УДК 303.732.4

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ОБЛАЧНЫХ ХРАНИЛИЩ НА ОСНОВЕ МЕТОДОВ КЛАССИФИКАЦИИ ДАННЫХ

Л. А. Подколзина, Д. К. Коваленко
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
podkolzinalu@gmail.com
roshtov_don@mail.ru

В статье поднимаются проблемы обеспечения безопасности данных в облачных хранилищах. Проанализированы подходы к организации мобильных облачных хранилищ. Основными аспектами являются вопросы безопасности и хранения информации. Наиболее оптимальным является построение облачных хранилищ с использованием методов классификации, позволяющих с большей эффективностью и безопасностью хранить конфиденциальные данные. Рассмотрены три предлагаемых уровня безопасности данных. Проведен анализ выполненной работы.

Ключевые слова: Mobile Cloud Computing (MCC), классификация данных, облачные хранилища, безопасность облачных мобильных хранилищ.

UDC 303.732.4

MOBILE CLOUD STORAGES SAFETY ON THE BASIS OF DATA CLASSIFICATION OF METHODS

L. A. Podkolzina, D. K. Kovalenko
Don State Technical University
Rostov-on-Don, Russian Federation

podkolzinalu@gmail.com
roshtov_don@mail.ru

The article deals with the problems of data security provision in cloud storages, provides the analysis of approaches to mobile cloud storage organization. The main issues are the security issues and the storage of information. The authors believe that the most optimal way is to build a cloud storage using the classification methods which allow private data storage with more efficiency and security. The article reviews three proposed levels of data security. The authors have carried out the analysis of their work.

Keywords: Mobile Cloud Computing (MCC), data classification, cloud storages, cloud mobile storage safety.

Введение. Облачные сервисы являются успешно развивающейся областью, включающей широкий спектр новых технологий и приложений. Среди понятий, связанных с этой областью, является Mobile Cloud Computing (MCC), которые позволяют пользователям получать доступ и использовать облачные сервисы и приложения с помощью мобильных устройств. Но, как известно, мобильные устройства имеют ряд проблем, ограничивающих их производительность, таких как время работы батареи, отсутствие вычислительных ресурсов и систем хранения. При этом реализация служб облачных систем для мобильных устройств помогает снизить зависимость хранения информации на внешних носителях в дополнение к сокращению эксплуатационных затрат и расходов на обслуживание. В облачных системах данные хранятся на удаленных серверах, что обеспечивает получение доступа к ним через Интернет. Данные могут включать финансовые операции, важные документы и мультимедийный контент. Увеличение объема персональных данных обуславливает повышение внимания к вопросам надежности их хранения. Однако, существующие платформы "облачного" хранилища используют единый размер ключа, чтобы зашифровать все данные. При этом обработка конфиденциальных данных средней и

высокой степени важности одинаковыми способом и на уровнем добавляет ненужные издержки и увеличивает время обработки данных. Хранение данных в «облачных» хранилищах имеет множество плюсов. Они обеспечивают лучшую доступность, например, это дает пользователям возможность доступа к данным с любого устройства, подключенного к интернету [1]. Нет необходимости для пользователей носить устройства хранения с собой, где находится вся информация. Можно использовать любой компьютер для сохранения и получения данных. Это улучшает работу в группах, открывая всем её членам единый доступ к общей информации. В дополнение к этому облачное хранилище снижает расходы на покупку и поддержку дорогих аппаратных средств хранения данных. Также, оно может быть использовано для резервного копирования, архивирования и аварийного восстановления. Более того, данные хранятся на многих серверах, что гарантирует устойчивое обслуживание клиентов, чтобы они могли получить доступ к своим данным в любое время. Несмотря на все преимущества, которые пользователь может получить от облачных сервисов хранения, они все равно имеют свои недостатки. Говоря об общедоступном облачном хранилище, данные уже не «в руках» пользователя, а на удаленных серверах, и этими данными может воспользоваться любой человек в любой точке мира. Удаление файла ещё не означает, что он действительно перестает существовать [2].

