УДК 004.056

А.Н. Волокита, А.Е. Бидков

ЗАЩИЩЕННАЯ МНОГОКАНАЛЬНАЯ ПЕРЕДАЧА ДАННЫХ В CLOUD COMPUTING

Аннотация: В статье рассматриваются проблемы безопасности и эффективности передачи данных. Описаны преимущества многоканальной передачи, рассматривается возможность использования протокола SCTP. Предложен метод многоканальной передачи данных с разными уровнями защиты в каждом канале и предварительным шифрованием, что позволяет повысить безопасность и эффективность передачи, гибкость в выборе уровня защищенности.

Ключевые слова: SCTP, AES, безопасность, эффективность передачи данных, cloud computing

Введение

Современные организации зависят от возможностей обработки данных, затрат и накладных расходов на управление своими вычислительными ресурсами. Концепция облачных вычислений предназначена освободить организации и их сотрудников от дополнительных расходов связанных с ИТ. Клиент может перенести хранение данных, обработку информации или даже всю информационную инфраструктуру к провайдеру услуг, что позволяет сфокусироваться на своей основной деятельности и оставить ИТ профессионалам [1].

В то время как концепция облачных вычислений предоставляет новый подход к обработке информации, проблемы безопасности выходят на первый план. Требования безопасности являются ключевым фактором для принятия решения об использовании информационно-технических услуг и, в частности, для решения о переходе к среде публичных облачных вычислений [2].

Важной частью облачных вычислений является обеспечение безопасного и эффективного доступа к большим объемам удаленных данных.

Практически все существующие решения обеспечения безопасности основываются на шифровании данных. Однако предложены и альтернативные решения, например, основанные на физическом разделении передачи для защиты данных. При этом предлагается использовать SCTP - надежный транспортный протокол, который обеспечивает стабильную, упорядоченную (с сохранением порядка следования пакетов) передачу данных между двумя конечными точками (подобно TCP) [3,4]. Протокол поддерживает многопоточную передачу данных и синхронное соединение между двумя узлами сети по двум и более независимым физическим каналам. Протокол SCTP за счет многопоточности позволяет повысить скорость передачи данных, а физическое разделение каналов усложняет задачу перехвата данных. Но данный метод не может быть

применен для передачи данных, требующих более высокого уровня защиты, так как существует вероятность перехвата информации из одного и более каналов.

Одним из предложенных ранее методов повышения эффективности передачи данных является использование выборочного шифрования [5]. Данный подход для защиты мультимедиа информации позволяет снизить вычислительные затраты связанные с шифрованием больших объемов данных. Использование выборочного шифрования для других видов информации весьма сомнительно, так как незашифрованная часть может содержать секретные данные.

В статье предлагается использование многоканальной передачи данных с различным шифрованием для каждого канала.

Многоканальная передача данных

Схема передачи данных

Для многоканальной передачи данных предлагается использовать протокол SCTP. На рис. 1 представлена схема подключения пользователя к сервису облачных вычислений. Будем различать открытые каналы (O), данные в которых дополнительно не шифруются, и защищенные каналы (S), данные в которых шифруются дополнительно. Каждый защищенный канал шифруется отдельным ключом. Большинство пользователей физически соединены с сетью одним каналом, поэтому каналы в данном случае виртуальные. Хотя использование физически разных каналов и не исключается.

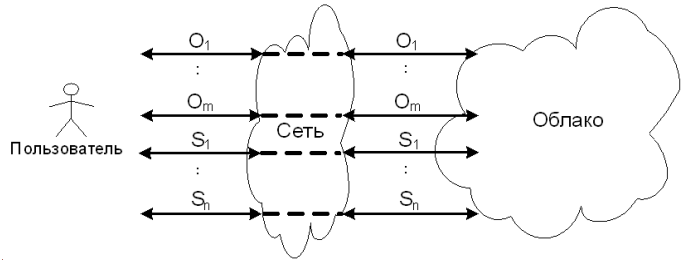

Рис. 1 – Схема многоканального соединения

Рассмотрим схему передачи данных для двух каналов: открытого и защищенного (рис. 2). Информация перед передачей делится на блоки, которые шифруются. Размер блоков выбирается исходя из требований метода шифрования. Каждый зашифрованный блок разделяется на части $N*X$, $N*(1-X)$, где N – размер блока, X – коэффициент разделения ($X \in [0,1]$). Коэффициент X можно варьировать, исходя из требований безопасности и/или вычислительных затрат.

