S.V. Zapechnikov
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoyeshosse 31 Moscow, 115409, Russia, e-mail: SVZapechnikov@mephi.ru, ORCID iD0000-0002-7975-6040

Securing Document Warehouses against Brute Force Query Attacks

Keywords: data warehouses, search queries, cryptographic protocols, authentication, digital signature.
The paper presents the scheme of data management and protocols for securing document collection against adversary users who try to abuse their access rights to find out the full content of confidential documents. The configuration of secure document retrieval system is described and a suite of protocols among the clients, warehouse server, audit server and database management server is specified. The scheme makes it infeasible for clients to establish correspondence between the documents relevant to different search queries until a moderator won't give access to these documents. The proposed solution allows ensuring higher security level for document warehouses.

С.В. Запечников
Национальный исследовательский ядерный университет «МИФИ», Каширское шоссе, 31, Москва, 115409, Россия, e-mail: SVZapechnikov@mephi.ru, ORCIDiD 0000-0002-7975-6040

ЗАЩИТА ХРАНИЛИЩ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ОТ АТАК МЕТОДОМ ПЕРЕБОРА ПОИСКОВЫХ ЗАПРОСОВ

Ключевые слова: хранилища документов, поисковые запросы, криптографические протоколы, аутентификация, электронная подпись.
В статье предложена схема управления данными и протоколы, обеспечивающие безопасность хранилища электронных документов в условиях воздействия противника, пытающегося злоупотреблять своими правами доступа с целью выведать полное содержание конфиденциальных документов. Описываются конфигурация защищенной системы доступа к электронным документам и набор протоколов взаимодействия между клиентами, сервером доступа к хранилищу, сервером регистрации запросов клиентов и сервером баз данных. Схема делает невозможным для клиентов установление соответствий между документами, релевантными разным поисковым запросам до тех пор, пока доступ к этим документам не будет предоставлен модератором. Предложенное решение позволяет обеспечить повышенный уровень защищенности хранилищ конфиденциальных электронных документов.

Введение

Задачи обеспечения безопасности доступа к базам данных (БД) играют важную роль в современных информационных технологиях. Эти задачи весьма многообразны, и без них практически невозможно построить ни одну технологию массового информационного обслуживания пользователей, в связи с чем в научной литературе уделяется весьма значительное место решению таких задач. Перечислим наиболее значительные задачи и работы последних лет, посвященные их решению.

Первостепенное значение имеет задача контроля доступа к информации, которая хранится в многопользовательских БД. Наиболее заметным достижением в этой области стало появление концепции атрибутного шифрования (attribute-basedencryption – ABE), впервые предложенной в [1]. Атрибутное шифрование позволяет применить для защиты данных наиболее развитую из существующих модель контроля доступа – атрибутную, являющуюся обобщением ранее известных: дискреционной, мандатной и ролевой. Весьма заметное преимущество атрибутного шифрования – отсутствие необходимости хранить множество копий одних и тех же данных, зашифрованных на разных ключах. Вместо этого шифруется один экземпляр файла, а пользователям выдаются ключи для доступа к нему с закодированными в них правами доступа. Возможны два варианта:

1) политика доступа присоединяется к шифртекстам, а атрибуты – к ключам. Это атрибутное шифрование с политикой, привязанной к шифртексту (ciphertext-policyattribute-basedencryption – CP-ABE) [2];

2) политика доступа присоединяется к ключам, а атрибуты – к шифртекстам. Это атрибутное шифрование с политикой, привязанной к ключу (key-policy attribute0based encryption – KP-ABE) [3].

Не менее важно сохранение различных аспектов конфиденциальности действий клиентов, обращающихся к базам данных (в частности, анонимности, невозможности для провайдера определить конкретную запись, к которой обращается клиент, и отследить историю запросов клиента). Решению этих задач посвящены такие работы, как [4 – 6].

С развитием сред облачных вычислений и облачных хранилищ данных повышенную остроту приобрела проблема обработки конфиденциальной информации в облачной среде. Радикальным решением данной проблемы сможет стать создание практичных схем гомоморфного шифрования [7]. Однако перспектива появления таких схем выглядит реальной лишь в дальнесрочной перспективе, предполагающей значительное увеличение в будущем вычислительной мощности компьютеров. Кроме того, гомоморфное шифрование позволяет реализовать лишь арифметические операции над зашифрованными данными, но, например, для полноценной обработки запросов к реляционным БД требуется, вообще говоря, реализация операций реляционной алгебры над зашифрованными данными. В связи с этим сейчас основные способы решения этой проблемы заключаются либо в создании «промежуточных» решений на основе схем шифрования со специальными свойствами [8], либо в операциях над специально построенными индексами [9].