Решения облачных сервисов различных компаний. В данной работе проведен анализ методов решения основных проблем, возникающих у пользователя при использовании услуг облачных систем. Первая - это опасения пользователей о совершении внутренних или внешних хакерских угроз. Вторая - невозможность шифрования всех данных, без учета степени её конфиденциальности. Количество представленных облачных сервисов для хранения файлов в интернете быстро растет, к примеру, облачные сервисы: Google Docs, Dropbox, JustCloud, Mozy и Google Drive - все это примеры услуг, которые предоставляют пространство для хранения цифровых данных. Существующее автономное программное обеспечение может зашифровать все данные пользовательской системы, однако у этого есть свои недостатки. Автономное программное обеспечение устанавливают, управляют и работают и на стороне клиента, и на стороне провайдера "облачного" хранилища. Все устройства, у которых есть доступ к данным, должны знать ключ, используемый в его шифровании. В случае если ключ был потерян, дешифрование данных никогда не будет возможно снова. Чтобы предотвратить потерю данных, ключи, используемые для шифрования данных, должны быть объединены в некоторую систему доверительного хранения ключа. Генерация ключей, используемых для шифрования данных, должна быть случайной и гарантировать различие двух шифров того же открытого текста. На 2014 год лишь 194 из 2500 обследованных облачных сервисов, предлагающих услуги хранения данных, удовлетворяют требованиям для решений корпоративного класса. Многие из них несут в себе не только угрозу безопасности, но и проблемы, связанные с законодательством [3]. Рассмотрим несколько мобильных облачных систем. Создатель Seiger и др. предложили SecCSIE – гибкую архитектуру системы под названием SecCSIE, позволяющую подключить различные типы провайдеров "облачного" сервиса к компьютеру сотрудника с обеспечением безопасности данных [4]. Предложенная архитектура универсальна, централизована прокси-сервером, шифрующим все данные и применяющего информационную дисперсию к ним прежде, чем они покинут внутреннюю сеть. Это гарантирует конфиденциальность данных, целостность и доступность. Основная цель этой архитектуры в расширении внутренних ресурсов IT организации, создание доступных и стабильных внешних хранилищ. Они сосредоточены на достижении высшего уровня безопасности помимо превосходного удобства пользования и универсальности. DEPSKY

предложен Bessani как безопасная и надежная система, берущая на себя заботу о повышении доступности, целостности и конфиденциальности хранимой информации путем шифрования, кодирования и репликации данных на разных облаках, образующих «облако в облаке» [5]. Система была реализована на основе используования четырех поставщиков услуг "облачного" хранилища (Amazon S3, Windows Azure, Nirvanix и Rackspace) и PlanetLab для обслуживания клиентов, расположенных по всему миру. В статье Bessani рассмотрены четыре недостатка разных облачных систем:

1) Потеря доступности.
2) Потеря и повреждение данных.
3) Утрата конфиденциальности.
4) Привязка к поставщикам.

Там же дано описание реализации системы DEPSKY на основе использования византийских методов обеспечения отказоустойчивости, криптографии, технологии «облако в облаке», что обеспечивает повышенную работоспособность. CloudSafe был предложен Zhang и др. [6] как система улучшения доступности и конфиденциальности информации в облаке посредством шифрования и кодирования данных в нескольких провайдерах "облачного" хранилища. Чтобы сделать возможным безопасный, надежный и быстрый репозитарий доступа к данным, CloudSafe предлагает кодирование данных между несколькими поставщиками облачных услуг (например, Dropbox, Google Drive, Microsoft SkyDrive и SugarSync). По словам Zhang и др., доступность улучшается из-за использования кодирования стирания для распределения данных по нескольким поставщикам "облачной" инфраструктуры, чтобы обеспечить восстановление доступа к данным, в случае, если провайдер прекратит деятельность. AES был использован для шифрования и дешифрования данных, чтобы сохранить конфиденциальность данных. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding: Безопасное стирание, основанное на коде системного "облачного" хранилища с безопасной передачей данных: Lin и др. [7] предложили пороговую схему перешифрования прокси и объединение ее с нецентрализованным кодом стирания для разработки безопасной распределенной системы хранения, обеспечивающей безопасное и усиленное хранение данных, а так же восстановление. Кроме того, предложенная система хранения позволяет пользователям передавать свои данные к серверу и другим пользователям. Предлагаемая система обеспечивает надежную конфиденциальность и секретность сообщений в хранилище сервера. При повторном шифровании схема повышает количество кодирования операций по зашифрованным сообщениям. Однако каждое из рассмотренных выше решений имеет множество ограничений:

