УДК 004.056

БЕЗПЕКА БАЗИ ДАНИХ У ВИСОКО РЕГУЛЬОВАНИХ ГАЛУЗЯХ

Ніколаєв А.О., Кривенко С.А.
e-mail: andrii.nikolaiev@nure.ua, e-mail: stanislav.kryvenko@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

The document discusses the importance of database security in highly regulated industries, particularly focusing on the use of Amazon RDS and various methods to enhance data protection. Users must evaluate data confidentiality and ownership standards in compliance with current laws, especially in healthcare and finance sectors. Cloud technologies like AMAZON RDS provide new research opportunities. Amazon RDS is suitable for OLTP, efficiently handling large volumes of transaction data, such as banking transactions, by securely storing and updating transaction details. A variety of methods are recommended to manage access and enhance security for Amazon RDS, including using virtual private clouds, SSL/TLS connections, encryption, and database security features.

Користувачі баз даних повинні оцінювати стандарти [1] з точки зору конфіденційності даних і власності на дані в контексті оцінки та використання стандартів відповідно до чинного законодавства та нормативних актів. В першу чергу це стосується охорони здоров’я та фінансів. Застосування хмарних технологій штучного інтелекту, наприклад AMAZON SAGEMAKER дозволяє відкрити новий горизонт досліджень [2].

Метою роботи є дослідження засобів покращення безпеки бази даних у високо регульованих галузях

Amazon RDS підходить для транзакцій OLTP (OnLine Transaction Processing). Протокол OLTP надійно та ефективно зберігає та оновлює дані транзакцій у великих обсягах. Одним із варіантів використання Amazon RDS є транзакційні таблиці даних, наприклад, банківські транзакції (рис. 1).

Рис. 1. Приклад використання Amazon RDS: банківські операції

Коли клієнт банку робить депозит або знімає кошти, він отримує доступ до банківської бази даних Aurora, яка розміщена в екземплярах

банківської програми EC2. У таблиці є рядки поточного рахунку клієнта банку. Кожна транзакція має унікальний ідентифікатор. Такі дані, як дата транзакції, опис, тип і сума, записуються для кожної транзакції.

Можна керувати доступом до ресурсів Amazon RDS і баз даних на екземплярі бази даних. Метод, який використовується для керування доступом, залежить від типу завдання, яке користувач має виконати за допомогою Amazon RDS. Нижче наведено рекомендовані методи безпеки.

Метод 1. Запускати екземпляр бази даних у спеціальній та приватній хмарі на основі служби Amazon VPC для максимально можливого контролю доступу до мережі.

Метод 2. Використовувати політики AWS IAM, щоб призначити дозволи, які визначають, кому дозволено керувати ресурсами Amazon RDS.

Метод 3. Використовувати групи безпеки, щоб контролювати, які IP-адреси або екземпляри EC2 можуть підключатися до цільових баз даних на DBinstance. Коли вперше створюється DBinstance, його брандмауер запобігає будь-якому доступу до бази даних, окрім правил, визначених пов'язаною групою безпеки.

Метод 4. Використовувати з'єднання SSL або TLS з екземплярами DB, на яких запущено механізми баз даних MySQL, MariaDB, PostgreSQL, Oracle або Microsoft SQL Server.

Метод 5. Використовувати шифрування Amazon RDS, щоб захистити цільові екземпляри бази даних і знімки в стані спокою. Шифрування Amazon RDS використовує галузевий стандартний алгоритм шифрування AES-256 для шифрування даних на сервері, на якому розміщено DBinstance. Для екземпляра зашифрованої бази даних Amazon RDS усі журнали, резервні копії та знімки зашифровано. Amazon RDS використовує ключ AWS KMS для шифрування цих ресурсів.

Метод 6. Використовувати функції безпеки цільової бази даних, щоб контролювати, хто може входити в бази даних в екземплярі бази даних. Ці функції працюють так, ніби база даних знаходиться у приватній локальній мережі.

Список використаних джерел:

1. Kryvenko, S. et al. IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security // *IEEE Std 2933-2024/UL 2933:2024*.2024. P. 1–274. doi: 10.1109/IEEESTD.2024.10697446.

2. Кирсанов О. О., Кривенко С. А. Конструювання ознак для застосування навчання машин при обробці клінічних даних // Infocommunication Technologies and Electronic Engineering = Інфокомунікаційні технології та електронна інженерія. – 2024. – Vol. 4, № 2. – P. 162–171. doi.org/10.23939/ictee2024.02.162