Наконец, еще одна серьезная проблема связана с обеспечением безопасности аналитической обработки данных, которая всё чаще «привязывается» к месту хранения данных. Примерами таких задач служат конфиденциальный поиск часто встречающихся подмножеств [10], конфиденциальное машинное обучение [11, 12] и конфиденциальное глубинное обучение нейронных сетей [13].

Однако проблема обеспечения безопасности доступа к информации не исчерпывается решением перечисленных задач. Даже при условии поддержания определенной политики доступа у пользователей остается возможность изучения содержания электронных документов путем перебора поисковых запросов и установление логической связи между ответами сервера БД.

В настоящей статье рассматривается один из возможных вариантов постановки и решения задачи защиты базы электронных документов от изучения содержания документов посредством перебора поисковых запросов.

Оставшаяся часть статьи организована следующим образом. В п. 1 рассматривается постановка решаемой задачи, в п. 2 – конфигурация системы, при которой возможна реализация предлагаемого решения, в п. 3 вводятся начальные предположения, п. 4 посвящен описанию структуры записей баз данных, пп. 5 – 7 содержат описания протоколов между участниками системы. В заключении подводятся итоги и формулируются основные результаты работы.

1. Постановка задачи

Пусть имеется множество электронных документов, содержащих конфиденциальную информацию и снабженных аннотациями (возможно, только часть документов содержит конфиденциальную информацию). Аннотации могут быть представлены как в форме связного текста, так и в форме списка ключевых слов (далее рассматривается второй случай). Множеству пользователей хранилища электронных документов предоставлена возможность поиска по аннотациям, благодаря чему пользователи могут найти в хранилище документы, релевантные их запросам. Однако доступ к полным текстам документов предоставляется модератором после дополнительной проверки необходимости (целесообразности) доступа конкретного пользователя к содержанию конкретного документа (эта процедура может быть автоматизирована путем использования методов интеллектуального анализа текстов, что выходит за рамки настоящей работы).

Требуется предложить такую конфигурацию системы доступа к хранилищу электронных документов и такие процедуры доступа пользователей, которые обеспечивали бы выполнение следующих требований:

1) доказательную регистрацию фактов отправки запросов конкретным пользователем с конкретным набором поисковых слов;

2) выдачу информации об электронных документах, релевантных поисковому запросу, по которой модератор может однозначно установить множеству соответствующих запросу документов для последующей проверки на предмет возможности предоставления доступа данному пользователю;

3) невозможность установления связи между документами, релевантными разным поисковым запросам (т.е. релевантен ли один и тот же документ или разные документы нескольким поисковым запросам одного пользователя), за исключением случаев угадывания этого соответствия с некоторой пренебрежимо малой вероятностью;

4) аутентификацию пользователей и серверов при их взаимодействии, а также (опционально) передачу данных по защищенному (секретному и аутентичному) каналу, если взаимодействие происходит в недоверенной среде.

Следует отметить, что именно свойство 3 является ключевым для рассматриваемой задачи, поскольку не позволяет пользователю делать выводы о содержании документа по набору слов, встречающихся в одном документе и обнаруженных в ходе подачи серии поисковых запросов.

2. Конфигурация системы

Конфигурация системы доступа к электронным документам, при которой возможна реализация предлагаемого решения, включает в себя (рис. 1):

1) пользователей системы, у каждого из которых установлено клиентское программное обеспечение для взаимодействия с серверной частью системы;

2) сервер доступа к хранилищу (СДХ) электронных документов;

3) базу данных регистрации запросов клиентов (БД РЗК), обслуживаемую сервером с установленной на нем системой управления базой данных (СУБД);

4) базу данных аннотаций документов (БД АнД), обслуживаемую сервером с установленной на нем СУБД, поддерживающей один из стандартных языков запросов: SQL [14] или аналогичный язык запросов для документно-ориентированных БД.

