УДК 004.9
https://doi.org/10.47533/2020.1606-146X.159

Е. Н. СЕЙТКУЛОВ*, Б. Б. ЕРГАЛИЕВА, Д. Ж. САТЫБАЛДИНА

Евразийский национальный университет им. Л.Н.Гумилева,
Нур-Султан, Казахстан

ПРОТОКОЛЫ БЕЗОПАСНОГО АУТСОРСИНГА ХРАНЕНИЯ ДАННЫХ В ОБЛАКЕ И АНАЛИЗ ИХ СТОЙКОСТИ К АКТИВНЫМ И ПАССИВНЫМ АТАКАМ

В работе изучаются новые подходы по разработке методов хранения больших данных с использованием различных криптографических решений, таких как метод разделения секрета Шамира, протокол распределения ключей Диффи-Хеллмана и т.д. Отметим, что различными исследователями были предложены различные методы хранения данных в облаке. В данной работе мы исследуем методы и протоколы безопасного аутсорсинга для хранения больших данных с использованием технологии разделения секрета и анализу их стойкости к активным и пассивным атакам. 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 вспомогательный инструмент для безопасного хранения данных.

Ключевые слова*: криптография, информационная безопасность, облачное хранение данных, клиент-серверное взаимодействие, Интернет вещей.*

Введение. Данная работа посвящена исследованию и разработкам методов безопасного аутсорсинга для хранения больших данных с использованием технологии разделения секрета и анализа их стойкости к активным и пассивным атакам. 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 вспомогательный инструмент для безопасного хранения данных.

В работе изучаются новые подходы по разработке методов 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 [1-14] были предложены методы хранения данных в облаке.

Постановка задачи. Предположим, что клиент i желает хранить свои данные (файлы, рисунки, фотографии и т.д.) в аутсорсинге, то есть в облачном хранилище. Для обмена информацией между клиентом и сервером могут быть использованы стандартные протоколы безопасного обмена информацией. Проблема заключается в том, что облачное хранилище (сервер) не является доверенным в том смысле, что в период хранения полученных данных возможны вмешательства злоумышленников. Однако сам сервер, который рассматривается как автоматизированная система, не отклоняется от протокола взаимодействия. То есть сервер со своей стороны желает протокольно

* E-mail корреспондирующего автора: yerzhan.seitkulov@gmail.com

защититься от таких несанкционированных вмешательств, как подмена информации, искажение содержания данных и т.д., именно в период хранения данных. Таким образом, данные, передаваемые серверу, не являются секретными, но сервер желает избежать искажения и подмены информации злоумышленниками, и поэтому выполняет все действия, описанные в протоколах обмена информацией и хранения данных.

Итак, предположим, что сам сервер в момент передачи и обмена информацией с клиентами не нарушает протокол взаимодействия и не происходит утечка информации. Но долгосрочное 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 конкретного клиента. В такой модели сервер протокольно заинтересован «забыть» этот общий ключ, но иметь возможность восстановить этот ключ для дешифрования данных только с участием того клиента, кому эти данные принадлежат [15].

Далее, под активной атакой называется случай, когда имеет место преднамеренное вмешательство третьих лиц или злоумышленников в клиент-серверное взаимодействие с целью подмены информации. А пассивная атака – это случай, когда сервер может непреднамеренно отправлять клиенту неверную информацию. Такие случаи возникают, когда происходят сбои на каналах связи.

Метод хранения данных в облаке с использованием классической асимметричной криптографии. Итак, пусть клиенту *i* необходимо отправить в облако большие данные для хранения в зашифрованном виде. Опишем процедуру аутсорсинга хранения данных в облаке следующим протоколом клиент-серверного взаимодействия.

Шаг 1. Клиент i и сервер выбирают достаточно большое простое число p и число d. Клиент i и сервер, независимо друг от друга, выбирают случайные натуральные числа a и b соответственно.

Далее, клиент i вычисляет число A_i:

$$A_i = d^a \bmod p;$$

а сервер находит число B:

$$B = d^b \bmod p.$$

Здесь число a является секретным ключом клиента i; b является секретным ключом сервера. А числа A_i и *B* являются открытыми ключами клиента и сервера соответственно.

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

– Клиент i вычисляет и отправляет серверу свой открытый ключ

$$A_i = d^a \bmod p,$$

а сервер отправляет клиенту свой открытый ключ

$$B = d^b \bmod p.$$

– Сервер вычисляет число

$$Q_i = A_i^b \text{ mop } d,$$

а клиент аналогично вычисляет то же число

$$Q_i = B^a \bmod p,$$

так как

$$B^a \bmod p = d^{ab} \bmod p = A_i^b \text{ mop } d;$$

– В качестве распределённого ключа k_i возьмем число Q_i. То есть мы имеем общий секретный ключ между конкретным клиентом i и сервером: k_i.

