ланцюгу неможливо видалити чи здійснити заміну/заміщення блока. Нові блоки завжди додаються виключно в кінець ланцюжка і кожен наступний блок залежить від попереднього. Дана технологія у повні мірі може бути використана при збереженні інформації у таблицях бази даних та перелікові атрибутів у таблиці, що допоможе забезпечити цілісність користувацької інформації, та незмінність атрибутів у БД.

Вигляд вікна тестового програмного засобу з використанням технології blockchain показано на рис. 4.

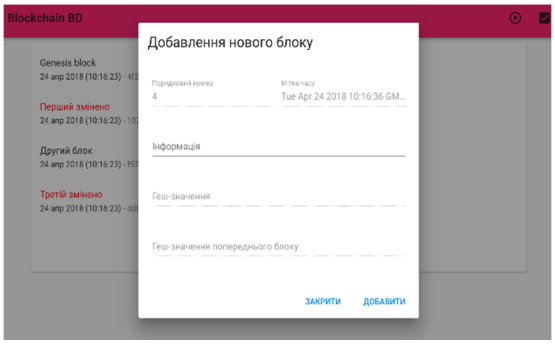

Рис. 4. Вигляд вікна тестового програмного засобу з використанням технології blockchain

Перший рівень захисту інформації у БД включає шифрування, яке забезпечить цілісність, доступність та конфіденційність інформації, яка у ній знаходиться. Отримавши прямий доступ до БД шляхом зламу СКБД, зловмисник зможе зчитати тільки зашифровану інформацію, а для отримання даних у відкритому вигляді йому необхідно пройти принаймні один рівень автентифікації, для отримання функцій першого рівня.

Другий рівень захисту інформації базується на технології blockchain, яка спрямована на забезпечення цілісності даних у таблицях та цілісності самих атрибутів таблиць.

Висновки

У ході аналізу сучасних СКБД було виявлено один з недоліків вбудованих в них засобів захисту, а саме використання дискреційної (рольової) моделі доступу до функцій з адміністрування СКБД групами користувачів.

Пропонується підхід, який передбачає включення багатошарового захисту, який полягає у тому, що при переході на наступний функціональний рівень керування СКБД використовується додатковий механізм автентифікації користувачів (наприклад, логін-пароль графічний пароль, та наявність апаратного ключа).

Наведено метод багатошарового захисту баз даних з використанням геш-функцій криптографічних алгоритмів та технології blockchain, які надаватимуть комплексний підхід до забезпечення цілісності та конфіденційності даних, що збережені у БД.

Для проведення експериментальних досліджень, реалізовано програмний засіб, що показує можливість реалізації методу захисту бази даних.

Література References

[1] Микитюк І.С., Войтович О.П. Захист баз даних шляхом фрагментування користувацького доступу // Матеріали XLVII Науково-технічної конференції факультету інформаційних технологій та компютерної інженерії (2018).

[2] Зрюмов, Е. А. Базы данных для инженеров: навчальний посібник / Е. А. Зрюмов, А. Г. Зрюмова; Алт. держ. техн. ун-т им. И. И. Ползунова. – Барнаул : Видав-во АлтГТУ, 2010. – 131 с.

[3] Kupershtein L. M. The database-oriented approach to data protection in Android operation system / Kupershtein L. M., Voytovych O. P., Procopcuk S.O., Kaplun V.A. // Вісник ХНУ : серія Технічні науки. - №1. -2018. - С. 18-22

[4] Баришев Ю. В., Каплун В. А., Неуйміна К. В. Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів // Наукові паці ВНТУ. – 2017. – №2. – 8 с.

[5] Шайтанова Н. Ж., Туленгалиева М.Г. Защита информации в базах данных [Електронний ресурс]. Режим доступу: URL : http://www.rusnauka.co m/10_DN_2014/Informatica/3_165120.doc.htm – Назва з екрану.

[6] Микитюк І.С., Баришев Ю.В. Підхід до захисту баз даних: тези на наукову конференцію // Матеріали XLVII Науково-технічної конференції факультету інформаційних технологій та компютерної інженерії (2017).

[7] Microsoft Docs. Роли уровня баз даных. [Електронний ресурс]. Режим доступу: URL: https://docs.microsoft.com/ru-ru/sql/relational-databases/security/authentication-access/database-level-roles - Назва з екрану.

[8] Полтавцева М. А., Хабаров А. Р. Безопасность баз данных: проблемы и перспективы //Программные продукты и системы. – 2016. – №. 3 (115).

[9] Сучасні криптографічні системи: Навч. посібник. – Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 стор.

[10] Євсеєв С.П. Гешування даних в інформаційних системах : монографія / С.П.Євсеєв, О.Ю.Йохов, О.Г.Король – Х. : Вид. ХНЕУ, 2013. – 312с.

[11] Щербань Е. Что такое блокчейн, и как он работает [Електронний ресурс]. Режим доступу: URL : https://revolverlab.com/how-its-works-blockchain-6d0355c43bfc – Назва з екрану.