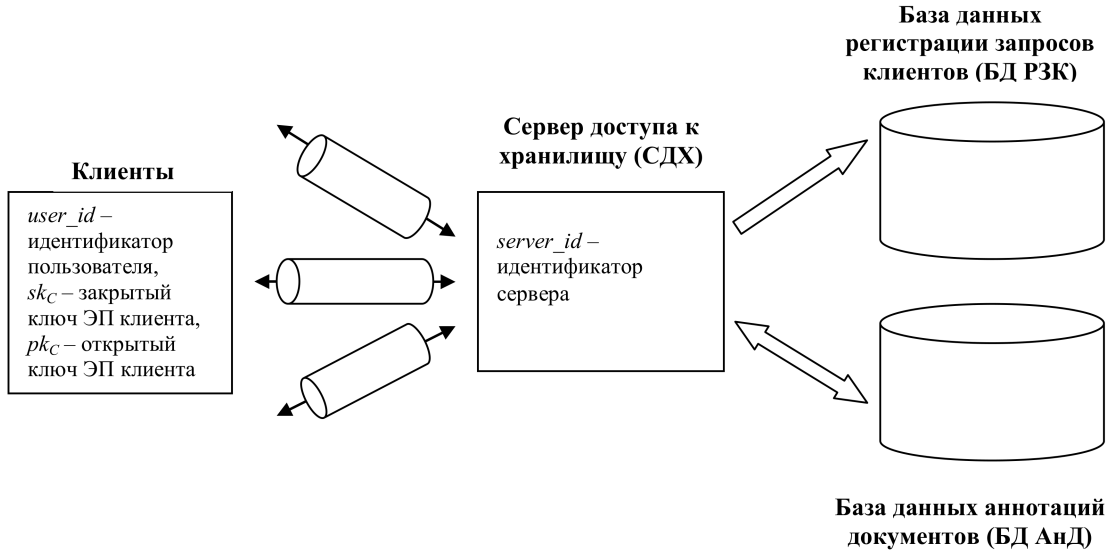

Рис. 1. Конфигурация системы доступа к электронным документам

Каждому клиенту системы присваивается уникальный идентификатор пользователя user_id (произвольная двоичная строка конечной длины) и выдается пара кличей электронной подписи (ЭП) (⟦sk⟧ _C, ⟦pk⟧ _C), где ⟦sk⟧ _C – закрытый ключ ЭП клиента, ⟦pk⟧ _C – открытый ключ ЭП клиента.

СДХ выдается уникальный идентификатор server_id (произвольная двоичная строка конечной длины).

БД РЗК должна быть открыта для СДХ только на запись.

БД АнД открыта для СДХ на чтение и запись (запись – лишь в определенные поля). СУБД на сервере, обслуживающем БД АнД, должна поддерживать язык запросов: в качестве такового далее рассматривается стандартный язык SQL.

3. Начальные условия

Для работы схемы выбираются H(·) – криптографическая хэш-функция, а также любая схема ЭП с дополнением. В качестве наиболее очевидных кандидатов на использование в предлагаемой схеме выступают функция хэширования по ГОСТ Р 34.11-2012 [15] и ЭП по ГОСТ Р 34.10-2012 [16]. Между каждым клиентом и СДХ, а также между СДХ и серверами БД РЗК и БД АнД устанавливается защищенный канал передачи данных (например, реализуется стандартный протокол TLS [17] или любой другой аналогичный по функциональности).

Если множество клиентов будет обращаться к множеству СДХ, между ними можно организовать аутентификация по протоколы Kerberos [18] или любому другому стандартному протоколу с аналогичной функциональностью.

Для проверки ЭП сообщений, пересылаемых между участниками системы, необходимо обеспечить аутентичность открытых ключей ЭП. Для этой цели может быть использован стандартный метод – поддержка инфраструктуры открытых ключей.

4. Структура записей баз данных

Для функционирования предлагаемой схемы необходимо, чтобы записи БД РЗК и БД АнД соответствовали формату, показанному на рис. 2 и 3.

P						*// Запрос клиента*
Q			*// ЭП запроса клиента*			

Рис. 2. Структура записи БД РЗК

doc_id							*// Идентификатор документа*
doc_ann							*// Аннотация документа*
doc_content	*// Полный текст документа (если предполагается хранение самих документов)*						
req_id	1		2		…	…	*// Идентификаторы запросов клиентов*
doc_req_id	1		2		…	…	*// Уникальные идентификаторы пар «запрос – документ»*
random	1		2		…	…	*// Одноразовые случайные числа*

Рис. 3. Структура записи БД АнД

Каждая запись БД РЗК должна состоять из полей, содержащих элементы запроса клиента *P* и ЭП запроса клиента *Q*.

Запрос клиента имеет следующий формат:

$$P = [user_{id}, server_{id}, time, \{keywords\}, req\_id],$$

где *user_id* – идентификатор клиента (см. п. 2);
server_id – идентификатор СДХ (см. п. 2);
time– метка времени, сгенерированная клиентом непосредственно перед моментом отсылки запроса;
$\{keywords\}$ – список ключевых слов запроса;
$req_{id} = H(user_{id}, server_{id}, time, \{keywords\})$ – идентификатор запроса, полученный путем хэширования всех предыдущих элементов запроса.

ЭП запроса генерируется по формуле

$$Q = \mathrm{Sign}_{sk_C}(P),$$

где *P* – запрос клиента, соответствующий описанному выше формату;
sk_C– закрытый ключ ЭП клиента;
Sign – алгоритм генерации подписи выбранной схемы ЭП.