– Сервер шифрует (например, AES или ГОСТ) исходные данные клиента i, используя общий секретный ключ k_i, и хранит зашифрованные данные у себя в хранилище. Эти зашифрованные данные обозначим F(i).

- Теперь клиент i и сервер удаляют из своих хранилищ числа a и b соответственно, то есть «забывают» их. Данное протокольное соглашение «забыть» свои секретные ключи является обязательным и выполняется в автоматизированном режиме и на стороне клиента, и на стороне сервера.

Шаг 3. Используем технологию разделения секрета Шамира:

– Обозначим через l значение произведения двух чисел:

$$l = Q_i A_i \bmod p;$$

– Сервер и клиент самостоятельно формируют один и тот же полином

$$f(x) = k_i + lx \bmod p$$

– Сервер и клиент случайным образом разделяют общий секретный ключ k_i на два ключа с использованием технологии разделения секрета Шамира. Обозначим их

$$SKey(i) = (x_1, f(x_l)) \text{ и } CKey(i) = (x_2, f(x_2)).$$

И сервер, и клиент хранят эти разделенные секреты каждый у себя и держат в секрете.

– Теперь сервер и клиент удаляют из своих хранилищ числа k_i и l из полинома

$$f(x) = k_i + lx,$$

то есть «забывают» эти параметры согласно протоколу. Перед удалением ключа k_i сервер вычисляет значение хеш-функции $h(k_i)$ и это значение отправляется в хранилище сервера.

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

– ID клиента;

– $h(k_i)$ (значение хеш-функции от ключа k_i);

– SKey(i) (разделенный секрет сервера);

– A_i (открытый ключ клиента);

– F(i) (зашифрованные данные клиента i).

Здесь $h(k_i)$ – значение криптографической хеш-функции (например, SHA-3) от распределенного общего ключа k_i между клиентом i и сервером. Хранение хеш-функции необходимо для аутентификации клиента.

Заметим, что информации в клиентской базе сервера достаточны для того, чтобы сервер мог восстановить общий секретный ключ k_i, который затем будет использован для дешифрования данных и дальнейшей передачи дешифрованных данных обратно клиенту.

Метод хранения данных с использованием криптографии на эллиптической кривой. Теперь мы покажем аналог описанного выше метода хранение данных, но с использованием криптограммы на эллиптической кривой. Итак, пусть клиенту i необходимо отправить в облако большие данные для хранения в зашифрованном виде.

Шаг 1. Пусть выбрана общая эллиптическая кривая

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

и точка G на ней является генератором, то есть G, [2]G, [3]G, ..., [q]G суть различные точки и [q]G = 0 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

$$d_sR_i = d_sr_iG = r_iD_s;$$

– В качестве распределённого ключа k_i возьмем первую координату x_1 точки $Q_i(x_1, y_1)$. То есть мы имеем общий секретный ключ между клиентом i и сервером: $k_i = x_1$.

– Сервер шифрует исходные данные клиента i, используя общий секретный ключ k_i, и хранит данные в зашифрованном виде у себя в хранилище. Эти зашифрованные данные обозначим F(i).

– Теперь сервер и клиент i удаляют секретные ключи d_s и r_i соответственно, то есть «забывают» их.

Шаг 3. Используем технологию разделения секрета Шамира:

– Обозначим через x_2 значение первой координаты суммы двух точек на эллиптической кривой

$$Q_i + R_i = L;$$

– Сервер и клиент теперь самостоятельно формируют один и тот же полином

$$f(z) = k_i + x_2 z \bmod q$$

– Сервер и клиент случайным образом разделяют общий секретный ключ k_i на два ключа с использованием технологии разделения секрета Шамира. Обозначим их

$$SKey(i) = (z_1, f(z_1)) \text{ и } CKey(i) = (z_2, f(z_2)).$$

И сервер, и клиент хранят эти разделенные секреты каждый у себя и держат в секрете.

– Теперь сервер и клиент удаляют из своих хранилищ точки Q_i и L, а также удаляют числа k_i и x_2 из полинома

$$f(z) = k_i + x_2 z,$$

то есть «забывают» эти точки и числа. Перед удалением ключа k_i сервер вычисляет значение хеш-функции $h(k_i)$ и это значение отправляется в хранилище сервера.

