Використання блокчейн-технології для підвищення безпеки від SQL ін'єкцій

УДК 004.056

Ірина Замрій[1], Іван Шахматов[2]

Державний університет інформаційно-комунікаційних технологій,
1irinafraktal@gmail.com, 2ivan.shakhmatov@gmail.com

Загроза SQL-ін'єкцій залишається актуальною проблемою у сфері веб-розробки, оскільки вони виявляють вразливості систем і дозволяють зловмисникам отримувати несанкціонований доступ до даних [1-2]. Цей вид атак полягає у введенні шкідливого SQL-коду через інтерфейс користувача, що може призвести до ннесанкціонованого доступу, витоку або втрати інформації. Зловмисники активно шукають слабкі місця у захисті для того, щоб отримати доступ до конфіденційної інформації, видалити критично важливі дані або навіть заволодіти контролем над серверами.

Модель BlockchainSQLSecure є рішенням для забезпечення безпеки SQL, яке поєднує технології блокчейн та фільтр Блума для виявлення та запобігання SQL ін'єкціям. Унікальність полягає в тому, що модель не обмежується лише відстеженням стандартних сценаріїв SQL-ін'єкцій, а замість цього використовує блокчейн для надійного зберігання інформації про попередні запити. Це дозволяє створити журнал стійкий до змін з можливістю перевірки у будь-який момент з метою забезпечення безпеки даних.

Розроблена модель не потребує великих обчислювальних ресурсів для своєї роботи і може легко інтегруватися у наявні системи. Фільтр Блума, у свою чергу, забезпечує високу швидкість і ефективність обробки, що робить його ідеальним для роботи з великими обсягами даних. У моделі BlockchainSQLSecure ключовим аспектом є визначення схожості між SQL-запитами для ефективного виявлення та запобігання спробам SQL-ін'єкцій. Для досягнення цієї мети використовується формула відстані Жаккара:

$$d(X, Y) = \frac{\sum_{i=1}^{n} X_i Y_i}{\sum_{i=1}^{n} X_i^2 + \sum_{i=1}^{n} Y_i^2 - \sum_{i=1}^{n} X_i Y_i} \quad (1)$$

де X_i, Y_i – координати векторів X та Y відповідно.

Ідентифікація між двома SQL-запитами відбувається за формулою (1), де значення, що прямує до 1, вказує подібність, а значення, що прямує до 0, вказує на відмінність. Ця відстань є важливим елементом алгоритму видалення дублікатів даних на основі фільтра Блума і підвищує ефективність і точність моделі. Метрика дозволяє швидко визначити, чи є новий SQL-запит варіантом вже існуючого SQL-запиту, що містить потенційну спробу ін'єкції. Використання відстані Жаккара в поєднанні з фільтром Блума підвищує ефективність і точність системи у виявленні та запобіганні SQL-ін'єкцій.

Запропонована UML-діаграма (рис. 1) показує класову структуру інноваційної системи, яка поєднує в собі функції обробки SQL-запитів, управління блокчейн-

транзакціями, контролю дій користувачів та використання фільтру Блума для оптимізації запитів. Розроблена UML-діаграма містить п'ять основних класів: User, SQLQuery, BlockchainManager, AuditLogger та BloomFilter, кожен з яких відіграє важливу роль у функціонуванні системи та встановленні взаємозв'язків, залежностей між класами.

Розробка системи на мові програмування Python дозволила прийняти принципи чистого кодування, забезпечивши якість, легкість розуміння та можливість подальшого розширення проекту. Архітектура системи була розроблена у вигляді модулів та класів, що забезпечило чітку структуру та розподіл обов'язків.

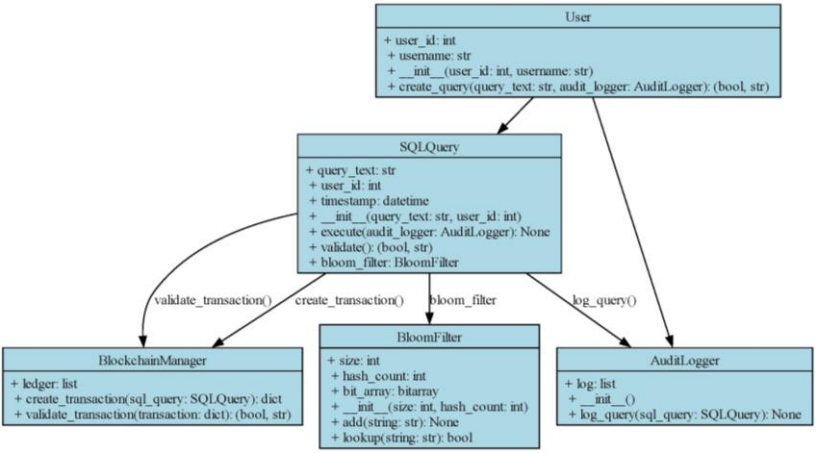

Рис. 1 UML-діаграма класів для системи управління базою даних та блокчейн-транзакціями

Створена система демонструє високий рівень структурованості, безпеки та ефективності. Використання UML-схеми дозволило нам ретельно спланувати архітектуру системи, визначивши ключові компоненти та їх взаємодію. Кожен клас відіграє унікальну роль, що сприяє створенню цілісної та надійної системи.

1. Tanrıverdi M., Tekerek A. Implementation of Blockchain Based Distributed Web Attack Detection Application. Feminist Press at CUNY. 2021. 102 p.
2. Alghawazi M., Alghazzawi D., Alarifi S., Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal Cybersecurity and Privacy*, 2022, 2(4), pp. 764-777.