Не смотря на то, что открытый канал не шифруется, данные по нему передаются уже в зашифрованном виде. Предложенный подход позво-

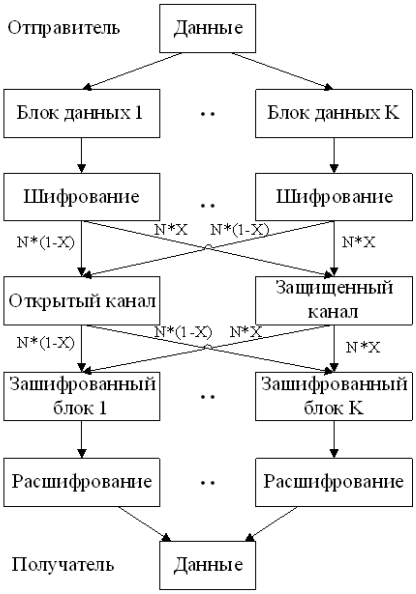

Рис. 2 – Схема передачи данных для двух каналов

ляет отказаться от шифрования вообще для тех случаев, когда передаваемые данные не требуют защиты.

При неравномерном распределении нагрузки на каналы, могут возникать задержки, связанные с ожиданием накопления данных перед отправкой, либо издержки связанные с передачей малого объема полезной информации в одном кадре.

Использование ключей разной длины для шифрования

Рассмотрим вариант использования ключей различной длины для предварительного шифрования и защищенного канала. В качестве примера используется алгоритм шифрования AES (Advanced Encryption Standard) – один из самых распространенных на сегодняшний день. AES – симметричный алгоритм блочного шифрования, в котором используются ключи размером 128, 192 и 256 бит [6]. В таблицах 1, 2 представлено необходимое количество операций для выполнения шифрования, расшифровывания соответственно для ключей 128 и 256 бит, где AND, OR, SHIFT – операции побитового И, ИЛИ, сдвига.

Как видно из таблиц, затраты на шифрование блоков данных не уменьшаются при уменьшении размера блока меньше чем ключ. Поэтому более эффективным является вариант использования для 256 битного ключа блоков размером также 256 бит.

На рис. 3 представлены вычислительные затраты на шифрование данных размером 1024 бита согласно таблице 1. AND, OR, SHIFT обозна-

Таблица 1

Затраты шифрование AES

Размер ключа, биты	Размер данных, биты	Необходимое количество операций		
		AND	OR	SHIFT
128	128	1720	1268	408
256	128	4912	3624	1168
256	256	4912	3624	1168

Таблица 2

Затраты расшифровывание AES

Размер ключа, биты	Размер данных, биты	Необходимое количество операций		
		AND	OR	SHIFT
128	128	5176	3860	1272
256	128	14896	11112	3664
256	256	14896	11112	3664

чают количество соответствующих битовых операций для шифрования данных блоками по 256 бит ключом размером 256 бит. AND мк / OR мк / SHIFT мк обозначают количество битовых операций для шифрования данных с использованием предложенной многоканальной схемы: все данные шифруются блоками в 128 бит ключом 128 бит. Часть зашифрованных данных (определяется X) передается по защищенному каналу с дополнительным шифрованием 256 битным ключом. При этом не учитываются возможные дополнительные издержки, связанные с необходимостью заполнения неполных блоков для шифрования.

Графики показывают, что предложенный метод позволяет снизить вычислительные затраты на шифрование данных при коэффициенте $X до \approx 0,77$. Так как информация в открытом канале не полная (для $X > 0$), то для получения всех переданных данных злоумышленнику необходимо дешифровать информацию из защищенного канала с длиной ключа 256 бит.

Сравнивая таблицы 3 и 4 очевидно, что для расшифровывания данных соотношения вычислительных затрат не изменятся.