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

– ID клиента;

– $h(k_i)$ (значение хеш-функции от ключа k_i);

– SKey(i) (разделенный секрет сервера);

– R_i (открытый ключ клиента);

– F(i) (зашифрованные данные клиента i).

Здесь $h(k_i)$ – значение криптографической хеш-функции (например, SHA-3) от распределенного общего ключа k_i между клиентом i и сервером. Хранение хеш-функции необходимо для аутентификации клиента.

Как и в предыдущем случае, информации в клиентской базе сервера достаточны для того, чтобы сервер мог восстановить общий секретный ключ k_i, который затем будет использован для дешифрования данных и дальнейшей передачи дешифрованных данных обратно клиенту.

Анализ стойкости к активным и пассивным атакам. В представленных двух протоколах клиент-серверного взаимодействия для хранения данных в облаке использованы классические криптографические алгоритмы. Но стойкость протоколов к активным и пассивным атакам зависит от других параметров. Итак, можно сразу исключить вопросы стойкости к пассивным атакам, так как согласно предложенной модели, сервер изначально не отклоняется от протокола взаимодействия, а верификация полученной информации от сервера обеспечивается надежными криптографическими алгоритмами, которые использованы в этих протоколах. Стойкость к активной атаке подразумевает, что при вмешательстве третьих лиц или злоумышленников в процесс

клиент-серверного взаимодействия клиент может проверить это путем верификации на своей стороне. Легко видеть, что при получении ложной информации, клиент сразу сможет это верифицировать, так как криптографические алгоритмы, использованные в этих протоколах, имеют некоторые свойства электронной цифровой подписи (RSA). Аналогичными свойствами обладает криптография на эллиптической кривой.

Заключение. В данной работе рассмотрен важный вопрос безопасного хранения данных в облаке с использованием технологии разделения секрета. В работе изучены новые подходы по разработке методов хранения больших данных с использованием различных криптографических решений, такие как метод разделения секрета Шамира, протокол распределения ключей Диффи-Хеллмана и т.д. А именно, мы исследовали методы и протоколы безопасного аутсорсинга для хранения больших данных с использованием технологии разделения секрета и анализу их стойкости к активным и пассивным атакам. 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 вспомогательный инструмент для безопасного хранения данных. В следующих работах нами будут предложены эффективные программные реализации представленных протоколов, а также экспериментальные расчеты.

Информация о финансировании. Работа выполнена при финансовой поддержке МЦРИАП РК, грант № AP06850817

ЛИТЕРАТУРА

1 Ю.Н. Сейткулов, Р.М. Оспанов, Б.Б. Ергалиева Об одном способе хранения информации в течение заданного времени. Вестник КАЗНИТУ, 143(3), 167-174. https://doi.org/10.51301/vest.su.2021.i3.22

2 Ержан Сейткулов, Гульден Улюкова, Бану Ергалиева, Айнур Жетписбаева Облачное хранилище больших данных с использованием технологии секретного обмена // 19-я Международная научная конференция «Информационные технологии и управление 2021» 22-23 апреля 2021 г., ISMA, Рига, Латвия, – с. 66-67.

3 Ержан Н. Сейткулов, Сейлхан Н. Боранбаев, Гульден Б. Улюкова, Бану Б. Ергалиева, Дина Сатыбалдина Методы безопасной облачной обработки больших данных // Индонезийский журнал электротехники и компьютерных наук, Том 22, № 3, июнь 2021 г., стр. 1650-1658, DOI: 10.11591/ijeecs.v22.i3.pp1650-1658.

4 Гульден Улюкова, Бану Ергалиева, Айнур Жетписбаева Облачное хранилище больших данных с использованием технологии секретного обмена // Материалы международной научной конференции студентов и молодых ученых «ФАРАБИ АЛЕМИ», Алматы, Казахстан, 6-8 апреля 2021 г., – С. 83.

5 М.О. Рабин, К. Торп. «Покадровая криптография», Технический отчет TR-22-06, Школа инженерных и компьютерных наук Гарвардского университета, 2006. - URL: https://www.eecs.harvard.edu /~cat/tlc.pdf

6 М.О. Рабин, К.А. Торп. «Способ и устройство для покадровой криптографии», Патент США 8 526 621, 2007. https://patents.google.com/patent/US8526621B2/e

7 Р. Доку, Д.Б. Рават и К. Лю. «О децентрализованном обмене данными на основе блокчейна для шифрования на основе событий для борьбы с атаками противника», IEEE

Transactions on Network Science and Engineering, Том 8, 2020, стр. 1033-1043. doi: 10.1109 / TNSE.2020.2987919.

