УДК 004.056.5:004.6

ИССЛЕДОВАТЕЛЬСКИЙ АНАЛИЗ ПО ХРАНЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ И ПУБЛИЧНОМУ АУДИТУ В ОБЛАЧНОМ ХРАНИЛИЩЕ

ЖОЛДЫ Т. М.

Евразийский национальный университет имени Л.Н.Гумилёва
(г. Астана, Казахстан)

Аннотация. Технология облачного хранения набирает популярность, поскольку позволяет пользователям выполнять больше работы при экспорте данных в облако. Он должен гарантировать, что только законный клиент или аутентифицированный пользователь может получить доступ к администрированию и никто другой. Одной из проблем является конфиденциальность данных в облачном хранилище и защита от многих проблем, связанных с аутсорсингом облачных данных, по сравнению с облачным аутсорсингом. Шифр находится в облаке. Помимо этого, исследовательская деятельность определяет публичный источник с целью новейшего прямого допуска, что возможно проконтролировать различным источником. Предлагаемая модель отпустит собственную сведение в публичные информации.

Annotation. Cloud storage technology is gaining popularity as it allows users to do a lot of the work of exporting data to the cloud. It must ensure that only a legitimate client or authenticated user can access administration and no one else. One of the concerns is data privacy in cloud storage and protection from many of the problems associated with cloud data outsourcing compared to cloud outsourcing. The cipher is in the cloud. In addition, research activity pursues a public source with the aim of subsequent direct hit. The proposed model releases the new information to the public.

Введение

Облачное хранилище рассматривается точно, как обыкновенный научно-технический прорыв. Облачные вычисления — это самый новый метод осуществить вычисляемые силы вместе с поддержкой удаленных серверов, которые дают средства с целью сохранения, вычислений, а также общего применения дополнений. Способности подобных сервисов становятся актуальными с целью огромного числа информации с применением приборов для сохранения, а также обработки. При случае единичные личности либо компании передают личные сведения подобным ресурсам, они уязвимы для 3 персон, так как сведения могут быть тронуты, а также ошибочно истолкованы. Допустимым решением для предоставления конфиденциальности информации способен быть за кодирование.

Кодирование — есть процедура хранения цифровой информации либо текстового информации в ином представлении, обеспечивающем защиту с разной неразрешенной сведении. Национальное организация способен применять данную платформу с целью исследования безопасного и еще эффективного метода обмена бумагами, а также информацией в облаке. Процедура извлечения в главном потребует весьма кратковременного периода с целью извлечения закодированных информации, поэтому необходимы разнообразные постановления с целью безопасного сохранения информации в полупроводниках для облака. Один из вероятных заключений, способных избежать неразрешенную информативную защищенность хакеров, считается шифрование документов, хранящихся в облаке.

Общеизвестно, что облачное хранилище может стать настоящей находкой для различных предприятий и клиентов. Его будущие приложения охватывают многие аспекты вычислений и, возможно, никогда не будут полностью реализованы. Облачные вычисления позволяют настроить несколько прав в разных местах и не так бюрократичны, как сопоставимые сервисы, обеспечивая высокий уровень безопасности и простой в использовании интерфейс. Ваша личность и личность этих людей должны храниться постоянно, что не допускается при использовании облака. Обмен информацией также важен. Это можно сделать с помощью мобильных устройств, таких как смартфоны и планшеты, а также через Интернет.

Основная часть

Определение способов конфиденциальной передачи данных. Для решения этой проблемы необходимо использовать криптографические механизмы, обеспечивающие надежное шифрование данных. Как известно, существует два типа алгоритмов шифрования — симметричные и асимметричные. Симметричное шифрование дает огромное преимущество с точки зрения скорости шифрования и снижения нагрузки на вычислительные ресурсы, но его надежность уступает асимметричному шифрованию из-за специфики аппаратной реализации некоторых математических преобразований. Конечно, использование смешанного шифрования имеет значительные преимущества. В качестве реализации рассмотрим следующие алгоритмы шифрования AES, RSA:1. Стандарт AES представляет собой алгоритм симметричного блочного шифрования.

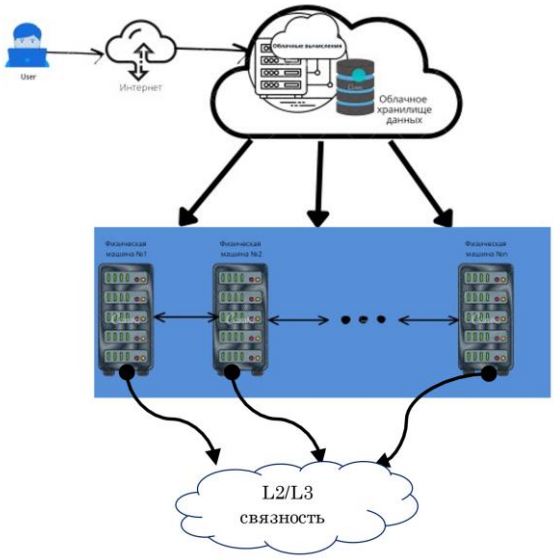

Рис. 1. Функциональная архитектура облачных сред

Алгоритм основан на нескольких заменах, подстановках и линейных преобразованиях, каждое из которых выполняется блоками по 16 байт. Операции повторяются несколько раз, каждая из которых называется «раунд». В каждом раунде вычисляется уникальный ключ раунда, который включается в расчет на основе ключа шифрования. Из-за схожей блочной структуры AES изменение даже одного бита в ключевом или текстовом блоке приводит к полной смене всего шифра, что является явным преимуществом перед традиционными потоковыми шифрами. Благодаря описанным преимуществам шифрование AES является криптографически стойким по результатам исследования Агентства национальной безопасности США.