Каждая запись БД АнД должна состоять из следующих полей:

doc_id – уникальный идентификатор документа (им может служить произвольная двоичная строка конечной длины);

doc_ann – аннотация документа (например, в форме списка ключевых слов);

doc_content – содержание документа, если предполагается хранение полных текстов документов;

req_id – идентификаторы запросов клиентов, которые добавляются в БД при каждом обращении клиента в случае совпадения ключевых слов поискового запроса с одним или несколькими ключевыми словами аннотации документа, при этом каждому такому идентификатору присваивается уникальный (в пределах документа) порядковый номер;

doc_req_id – уникальные идентификаторы пар «запрос – ответ», которые вычисляются СДХ в ходе выполнения протокола с БД АнД, каждому такому идентификатору также присваивается уникальный (в пределах документа) порядковый номер;

random – случайное число, которое генерируется СДХ и используется им для вычисления *doc_req_id*, каждому такому числу также присваивается уникальный (в пределах документа) порядковый номер.

Присвоение уникальных порядковых номеров трем последним элементам записи БД АнД необходимо для обеспечения возможности проверки поисковых запросов, на основании которых пользователю был предоставлен доступ к конфиденциальному документу.

5. Протокол взаимодействия клиента и СДХ

Протокол взаимодействия клиента и СДХ, в ходе которого происходят пересылка запроса клиента, обработка его СДХ и возврат ответа клиенту, показан на рис. 4.