1) Система Seiger и др. требует больше ресурсов, но самая главная проблема в том, что ключи находятся в ведении провайдера и данные могут быть подвержены хакерским атакам. Атаки могут быть осуществлены, когда пользователь отправляет информацию на серверы поставщика услуг или в случае, если хакер ломает передачу протокола безопасности.
2) Bessani и соавт. требует много физических ресурсов, что приводит к росту затрат. Другим недостатком этой системы является небезопасность хранения ключей. Так, ключи могут находиться в ведении множества серверов, что повышает риск атак.
3) Somani и соавт. используют метод шифрования RSA, который является менее безопасным и медленным в шифровании и дешифровании большого объема данных. RSA содержит открытый и закрытый ключ, поэтому управление происходит от третьего лица, что увеличивает риск.
4) Предложенная коллективом авторов Lo’ai Tawalbeh, Nour S. Darwazeh и др. модель

системы безопасного облачного хранилища данных позволяет пользователям шифровать собственные данные, используя ключ, который не доступен для провайдера [8]. В дополнение происходит шифрование базы данных по степени конфиденциальности.

В данной работе под безопасным облачным хранилищем данных понимается модель, шифрующая данные по степени ее конфиденциальности через три уровня: базовый, конфиденциальный и строго конфиденциальный. Предлагаемое решение базируется на идее ручной классификации, которая означает, что пользователь должен будет сам указать уровень конфиденциальности данных.

Мобильное облачное хранилище на основе методов классификации данных. Классификация данных – это процесс, позволяющий организациям и физическим лицам классифицировать различные виды данных и информационные активы по степени конфиденциальности, которая будет определять степень безопасности данных. Классификация производится для гарантии конфиденциальности информации и надлежащей защиты путем низкой защищаемой информации. Данные могут также быть классифицированы в соответствии с тем, как часто они запрашиваемы, т. е. берется критическое значение. Данные с более критическим значением будут храниться на более быстром носителе данных, в то время как менее критичные хранятся на более медленных. Разные алгоритмы шифрования, такие как: безопасный алгоритм хэширования (SHA), улучшенный стандарт шифрования (AES), безопасность транспортного уровня (TLS) и криптографические функции используются в основе уровня безопасности данных. На рисунке 1 представлены три уровня безопасности в данной модели: базовый, конфиденциальный и высоко конфиденциальный уровень.

