УДК 004

ХРАНЕНИЕ БОЛЬШИХ ДАННЫХ В ОБЛАКЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАЗДЕЛЕНИЯ СЕКРЕТА

Улюкова Гулден Бектемировна, Ергалиева Бану Бакытжановна, Жетписбаева Айнур Турсынкановна
u.g.b@bk.ru
Научные сотрудники НИИ информационной безопасности и криптологии
ЕНУ им. Л.Н.Гумилева

Данная статья посвящена исследованию метода хранения данных в облачных хранилищах с использованием технологии разделения секрета. Такие проблемы особенно актуальны в условиях стремительного развития Интернета Вещей (IoT). Чипы, смарт-карты и прочие физически маленькие устройства, как правило, имеют значительные ограничения памяти, поэтому возникает необходимость использования облачных хранилищ как вспомогательных инструмент для безопасного хранения данных. Идея нового подхода заключается в разработке метода хранения больших данных с использованием различных криптографических решений, такие как метод разделения секрета Шамира, протокол распределения ключей Диффи-Хеллмана и т.д. Отметим, что различными исследователями [1-10] были предложены методы хранения и безопасной обработки данных в облаке.

В рамках этой работы мы предположим, что клиент i желает хранить свои данные (файлы, рисунки, фотографии и т.д.) в аутсорсинге, то есть в облачном хранилище. При этом сами данные не являются секретами от сервера, поэтому для обмена информацией между

клиентами и сервером могут быть использованы стандартные протокола безопасного обмена информацией. Проблема заключается в том, что облачное хранилище (сервер) не является доверенным в том смысле, что возможны вмешательства злоумышленников на стороне сервера, такие как подмена информации, искажение содержания данных и т.д. Кроме того, предположим, что сам сервер в момент передачи и обмена информацией с клиентами не нарушает протокол взаимодействия и не происходит утечка информации. Но хранение самих данных в облаке может быть небезопасным, поэтому исходные данные, после передачи в сервер, необходимо держать в зашифрованном виде с использованием стандартных симметричных алгоритмов шифрования, например ГОСТ, AES и т.д.. Таким образом, для каждого клиента и сервера стоит задача выработки общего секретного ключа, который будет использоваться сервером как ключ шифрования данных. В такой модели, сервер заинтересован «забыть» этот общий ключ, но иметь возможность восстановить этот ключ для дешифрования данных только с участием того клиента, кому эти данные принадлежат.

Итак, пусть клиенту i необходимо отправить в облако большие данные для хранения в зашифрованном виде.

Шаг 1. Пусть выбрана общая эллиптическая кривая

$$E_p(a,b)\colon y^2 = x^3 + ax + b \bmod p,\ \ (4a^3 + 27b^2) \bmod p \neq 0,$$

и точка G на ней является генератором, то есть G, [2]G, [3]G,…,[q]G суть различные точки и [q]G=O для некоторого простого числа q.

Клиент i выбирает случайное число $r_i,\ 0 < r_i < q$, которое хранит как свой секретный ключ и вычисляет точку на кривой $R_i = [r_i]G$, которая будет его открытым ключом. Аналогично, сервер случайным образом генерирует число $d_s, 0 < d_s < q$, которое хранит как свой секретный ключ и вычисляет точку на кривой $D_s = [d_s]G$. Открытыми и общедоступными данными также являются следующие параметры: p, a, b, G, q.

Шаг 2. Распределение ключей осуществим с использованием хорошо известного протокола Диффи-Хеллмана на эллиптической кривой:

- Клиент i вычисляет и отправляет серверу свой открытый ключ $R_i = [r_i]G$, а сервер отправляет клиенту свой открытый ключ $D_s = [d_s]G$;

- Сервер вычисляет точку $Q_i = d_s R_i$, а клиент аналогично вычисляет ту же точку $Q_i = r_i D_s$, так как $d_s R_i = d_s r_i G = r_i D_s$;

- В качестве распределённого ключа k_i возьмем первую координату x точки $Q_i(x, y)$. То есть мы имеем общий секретный ключ между клиентом i и сервером: $k_i = x$.