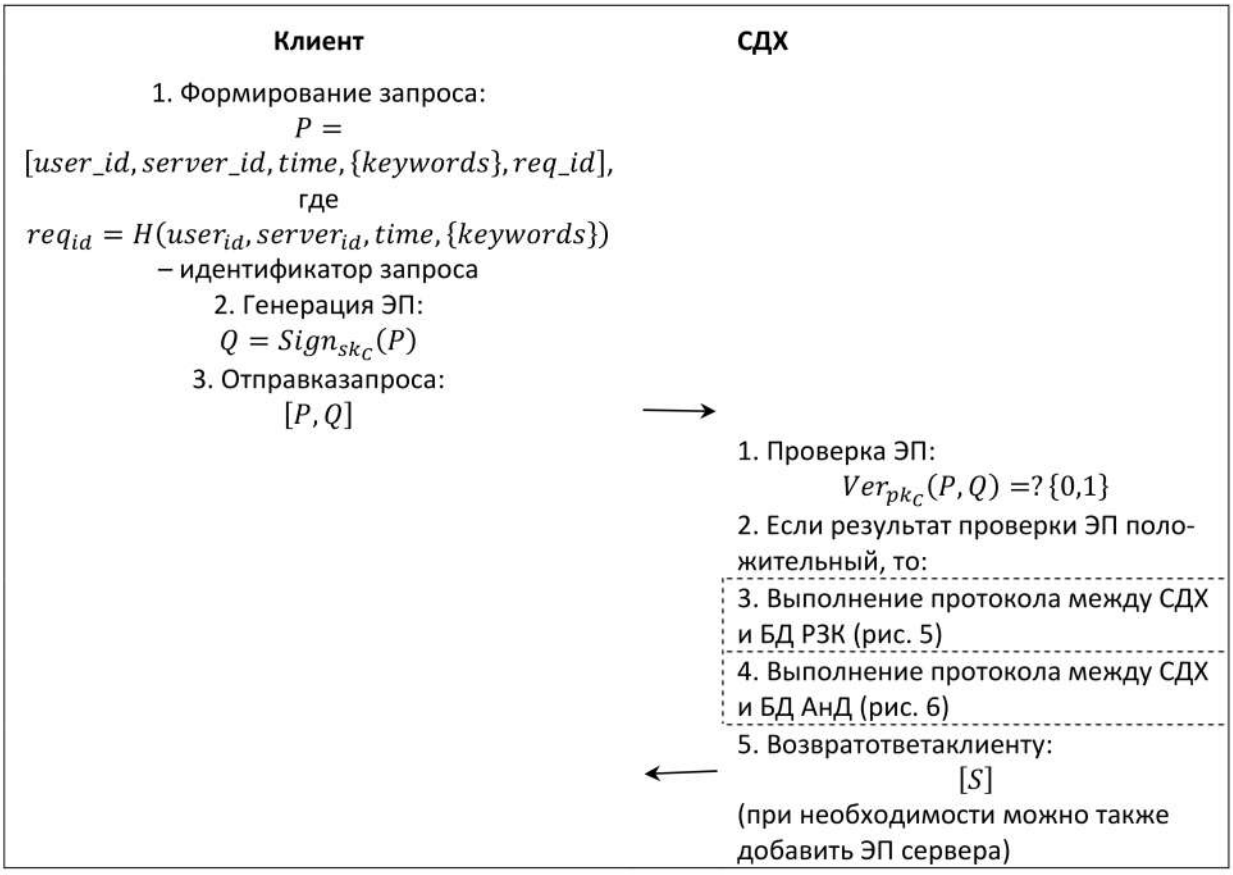

Рис. 4. Протокол взаимодействия клиента и СДХ

Особенность протокола заключается в том, что СДХ в ходе выполнения запроса клиента выполняет протоколы с БД РЗК и БД АнД, которые оказываются «встроены» в рассматриваемый протокол в качестве подпротоколов.
Рассмотрим протокол взаимодействия клиента и СДХ по шагам.

На первом этапе клиент формирует запрос P, формат которого соответствует описанному в п. 4, подписывает его своей ЭП Q и отправляет подписанный запрос [P,Q] серверу.

На втором этапе сервер проверяет подпись запроса и все дальнейшие шаги выполняет лишь при условии положительного результата проверки ЭП. Дальнейшие действия СДХ заключаются в выполнении протоколов взаимодействия с БД РЗК и БД АнД, что будет описано далее. После завершения выполнения этих двух протоколов СДХ формирует и пересылает ответ S клиенту. Возможны три варианта ответа.

1. Ответ формируется в виде

$$S = [\{doc\_req\_id\}].$$

При этом достигается максимальная конфиденциальность: клиент получает только уникальные идентификаторы «запрос – документ», которые ничего не сообщают о документе, сами документы могут быть предоставлены после ручной проверки модератором.

2. Ответ формируется в виде

$$S = [\{doc\_req\_id,doc\_ann\}].$$

Клиенту предоставляются идентификаторы пары «запрос – документ» и аннотации документов. Если аннотация состоит из ключевых слов (нет связного текста), то совпадение аннотаций ничего не говорит клиенту о том, один ли это документ или разные.

3. Ответ формируется в виде:

$$S = [\{doc\_req\_id,doc\_ann,doc\_content\}].$$

Клиенту сразу предоставляется полный текст всех релевантных запросу документов.

При необходимости ответ S может быть также подписан ЭП сервера.

6. Протокол взаимодействия СДХ и БД РЗК

Протокол взаимодействия СДХ и сервера, поддерживающего БД РЗК, состоит из одной пересылки сообщения вида [P,Q] от СДХ на сервер, поддерживающий БД РЗК, и подтверждения регистрации запроса от последнего (рис. 5).

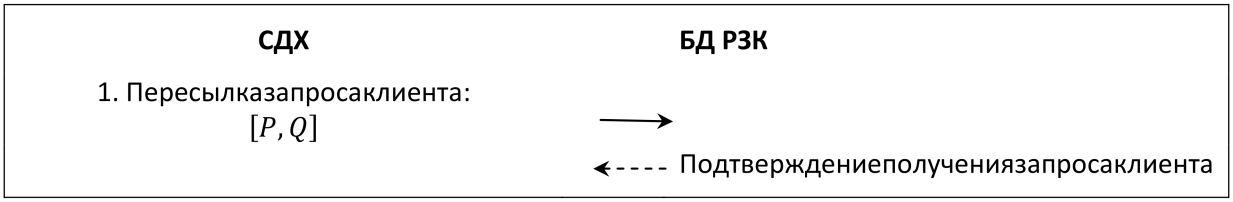

Рис. 5. Протокол взаимодействия СДХ и БД РЗК

С целью обеспечения невозможности отказа от факта обращения клиента с запросом пересылаемые сообщения могут снабжаться ЭП отправителей (на рисунке не показаны). Для обеспечения невозможности редактирования записей, внесенных в БД РЗК, можно использовать в качестве таковой БД, построенную по принципу цепочки блоков, связанных функциями хэширования – блокчейна [19].

7. Протокол взаимодействия СДХ и БД АнД

Протокол, показанный на рис. 6, выполняется после завершения регистрации запроса клиента в БД РЗК и имеет целью подготовку всех данных, необходимых для формирования ответа S клиенту на его запрос P, направленный СДХ.