8 Альварес Рамиро и Ноджумиан Мехрдад, “Всесторонний обзор протоколов сохранения конфиденциальности для аукционов с закрытыми ставками”, Компьютеры и безопасность. Том 88, 101502, 2020. https://www.sciencedirect.com/science/article/pii/S0167404818306631?via%3Dihub

9 С. Цзяцзюнь, Л. Нинчжун, «Стимулирование проверяемых механизмов защиты конфиденциальности для автономных приложений краудсенсинга», Sensors (Швейцария). 17 (9), 2017. doi: 10.3390/s17092024.

10 Н. Конг. «Применение экономических и ценовых моделей для обеспечения безопасности беспроводной сети: Обзор», IEEE Communications Surveys and Tutorials. Том 19, № 4, 2017, стр. 2735-2767, doi: 10.1109/COMST.2017.2732462.

11 Дж. Барон, К. Эль Дефрави, Дж. Лэмпкинс, Р. Островский. «Коммуникационно-оптимальный упреждающий обмен секретами для динамических групп, Криптология», Архив ePrint, Отчет 2015/304, 2015, https://eprint.iacr.org/2015/304

12 Дж. Брендель, Д. Демирель. «Эффективный упреждающий обмен секретами», Архив криптологии ePrint, Отчет 2017/719, 2017, https://eprint.iacr.org/2017/719 .

13 И. Ахмед. «Краткий обзор: проблемы безопасности в облачных вычислениях и их решения», Telkomnika, 17 (6), стр. 2812-2817, 2019, doi: 10.12928/TELKOMNIKA.v17i6.12490

14 С. Зайнельдин, А. Ате. «Улучшенная безопасность передачи облачных данных с использованием гибридного алгоритма шифрования», Индонезийский журнал электротехники и компьютерных наук, 20 (1), 2020, стр. 521-527.

15 Бану Б. Ергалиева, Ержан Н. Сейткулов, Дина Сатыбалдина, Руслан М. Оспанов, О некоторых методах хранения данных в облаке в течение заданного времени // TELKOMNIKA (Телекоммуникации, вычислительная техника, электроника и управление), Том 20, № 2, 2022, стр. 366-372. DOI: 10.12928/telkomnika.v20i2.21887

REFERENCES

1 Y.N. Seitkulov, R.M. Ospanov, B.B. Yergaliyeva On one method of storing information for a specified time. VESTNIK KAZNRTU, 143(3), 167–174. https://doi.org/10.51301/vest.su.2021.i3.22

2 Yerzhan Seitkulov, Gulden Ulyukova, Banu Yergaliyeva, Ainur Zhetpisbayeva Cloud storage of big data using secret sharing technology // The 19th International Scientific Conference Information Technologies and Management 2021 April 22-23, 2021, ISMA, Riga, Latvia, -pp. 66-67.

3 Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Gulden B. Ulyukova, Banu B. Yergaliyeva, Dina Satybaldina Methods for secure cloud processing of big data // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 3, June 2021, pp. 1650-1658, DOI: 10.11591/ijeecs.v22.i3.pp1650-1658.

4 Gulden Ulyukova, Banu Yergaliyeva, Ainur Zhetpisbayeva Cloud storage of big data using secret sharing technology // Materials of the international scientific conference of students and young scientists “FARABI ALEMI”, Almaty, Kazakhstan, April 6-8, 2021, - P. 83.

5 M.O. Rabin, C. Thorpe, “Time-lapse cryptography,” Technical report TR-22-06, Harvard University School of Engineering and Computer Science, 2006. - URL: https://www.eecs.harvard.edu/~cat/tlc.pdf

6 M.O. Rabin, C.A. Thorpe, “Method and apparatus for time-lapse cryptography,” U.S. Patent 8,526,621, 2007. https://patents.google.com/patent/US8526621B2/e

7 R. Doku, D.B. Rawat and C. Liu, “On the Blockchain-Based Decentralized Data Sharing for Event Based Encryption to Combat Adversarial Attacks,” IEEE Transactions on Network Science and Engineering, Vol. 8, 2020, pp. 1033-1043. doi: 10.1109/TNSE.2020.2987919.

8 Alvarez Ramiro and Nojoumian Mehrdad, "Comprehensive Survey on Privacy-Preserving Protocols for Sealed-Bid Auctions," Computers & Security. Vol. 88, 101502, 2020. https://www.sciencedirect.com/science/article/pii/S0167404818306631?via%3Dihub

9 S. Jiajun, L. Ningzhong, "Incentivizing Verifiable Privacy-Protection Mechanisms for Offline Crowdsensing Applications," Sensors (Switzerland). 17(9), 2017. doi: 10.3390/s17092024.