Полученные результаты позволяют рассматривать возможность дополнительного шифрования без увеличения вычислительных затрат. При значении $X до \approx 0.77$ вычислительные затраты соответствуют полному шифрованию 256 битным ключом. При этом злоумышленнику потребуется дешифровать данные сначала из защищенного канала, зашифрованные 256 битным ключом. После, объединив результат с информацией из открытого канала, выполнить дешифрование еще раз для шифрования 128 битного ключа.

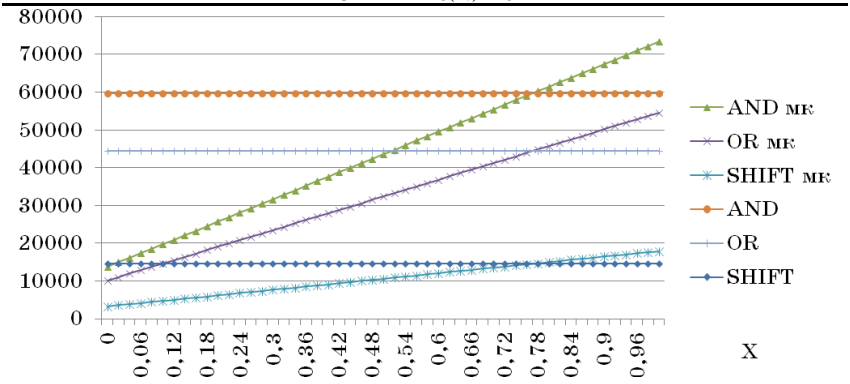

Рис. 3 – Вычислительные затраты на шифрование данных (размер блока данных/размер ключа – 128/128, 256/256)

Управление коэффициентом передачи

В большинстве случаев пользователю не требуется шифрование с ключом 256 бит. Соответственно можно экономить вычислительные затраты сервиса и клиента изменяя коэффициент передачи по защищенному каналу (X).

Изменять коэффициент можно либо по запросу пользователя, либо исходя из требуемого уровня секретности информации. Второй вариант больше подходит для передачи файлов, так как появляется возможность задать уровень защиты как атрибут файла.

Уровень секретности (уровень защищенности передачи) задается коэффициентом X, так как он определяет, какой объем данных шифруется ключом 256 бит. Самым низким будет уровень при $X = 0$ – данные передаются только по открытому каналу, а самый высокий при $X = 1$ – данные передаются только по защищенному каналу.

При $X = 0$ также следует определять, нужно ли выполнять предварительное шифрование, либо передаваемые данные не требуют защиты.

При $X = 1$ все данные фактически шифруются 2 раза: сначала 128 битным ключом, потом 256 битным, что требует дополнительных вычислительных затрат.

Выводы

Предложен метод защищенной многоканальной передачи данных, позволяющий повысить безопасность передачи данных, снизить вычислительные затраты, связанные с шифрованием.

При передаче малых объемов данных использование множества каналов может быть неэффективным, так как будут возникать дополнительные издержки при передаче данных по всем каналам. Поэтому

предложенный метод эффективен для передачи больших объемов данных.

Направление будущих исследований - определение минимального значения коэффициента X, при котором можно считать информацию из открытого канала недостаточной для дешифрования.

Для определения эффективности предложенного метода планируется проведение практических экспериментов.

Литература

1. Wang W., Owens R., Li Z., Bhargava B. Secure and Efficient Access to Outsourced Data. Proceedings of the 2009 ACM workshop on Cloud computing security. Pages 55-65, 2009.
2. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology Draft Special Publication 800-144. 60 pages, Jan. 2011.
3. Lindskog S., Grinnemo K., Brunstrom A. Physical Separation for Data Protection based on SCTP Multihoming.
4. URL: http://www.cs.kau.se/~stefan/publications/SNCNW04/paper.pdf
5. Джонс Т. Надежная передача данных по протоколу SCTP. URL: http://www.ibm.com/developerworks/ru/library/l-sctp/
6. Liu X., Eskicioglu A. Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions. 2003. URL: http://web.cs.gc.cuny.edu/~xliu/index_files/CIIT2003.pdf
7. Granelli F, Boato G. A novel methodology for analysis of the computational complexity of block ciphers: Rijndael, Camellia and Shacal-2 compared. Technical Report DIT-04-004. Jan. 2004.

Отримано 19.03.2012 р.

 ISSN 1560-8956