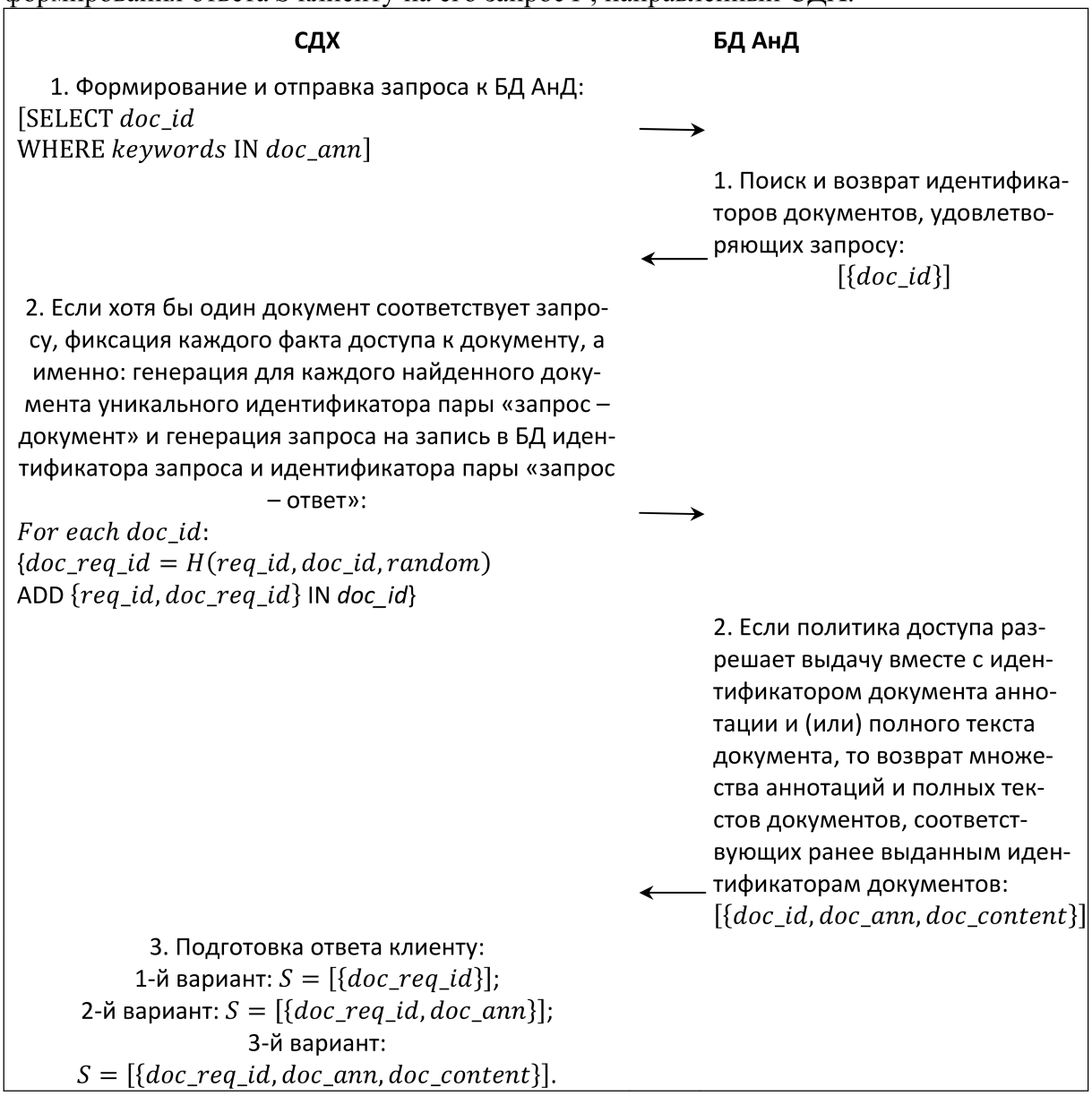

Рис. 6. Протокол взаимодействия СДХ и БД АнД

Рассмотрим протокол взаимодействия СДХ и БД АнД по шагам.

На первом этапе СДХ формирует запрос к БД АнД. Для определенности будем полагать, что запрос имеет вид

[SELECT *doc_id*
WHERE *keywords* IN *doc_ann*].

В ответ на запрос сервер, поддерживающий БД АнД, отправляет множество идентификаторов документов, удовлетворяющих запросу: [$\{doc\_id\}$].
Если хотя бы один документ соответствует запросу, на втором этапе фиксируется каждый факт доступа к аннотации документа. С этой целью для каждого найденного документа вычисляется идентификатор пары «запрос – документ» вида

$$doc\_req\_id = H(req\_id, doc\_id, random),$$

после чего СДХ направляет серверу, поддерживающему БД АнД сообщение с SQL-оператором вида

ADD $\{req\_id, doc\_req\_id\}$ IN doc_id,

выполнение которого приводит к добавлению в соответствующую запись БД идентификаторов запроса клиента и пары «запрос – документ».