2.RSA — один из самых успешных алгоритмов асимметричного шифрования на сегодняшний день. В отличие от традиционных систем симметричного шифрования, RSA работает с двумя разными ключами: «открытым» ключом и «закрытым» ключом. Оба работают вместе, и сообщение, зашифрованное одним, может быть расшифровано только другим. Поскольку закрытый ключ нельзя вычислить из открытого ключа, последний можно хранить в открытом доступе. Безопасность RSA основана на математической проблеме целочисленной факторизации. Зашифрованное сообщение обрабатывается как большое число. При шифровании его возводят в степень ключа и делят с остатком на произведение первых двух. Повторив процесс с другим ключом, вы можете получить исходный текст. Самый известный трюк — включить множитель, используемый при делении.

Сегодня невозможно выполнить такую факторизацию для чисел больше 768 бит. Поэтому современные системы шифрования используют минимальную длину ключа 3072 бита. Важно отметить, что для снижения вероятности перехвата передаваемого сообщения в открытом виде шифрование данных должно происходить до того, как информация покинет браузер пользователя (то есть до отправки сообщения на сервер).

Рассмотрим защищенный протокол передачи данных TLS v1.2, в котором реализованы алгоритмы шифрования информации на основе уже рассмотренных алгоритмов AES, RSA, аутентификации пользователя и контроля целостности данных.

Работа протокола TLS начинается с согласования используемой версии протокола, метода шифрования данных между узлами соединения, а также проверки валидности полученных сертификатов, после чего будет установлен криптографически безопасный канал. Отметим, что шифрование с открытым ключом следует использовать только в начальной процедуре настройки соединения, что позволяет определить общий секретный ключ шифрования без предварительного знания узлов соединения. После настройки туннеля необходимо использовать симметричную криптографию, связь в рамках текущей сессии будет шифроваться именно установленными симметричными ключами.

Таким образом, было показано, что использование протокола TLS v1.2 позволяет создать конфиденциальный канал передачи данных. Следует, отметить, что механизмы работы этого протокола не предусматривают контроль времени жизни каждой пользовательской сессии и повторную аутентификацию клиента с целью возобновления сессии в случае разрыва соединения. Также отметим, что протокол TLS v1.2 не позволяет проводить аутентификацию самого пользователя, поэтому мы будем рассматривать механизм аутентификации пользователей по протоколу OAuth2.0.

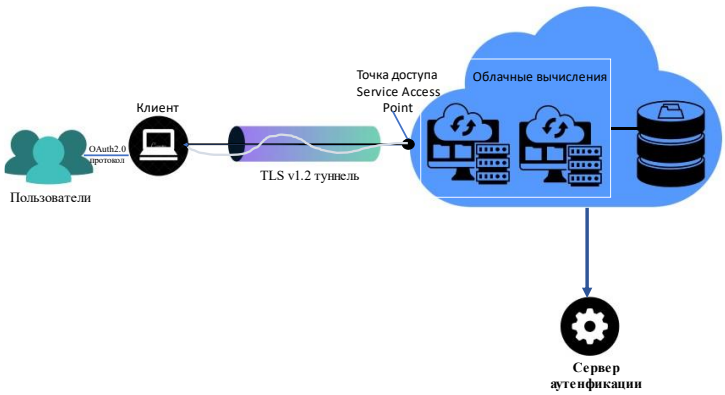

Рис. 2. Концептуальная схема построения защищенной облачной среды

Заключение

В работе рассмотрены алгоритм установления безопасного TLS-соединения на основе обмена открытыми криптографическими ключами, алгоритм обмена сертификатами для проверки валидности узлов, участвующих в обмене конфиденциальными данными, а также алгоритм проверки целостности информация, полученная принимающей стороной хоста (клиентом или сервером), на основе расчета суммы MAC-адресов каждого отправленного сообщения. Оказалось, что для создания надежного TLS-соединения важно иметь возможность аутентифицировать клиентскую часть приложения, а не самого пользователя.

В заключение исследования представлена обобщенная схема организации безопасного доступа к облачной среде, включающая рассмотренные ранее механизмы, гарантирующие целостность, конфиденциальность и доступность.

Следующими этапами исследования можно считать рассмотрение способов хранения конфиденциальной информации в зашифрованном виде, а также методов ее обработки и поиска в облачных хранилищах.

Список использованных источников

1. NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Comput ing. December 09, 2011. 80 p. URL: http://www.nist.gov/cus tomef/get_pdfefm?pub_id=909494
2. Side root Qing, Takamatsu, Shao Bilin. For cloud storage distributed storage security architecture [J]. Journal of Xi'an Jiao Tong University. 2011 (04).
3. Feng Dengguo, Aman Chang, Zhang Yan, Xu Zhen. Research on the security of cloud computing [J]. software journal. 2011 (01).
4. "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY, International Journal of Engineering Science and Technology (!JEST), Vol. 3 No. 9 September 2011.
5. Chopde, International lournal of Computer Applications (0975 - 8887) Volume 34- No.9, November 2011
6. A.O. AI-Badrani, M.Y. Saif, Review of security challenge facing a cloud-based organization, Int. I. 7 (2018).
7. Z.A. Musaylim, N. Jhanjhi, Comprehensive review: protecting user privacy in mobile cloud computing services, Wirel. Perscom. 111 (2020) 541-564