УДК: 004.056.55

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Легков Н.С

Федеральное государственное бюджетное образовательное учреждение высшего образования «Брянский государственный университет имени академика И.Г. Петровского», Россия, Брянск, e-mail: legkovnickitka@yandex.ru

Исследования в области конфиденциальности вычислений показали, что решение данной проблемы сложнее задач, которые решаются распространёнными криптографическими средствами. Статья предусматривает варианты решения проблемы безопасности и конфиденциальности данных в облаке.

Ключевые слова: защита информации, облачные вычисления, криптография, инновации.

CRYPTOGRAPHY AND DATA SECURITY IN CLOUD COMPUTING

Legkov N.S.

Federal State Budgetary Educational Institution of Higher Education "Bryansk State University named after Academician I.G. Petrovsky", Russia, Bryansk, e-mail: legkovnickitka@yandex.ru

Research in the field of computing privacy has shown that solving this problem is more difficult than tasks that are solved by common cryptographic means. The article provides options for solving the problem of data security and confidentiality in the cloud.

Keywords: information security, cloud computing, cryptography, innovation.

Облачные вычисления получили значительное развитие в последние годы. Действительно, эта технология очень удобна для пользователей, она предоставляет доступ к пользовательским данным в любое время в любом месте. С другой стороны, как правило, облачные ресурсы в значительной мере превосходят ресурсы, которыми обладают обычные пользователи, поэтому могут решать некоторые сложные задачи за более короткое время.

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 потери данных и несанкционированного доступа.

Во-вторых, облачные центры обработки данных уязвимы для атак, что ставит под угрозу безопасность данных в облаке.

В-третьих, их владельцы не могут полностью доверять операциям управления данными.

В-четвертых, обработка данных и облачные вычисления раскрывают конфиденциальность владельцев данных.

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

В 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.

Безопасное облачное хранилище

В статье «Поддержка динамических обновлений в облачных хранилищах» Кастильоне и др. попытались решить проблему применимости иерархических схем назначения ключей для управления доступом. После анализа проблемы динамических обновлений и операции замены ключей с учетом, они предоставили новые результаты по схеме Акла-Тейлора и доказали, что предложенные схемы безопасны в отношении понятия восстановления ключа.

Конфиденциальность в облаке

Для защиты опубликованных данных и интересов подписчиков на услуги публикации данных Ян и др. предложили схему подписки на публикацию (AKPS) с конфиденциальностью данных на основе атрибутов и ключевых слов в статье "Сервис публикации-подписки на основе атрибутов и ключевых слов, сохраняющий конфиденциальность". На облачных платформах". Они использовали шифрование на основе атрибутов для шифрования опубликованных данных и предложили новый вариант с возможностью поиска, который позволяет подписчикам выборочно извлекать нужные данные. AK PS может обрабатывать несколько издателей и подписчиков, и у них не должно быть одинаковых зашифрованных ключей.

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 базы данных с многопользовательскими изменениями и большей эффективностью. Авторы предложили новую схему подписи, которая позволяет пользователям самостоятельно подписывать измененные данные.

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 эффективным алгоритмом факторизации целых чисел, длина которых более 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.

И так, в научной работе по указанной тематике были рассмотрены и проанализированы варианты решения проблемы безопасности и конфиденциальности облачных данных, была аргументирована важность защиты данных.

В заключение, хочется сказать, что безопасность не всегда обеспечивается только защитой. Она может быть достигнута также соответствующими правилами поведения и взаимодействия объектов, высокой профессиональной подготовкой персонала, безотказностью работы техники, надёжностью всех видов обеспечения функционирования объектов информационной безопасности.

Список литературы

1. Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, Xinyi Huang, Aniello Castiglione. Supporting Dynamic Updates in Storage Clouds with the Akl-Taylor Scheme. Information Sciences, 2017, volume 387, pp. 56-74.

2. Kan Yang, Kuan Zhang, Xiaohua Jia, M. Anwar Hasan, Xuemin (Sherman)Shen. Privacy-Preserving Attribute-Keyword Based Data Publish-Subscribe Service on Cloud Platforms. Information Sciences, 2017, volume 387, pp. 116-131.

3. Wei Song, Bing Wang, Qian Wang, Zhiyong Peng, Wenjing Lou. Tell me the Truth: Practically Public Authentication for Outsourced Databases with Multi-User Modification. Information Sciences, 2017, volume 387, pp. 221-237.

4. Laurence T. Yang, Gaoyuan Huang, Jun Feng, Li Xu. Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing. Information Sciences, 2017, volume 387, pp. 254-265.

5. Куропятникова А.Ю., Дацева Э.Г. КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ // Молодежный научный форум: электр. сб. ст. по мат. CLIII междунар. студ. науч.-практ. конф. № 2(153): [Электронный ресурс]. URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/2(153).pdf. / Текст : непосредственный (дата обращения: 07.02.2022).

6. Котяшичев, И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова. — Текст : непосредственный // Молодой ученый. — 2015. — № 6.4 (86.4). — С. 30-34. — URL: https://moluch.ru/archive/86/16357/ (дата обращения: 24.02.2022).