



НАУЧНЫЙ ЖУРНАЛ НАУКА И МИРОВОЗЗРЕНИЕ

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Куропятникова Алёна Юрьевна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

Дацева Элизабет Галибовна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

Аннотация. Защита информации в облачных вычислениях активно исследуется мировым научным сообществом. Эти исследования показали, что обозначенная проблема намного сложнее тех задач защиты информации, которые решаются известными криптографическими средствами. В данной статье рассматриваются варианты решения проблемы обеспечения безопасности и конфиденциальности облачных данных.

Ключевые слова: защита информации, облачные вычисления, вычисления над зашифрованными данными, гомоморфные вычисления.

Облачные вычисления открывают новый способ предоставления услуг, переупорядочивая различные ресурсы и предоставляя их пользователям в соответствии с их требованиями. Они также играют важную роль в мобильных сетях и услугах следующего поколения (5G), а также в киберфизических и социальных вычислениях (CPSC). Хранение данных в облаке значительно снижает нагрузку на пользователей и обеспечивает им удобный доступ к данным в любом месте и в любое время. Поэтому эта технология стала одним из самых важных облачных сервисом.

Однако безопасность и конфиденциальность облачных данных становятся критически важной проблемой, которая влияет на успех облачных вычислений и становится препятствием развитию 5G и CPSC. Во-первых, хранение данных в облаке увеличивает риск утечки данных и несанкционированного доступа. Во-вторых, облачные центры обработки данных становятся объектами атак и вторжений, что ставит под угрозу безопасность облачных данных. В-третьих, операциям управления данными, таким как хранение данных, резервное копирование, миграция, удаление, обновление, поиск, запросы и доступ в облаке, могут не полностью доверять их владельцы. Владелец данных необходимо проверять надежность управления данными. Любые источники вторжений и атак должны быть обнаружены и отслежены. Вышеупомянутые требования на самом деле создают серьезную проблему безопасности, особенно при хранении и управлении большими данными. В-четвертых, обработка данных и вычисления в облаке могут раскрыть конфиденциальность владельцев данных или связанных организаций несанкционированным лицам.

Безопасность и конфиденциальность облачных данных действительно становятся ключевыми проблемами, влияющими на успех облачных вычислений.

Криптография широко применяется для обеспечения безопасности данных, конфиденциальности и надежности облачным вычислениям. Но существующие решения по-прежнему несовершенны и неэффективны, а значит, непрактичны. Хранение зашифрованных данных в облаке затрудняет выполнение аудита управления данными, хотя риск утечки конфиденциальности значительно снижается. Шифрование требует дополнительных затрат на вычисления и связь. Кроме того, такие операции, как слияние, агрегирование и интеллектуальный анализ зашифрованных данных, по-прежнему нецелесообразно развертывать из-за высокой сложности вычислений и неэффективности. Криптография в облачных вычислениях обещает множество новых решений, и в то же время многие проблемы еще предстоит решить.

В этой работе собрано 4 статьи, посвящённые оригинальным неопубликованным исследованиям, представляющих тему «Криптография и безопасность данных в облачных вычислениях». Классифицируем их по четырем категориям и кратко представим их ниже.

1. Безопасное облачное хранилище данных

В статье «Supporting Dynamic Updates in Storage Clouds with the Akl-Taylor Scheme» Кастильоне и др. пытался преодолеть проблему применимости схем иерархического назначения ключей для управления криптографическим доступом. После тщательного анализа проблемы поддержки динамических обновлений и операций замены ключей с учетом различных стратегий назначения ключей. Они предоставили новые результаты по схеме Акла Тейлора и доказательство того, что предложенные схемы безопасны в отношении понятия восстановления ключа.

2. Защита конфиденциальности данных в облаке

Чтобы сохранить конфиденциальность опубликованных данных и интересы подписчиков в услугах публикации и подписки данных через облако, Ян и др. предложили схему Публикации Подписки (AKPS) с сохранением конфиденциальности данных на основе атрибутов и ключевых слов в статье «Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms». Они использовали шифрование на основе атрибутов с аутсорсингом дешифрования для шифрования опубликованных данных и предложили новое с возможностью поиска, которое позволяет подписчикам выборочно получать интересующие данные. AKPS является оригинальным и отличается от существующих методов, потому что он может поддерживать нескольких издателей и нескольких подписчиков, в то время как ни один из двух издателей / подписчиков не имеет одинаковых секретных ключей. Более того, он умело связывает политику доступа и политику подписки двумя секретными ключами, что позволяет избежать обхода процедуры проверки политики доступа / подписки.

3. Надежное управление облачными данными

Статья «Tell me the Truth: Practically Public Authentication for Outsourced Databases with Multi User Modification» направлена на решение проблемы проверки целостности аутсорсинговой базы данных с многопользовательской модификацией и повышенной эффективностью. Авторы предложили новую схему подписи, которая позволяет пользователям подписывать измененные данные независимо и гомоморфно проверяемая.

4. Криптография, связанная с безопасностью облачных данных

Как один из самых популярных криптографических алгоритмов с открытым ключом, алгоритм RSA широко используется для защиты облачных вычислений. Безопасность RSA заключается в сложности эффективного разложения больших целых чисел. Алгоритм «General Number Field Sieve» (GNFS) является наиболее эффективным алгоритмом факторизации целых чисел, длина которых превышает 110 цифр. В статье «Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing» исследуется алгоритм GNFS в облаке. Он предлагает новый параллельный блочный алгоритм Видемана для повышения производительности выполнения и снижения коммуникационных затрат при решении больших и разреженных линейных систем через GF, что является одним из наиболее трудоемких этапов алгоритма GNFS.