БД АнД возвращает подтверждение записи идентификаторов для учета каждого факта обращения, и если политика доступа разрешает выдачу вместе с идентификатором документа аннотации и (или) полного текста документа, то БД АнД возвращает СДХ также множество аннотаций и полных текстов документов, соответствующих ранее выданным идентификаторам документов: [$\{doc\_id, doc\_ann, doc\_content\}$].

Заключительный этап – подготовка ответа S на запрос клиента. Возможны три варианта формирования ответа:

1-й вариант – в ответ включаются только идентификаторы пар «запрос – документ» – обеспечивает максимальную конфиденциальность: уникальные идентификаторы пар ничего не сообщают клиенту о документах и их соответствиям разным поисковым запросам, сами документы могут быть предоставлены после ручной проверки модератором;

2-й вариант – в ответ включаются идентификаторы пар «запрос – документ» и аннотации документов – обеспечивают меньшую степень конфиденциальности: если аннотация состоит из ключевых слов (нет связного текста), то совпадение подмножества ключевых слов в аннотациях документов еще ничего не говорит клиенту о том, один ли это документ или разные;

3-й вариант – в ответ включаются идентификаторы пар «запрос – документ», аннотации документов и полные тексты документов – дает возможность сразу предоставлять клиенту содержание всех найденных документов, этот вариант не обеспечивает конфиденциальность, но обеспечивает доказательную регистрацию всех запросов пользователей.

После завершения описанного протокола СДХ подготовил все необходимые данные для ответа клиенту. Далее происходит возвращение к выполнению протокола взаимодействия клиента и СДХ, описанного в п. 5.

Заключение

В статье предложено решение задачи защиты хранилища электронных документов от атак методом перебора поисковых запросов. Решение включает в себя описание конфигурации системы, требуемой для решения задачи, спецификацию начальных условий и трех протоколов, выполняемых между участниками системы.

Практическая ценность предложенного решения состоит в возможности с его помощью обеспечивать повышенный уровень защищенности хранилищ электронных документов конфиденциального содержания и других баз данных, содержащих текстовую информацию.

Перспективы продолжения исследования заключаются в решении задач контроля доступа (при одновременном обеспечении безопасности пользователей) к хранилищам данных более сложной структуры, в частности к многомерным массивам данных.

СПИСОКЛИТЕРАТУРЫ:

1.Sahai A., Waters B. Fuzzy identity-based encryption. 15 pp. URL: http://eprint.iacr.org/2004/086 (дата обращения: 25.01.2017 г.)
2. Goyal V., Pandey O., Sahai A., Waters B. Attribute-based encryption for fine-grained access control of encrypted data. 28 pp. URL: http://eprint.iacr.org/2006/309 (дата обращения: 25.01.2017).
3. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption. 15 pp. URL: http://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe.pdf (дата обращения: 25.01.2017).
4. Camenisch J., Dubovitskaya M., Neven G. Oblivious transfer with access control. Proc. of ACM CCS 09, Chicago, Illinois, USA, November 9-13, 2009. ACM Press. Pp. 131–140.
5. Camenisch J., Dubovitskaya M., Neven G. Unlinkable priced oblivious transfer with rechargeable wallets. Proc. of Financial Cryptography'10. Pp. 66–81.
6. Camenisch J., Dubovitskaya M., Neven G., Zaverucha G. Oblivious transfer with hidden access control policies. Proc. of PKC 2011, volume 6571 of LNCS, Taormina, Italy, March 6-9, 2011.Springer, Berlin, Germany.Pp. 192–209.
7. van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. Fully Homomorphic Encryption over the Integers. Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. Pp. 24–43.
8. Popa R.A., Redfield C., Zeldovich N., Balakrishnan H. CryptDB: Protecting confidentiality with encrypted query processing. Proc. of the 23rd ACM Symposium on operating systems principles (SOSP), Cascais, Portugal, Oct. 2011.ACM, New York, USA. Pp. 85–100.
9. Poddar R., Boelter T., Popa R.A. Arx: A strongly encrypted database system.2016. URL: http://eprint.iacr.org/2016/591.pdf (дата обращения: 02.02.2017).
10. Laud P., Pankova A. Privacy-preserving frequent itemset mining for sparse and dense data. URL: http://eprint.iacr.org/2015/671.pdf (датаобращения: 02.02.2017).
11. Graepel T., Lauter K., Naehrig M. ML confidential: Machine learning on encrypted data. Proc. on 15th International conference «Information security and cryptology» (ICISC) 2012. Seoul, Korea. Nov. 28-30, 2012. LNCS 7893.Springer, 2013. Pp. 1–21.
12. Bost R., Popa R.A., Tu S., Goldwasser S. Machine learning classification over encrypted data. Proc. on Network and Distributed System Security Symposium (NDSS) 2015, 8–11 February 2015, San Diego, CA, USA.
13. Chabanne H., de Wargny A., Milgram J., Morel C., Prouff E. Privacy-preserving classification on deep neural network. URL: http://eprint.iacr.org/2017/035 (дата обращения: 03.02.2017).
14. ISO/IEC 9075: Information technology - Database languages – SQL. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45342 (дата обращения: 03.02.2017).
15. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (дата обращения: 03.02.2017).
16. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (дата обращения: 03.02.2017).
17. Dierks, T., and Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug. 2008. URL: https://tools. ietf.org/html/rfc4346 (дата обращения: 03.02.2017).
18. Kohl J., Neuman C. The Kerberos Network Authentication Service (V5). RFC 4120. (Proposed Standard), Jul. 2005. URL: https://tools. ietf.org/html/rfc4120 (датаобращения: 03.02.2017).
19. Swan M. Blockchain: Blueprint for a new economy. O'Really Media Inc., 2015. 129 p.

