0.1. *Яковлев Г.А.* Алгоритмы защиты данных в облачной СУБД

В работе представлены результаты анализа алгоритмов обеспечения безопасности в облачной СУБД в недоверенной среде, лежащие в основе решений ZeroDB [1], CryptDB [2], Arx с использованием разного рода криптографических алгоритмов PHE, FHE (гомоморфное шифрование), OPE (сохраняющие порядок шифрование). Приведено сравнение и описание особенностей алгоритмов для линейного поиска, поиска со сравнением, вычисления функций агрегирования и объединения запросов. Выявлены следующие проблемы: 1) детерминированное шифрование (DE) сохраняет частоты открытых текстов в шифротекстах (что позволяет проводить частотный анализ); 2) схема OPE является детерминированной, и в случае если данные открытого текста плотные (встречается каждый возможный открытый текст), тогда злоумышленник с моментальным снимком (копия диска с БД) может узнать соответствующие открытые тексты (т.е. просто упорядочить шифротексты и получить открытые тексты); 3) при использовании OPE происходит утечка информации об открытом тексте, поэтому следует изучить последствия для конфиденциальности; 4) для вычислений над данными безопасность зависит от выбранной схемы гомоморфного шифрования и предоставленных гарантий безопасности (например безопасность аналогично симметричному шифрованию со 128-битным ключом); 5) схемы шифрования с возможностью поиска (SSE) раскрывают количество ключевых слов и могут раскрывать количество повторений каждого ключевого слова (в некоторых конфигурациях). Приведены результаты сравнения алгоритмов по уровню безопасности, используемых в современных защищенных СУБД, представлены известные алгоритмы защиты данных и описаны потенциальные проблемы предлагаемых архитектур и алгоритмов для реализации в защищенных СУБД. Результаты работы будут полезны при анализе безопасности СУБД, оценке возможных потерь производительности, а также могут быть использованы с целью определения наиболее подходящих алгоритмов защиты данных для реализации в собственной защищенной СУБД.

ЛИТЕРАТУРА

1. M. Egorov, M. Wilkison “ZeroDB white paper” // Cryptography and Security (cs.CR). arXiv, 2016. 2. Vimercati Sabrina, Foresti Sara, Livraga Giovanni, Samarati Pierangela // Practical Techniques Building on Encryption for Protecting and Managing Data in the Cloud, 2016. 3. Poddar Rishabh, Boelter Tobias, Popa Raluca. Arx: an encrypted database using semantically secure encryption. Proceedings of the VLDB Endowment. 12, pp. 1664-1678, 2019.