0.1. *Яковлев Г.А., Тренькаев В.Н.* Платформа SecureDBMS для исследования защищенных облачных СУБД

Применение мощных облачных вычислительных ресурсов, а также производительных хранилищ данных и их высокая доступность для бизнеса привела к росту популярности таких решений. Пока процессы обработки и хранения данных переносятся «в облако», требуется обеспечить достаточный уровень безопасности, в частности, конфиденциальности передаваемых, хранимых и обрабатываемых данных.

Часто в таких системах используются развернутые «в облаке» системы управления базами данных (СУБД). Современные решения в большинстве своем обеспечивают защиту данных при передаче, а также хранении. Объектами множества исследований являются алгоритмы защиты данных, на их основе были построены некоторые исследовательские проекты, например, CryptDB [1] и ZeroDB [2], реализующие СУБД с применением таких алгоритмов для шифрования данных.

В результате проведенного авторами анализа литературы и существующих решений была предложена архитектура платформы для разработки и исследования защищенных облачных СУБД. Авторами была разработана концепция программной платформы SecureDBMS, которая обобщает наработки других исследователей. Данная платформа позволяет построить защищенную облачную СУБД на базе целевого сервера базы данных (в данном случае MySQL), сделать оценку производительности разработанной СУБД, а также провести практические исследования по анализу безопасности используемых алгоритмов и протоколов защиты. Исключается использование нестандартных клиентских библиотек и модификация сервера базы данных.

Единая универсальная архитектура позволяет моделировать различные варианты облачных СУБД. Важными особенностями платформы являются: использование компонентов с открытым исходным кодом и предоставление интерфейсов для подключения пользовательских модулей, реализующих основной функционал – шифрование данных или управление ключами. Это позволит развивать проект с возможностями развития в будущем, с упором на исследование в рамках облачных СУБД алгоритмов защиты данных (реализация алгоритмов из СУБД Arx [4] для которой исходные коды не доступны), кроме того позволит проводить сравнение с уже известными алгоритмами, которые представлены в виде программных библиотек или в составе существующих решений (например, алгоритм шифрования OPE [5]).

Список литературы:

1. Popa R.A. CryptDB: Protecting confidentiality with encrypted query processing. / R.A. Popa, C. Redfield, N. Zeldovich, H. Balakrishnan // SOSP'11 - Proceedings of the 23rd ACM Symposium on Operating Systems Principles. – 2011. – P. 85-100. – DOI: 10.1145/2043556.2043566.

2. Egorov M. ZeroDB white paper / M. Egorov, M. Wilkison // Cryptography and Security (cs.CR). arXiv, – 2016. – DOI: 10.48550/arXiv.1602.07168

3. Яковлев Г.А., Тренькаев В.Н Анализ архитектур защищенных СУБД с недоверенным сервером // Материалы X Международной молодежной научной конференции «Математическое и программное обеспечение информационных, технических и экономических систем» Т. 337, С. 147-151 Томск, 2022 – DOI: 10.17223/978-5-907572-27-0-2022-22

4. Poddar R. Arx: an encrypted database using semantically secure encryption. / R. Poddar, T. Boelter, R. A. Popa. // Proceedings of the VLDB Endowment. – 2019. – Vol. 12 – P. 1664–1678. – DOI: 10.14778/3342263.3342641.

5. Boldyreva A. Order-Preserving Symmetric Encryption / A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill // EUROCRYPT 2009, LNCS 5479. – 2009. – P. 224–241. – DOI: 10.1007/978-3-642-01001-9_13