REFERENCES:

1. Sahai A., Waters B. Fuzzy identity-based encryption. 15 pp. URL: http://eprint.iacr.org/2004/086 (date of access: 25.01.2017).

2. Goyal V., Pandey O., Sahai A., Waters B. Attribute-based encryption for fine-grained access control of encrypted data. 28 pp. URL: http://eprint.iacr.org/2006/309 (date of access: 25.01.2017).
3. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption. 15 pp. URL: http://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe.pdf (date of access: 25.01.2017).
4. Camenisch J., Dubovitskaya M., Neven G. Oblivious transfer with access control. Proc. of ACM CCS 09, Chicago, Illinois, USA, November 9-13, 2009. ACM Press. Pp. 131–140.
5. Camenisch J., Dubovitskaya M., Neven G. Unlinkable priced oblivious transfer with rechargeable wallets. Proc. of Financial Cryptography'10. Pp. 66–81.
6. Camenisch J., Dubovitskaya M., Neven G., Zaverucha G. Oblivious transfer with hidden access control policies. Proc. of PKC 2011, volume 6571 of LNCS, Taormina, Italy, March 6–9, 2011.Springer, Berlin, Germany.Pp. 192–209.
7. van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. Fully Homomorphic Encryption over the Integers. Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. Pp. 24–43.
8. Popa R.A., Redfield C., Zeldovich N., Balakrishnan H. CryptDB: Protecting confidentiality with encrypted query processing. Proc. of the 23rd ACM Symposium on operating systems principles (SOSP), Cascais, Portugal, Oct. 2011. ACM, New York, USA. Pp. 85–100.
9. Poddar R., Boelter T., Popa R.A. Arx: A strongly encrypted database system.2016. URL: http://eprint.iacr.org/2016/591.pdf (date of access: 02.02.2017).
10. Laud P., Pankova A. Privacy-preserving frequent itemset mining for sparse and dense data. URL: http://eprint.iacr.org/2015/671.pdf (date of access: 02.02.2017).
11. Graepel T., Lauter K., Naehrig M. ML confidential: Machine learning on encrypted data. Proc. on 15th International conference «Information security and cryptology» (ICISC) 2012. Seoul, Korea. Nov. 28-30, 2012. LNCS 7893. Springer, 2013. Pp. 1–21.
12. Bost R., Popa R.A., Tu S., Goldwasser S. Machine learning classification over encrypted data. Proc. on Network and Distributed System Security Symposium (NDSS) 2015, 8–11 February 2015, San Diego, CA, USA.
13. Chabanne H., de Wargny A., Milgram J., Morel C., Prouff E. Privacy-preserving classification on deep neural network. URL: http://eprint.iacr.org/2017/035 (date of access: 03.02.2017).
14. ISO/IEC 9075: Information technology – Database languages – SQL. URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45342 (date of access: 03.02.2017).
15. GOST R 34.11-2012. Information technology.Cryptographic data security. Hash function. URL: http://protect.gost.ru/document.aspx?control=7&id=180209 (date of access: 03.02.2017).
16. GOST R 34.11-2012. Information technology.Cryptographic data security.Signature and verification processes of [electronic] digital signature. URL: http://protect.gost.ru/document.aspx?control=7&id=180151 (date of access: 03.02.2017).
17. Dierks, T., and Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), Aug. 2008. URL: https://tools. ietf.org/html/rfc4346 (date of access: 03.02.2017).
18. Kohl J., Neuman C. The Kerberos Network Authentication Service (V5). RFC 4120. (Proposed Standard), Jul. 2005. URL: https://tools. ietf.org/html/rfc4120 (date of access: 03.02.2017 г.).
19. Swan M. Blockchain: Blueprint for a new economy. O'Really Media Inc., 2015. 129 p.