- Сервер шифрует исходные данные клиента i, используя общий секретный ключ k_i, и хранит данные в зашифрованном виде.

- Теперь сервер и клиент i удаляют из своих хранилищ d_s и r_i соответственно, то есть «забывают» их.

Шаг 3. Используем технологию разделения секрета Шамира:

- Обозначим через a значение первой координаты суммы двух точек на эллиптической кривой $Q_i + R_i$;

- Сервер и клиент самостоятельно формируют один и тот же полином

$$f(x) = k_i + ax$$

- Сервер и клиент случайным образом разделяют общий секретный ключ k_i на два ключа с использованием технологии разделения секрета Шамира. Обозначим их $ServerKey(i) = \big(x_1, f(x_1)\big)$ и $ClientKey(i) = \big(x_2, f(x_2)\big)$;

- Теперь сервер и клиент удаляют из своих хранилищ, то есть «забывают», точку Q_i и полином со всеми параметрами $f(x) = k_i + ax$.

Шаг 4. Сервер формирует клиентскую базу, то есть для каждого клиента i будет храниться только следующая информация (профайл -го клиента):

ID клиента	h(k_i)	*ServerKey(i)*	R_i

Здесь h(k_i) – значение криптографической хеш-функции от распределенного общего ключа k_i между клиентом i и сервером. Хранение хеш-функции необходимо для аутентификации клиента. Заметим, что эти данные достаточны для того, чтобы сервер мог восстановить общий секретный ключ k_i для дешифрования данных и дальнейшей передачи исходных данных клиенту.

Информация об поддержки. Данная работа выполнена при финансовой поддержке грантового финансирования МЦРИАП, № AP06850817.

Список использованных источников

1. Seitkulov Ye. New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, Springer US, Print ISSN 0920-8542, Volume 65, Issue 1, 2013, pp 469-482.
2. Jianhua Yu, Xueli Wang, Wei Gao Improvement and applications of secure outsourcing of scientific computations // Journal of Ambient Intelligence and Humanized Computing, December 2015, Volume 6, Issue 6, pp. 763–772.
3. Xing Hu, Chunming Tang Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix // Journal of Cloud Computing, Springer Berlin Heidelberg, 4:7 DOI 10.1186/s13677-015-0033-9, 2015, ISSN 2192-113X, online https://eprint.iacr.org/2014/442.pdf
4. Cong Wang, Kui Ren, Jia Wang Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming // IEEE Transactions on Computers, Volume: 65, Issue 1, Jan. 1 2016, pp. 216 – 229.
5. Vyas R., Singh A., Singh J., Soni G., Purushothama B.R.: Design of an efficient verification scheme for correctness of outsourced computations in cloud computing // Security in Computing and Communications, Springer, 2015, vol. 536, pp. 66–77.
6. Atallah M., Frikken K. Securely outsourcing linear algebra computations // In: Proceedings of ASIACCS. New York, 2010, pp 48–59.
7. Benjamin D., Atallah M. Private and cheating-free outsourcing of algebraic computations // Proceedings of 6th conference on privacy, security, and trust (PST), 2008, pp 240–245.
8. Tsutomu Matsumoto, Koki Kato, Hideki Imai Speeding Up Secret Computations with Insecure Auxiliary Devices // CRYPTO 1988: Advances in Cryptology — CRYPTO' 88, pp. 497-506.
9. Thierry Mefenza, Damien Vergnaud Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting // Published 2018 online: https://www.di.ens.fr/~mefenza/Cryptanalysis%20of%20Server-Aided%20RSA.pdf
10. Kai Zhou, M. H. Afifi, Jian Ren ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing // IEEE Transactions on Information Forensics and Security, Volume 12 , Issue 11, Nov. 2017, pp. 2518 – 2531.