10 N. Cong, "Applications of Economic and Pricing Models for Wireless Network Security: A Survey," IEEE Communications Surveys and Tutorials. Vol. 19, No 4, 2017, pp. 2735-2767, doi: 10.1109/COMST.2017.2732462.

11 J. Baron, K. El Defrawy, J. Lampkins, R. Ostrovsky, "Communication-Optimal Proactive Secret Sharing for Dynamic Groups, Cryptology," ePrint Archive, Report 2015/304, 2015, https://eprint.iacr.org/2015/304.

12 J. Brendel, D. Demirel, "Efficient Proactive Secret Sharing," Cryptology ePrint Archive, Report 2017/719, 2017, https://eprint.iacr.org/2017/719.

13 I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," Telkomnika, 17(6), pp. 2812-2817, 2019, doi: 10.12928/TELKOMNIKA.v17i6.12490

14 S. Zaineldeen, A. Ate, "Improved cloud data transfer security using hybrid encryption algorithm," Indonesian Journal of Electrical Engineering and Computer Science, 20(1), 2020, pp. 521-527.

15 Banu B. Yergaliyeva, Yerzhan N. Seitkulov, Dina Satybaldina, Ruslan M. Ospanov, On some methods of storing data in the cloud for a given time // TELKOMNIKA (Telecommunication, Computing, Electronics and Control), Vol 20, No2, 2022, pp. 366-372. DOI: 10.12928/telkomnika.v20i2.21887

Е. Н. СЕЙТҚҰЛОВ, Б. Б. ЕРҒАЛИЕВА, Д. Ж. САТЫБАЛДИНА

Л.Н.Гумилев атындағы Еуразия ұлттық университеті. Нұр-Сұлтан, Қазақстан

БҰЛТТА ДЕРЕКТЕРДІ САҚТАУДЫҢ ҚАУІПСІЗ АУТСОРСИНГІНЕ АРНАЛҒАН ПРОТОКОЛДАР ЖӘНЕ ОЛАРДЫҢ БЕЛСЕНДІ ЖӘНЕ ПАССИВТІ ШАБУЫЛДАРҒА ТӨЗІМДІЛІГІН ТАЛДАУ

Бұл мақала әртүрлі криптографиялық шешімдерді пайдалана отырып, үлкен деректерді сақтау әдістерін әзірлеудің жаңа тәсілдерін зерттейді, мысалы, Shamir құпия бөлісу әдісі, Диффи-Хеллман кілттерін тарату хаттамасы және т.б. Әртүрлі зерттеушілер бұлтта деректерді сақтаудың әртүрлі әдістерін ұсынғанын ескеріңіз. Бұл мақалада біз құпия бөлісу технологиясын пайдалана отырып, үлкен деректерді сақтау үшін қауіпсіз аутсорсинг әдістері мен протоколдарын зерттейміз және олардың белсенді және пассивті шабуылдарға төзімділігін талдаймыз. Мұндай мәселелер әсіресе заттар интернетінің (IoT) қарқынды дамуы жағдайында өзекті болып табылады. Чиптердің, смарт карталардың және басқа физикалық шағын құрылғылардың жадында айтарлықтай шектеулер бар, сондықтан бұлтты сақтауды деректерді қауіпсіз сақтау үшін көмекші құрал ретінде пайдалану қажет.

Түйін сөздер*: криптография, ақпараттық қауіпсіздік, бұлтты сақтау, клиент пен сервердің өзара әрекеттесуі, заттардың Интернеті.*

YERZHAN N. SEITKULOV, BANU B. YERGALIYEVA, DINA ZH. SATYBALDINA

Gumilyov Eurasian National University
Nur-Sultan, Kazakhstan

PROTOCOLS FOR SECURE OUTSOURCING OF DATA STORAGE IN THE CLOUD AND ANALYSIS OF THEIR RESISTANCE TO ACTIVE AND PASSIVE ATTACKS

The paper explores new approaches to developing methods for storing big data using various cryptographic solutions, such as the Shamir secret sharing method, the Diffie-Hellman key distribution protocol, etc. Note that various researchers have proposed various methods for storing data in the cloud. In this paper, we explore methods and protocols for secure outsourcing for storing big data using secret sharing technology and analyze their resistance to active and passive attacks. Such problems are especially relevant in the context of the rapid development of the Internet of Things (IoT). Chips, smart cards, and other physically small devices tend to have significant memory limitations, so there is a need to use cloud storage as an auxiliary tool for secure data storage.

***Keywords**: cryptography, information security, cloud storage, client-server interaction, internet of things.*