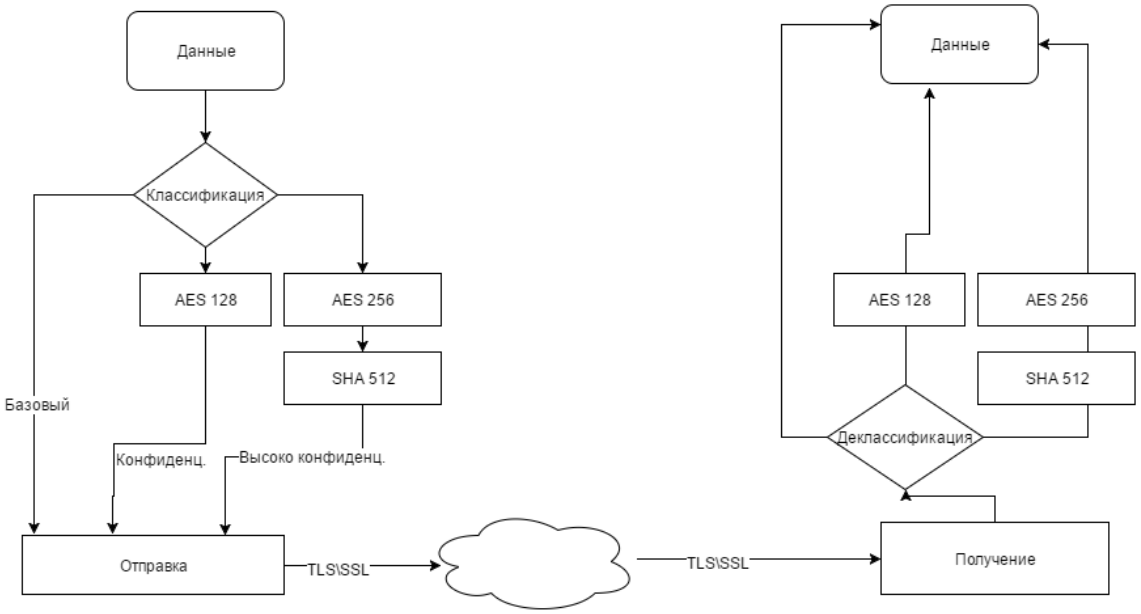

Рис. 1. Базовый, конфиденциальный и высоко конфиденциальный уровень безопасности данных

Базовый уровень: базовый уровень участвует в шифровании общего типа данных (видео и фотографии, для которых не нужна высокая степень конфиденциальности, по мнению пользователя). Следовательно, он реализует базовый уровень безопасности и используется большинством продуктов, доступных онлайн. Для этого рекомендуется использовать TLS для шифрования передачи между приложением клиента и сервером, с использованием HTTPS. TLS гарантирует конфиденциальность связи между пользователями в Интернете. Важно отметить, что данные на базовом уровне безопасности не будут зашифрованы на стороне клиента; они будут

зашифрованы, используя ключ шифрования резервной службы после передачи данных на сторону сервера. Конфиденциальный уровень: Конфиденциальный уровень разработан для данных со средним статусом конфиденциальности персональных файлов, фотографий и видео. На этом уровне шифрование осуществляется на стороне клиента, т.е. это основывается на клиентском шифровании. На конфиденциальном уровне используется AES – блочный алгоритм шифрования симметричного ключа с фиксированным размером блока 128 битов и длиной ключа 128. Математические операции в AES выполнены в 10 раундах для 128-разрядных ключей. Каждый раунд состоит из многократных шагов обработки. Высоко конфиденциальный уровень обрабатывает самые важные данные, например, финансовые операции, данные карт и пр. Поэтому для данной информации предпочтительнее использовать сочетание: алгоритм шифрования AES 256, который также рекомендуется американским агентством национальной безопасности (NSA) для шифрования сверхсекретных данных, чтобы предотвратить несанкционированный доступ; и безопасный алгоритм хеширования SHA 2. Данные алгоритмы гарантируют целостность данных. Они выполняются на данных прежде, чем отправить или загрузить их, вычисляя значение хэш-функции. Когда пользователь получает данные назад, алгоритм вычисляет значение хэш-функции для полученных данных, если значение совпадает с первым тогда, пользователь может быть уверен, что в данные не поступила информация извне.

Заключение. В статье наиболее оптимальным решением является эффективная, основанная на конфиденциальности, платформа "облачного" хранилища, улучшающая время обработки и гарантирующая конфиденциальность и целостность через классификацию данных с применением TLS, AES и SHA на основе типа классифицированных данных.

Библиографический список

1. Wu J, Ping L, Ge X, Wang Y, Fu J. Cloud Storage as the Infrastructure of Cloud Computing, Proceedings of the International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), pp. 380-383, Kuala Lumpur, 22-23 June 2010.

2. Ogigau-Neamtiu F. Cloud Computing Security Issues, Journal of Defense Resources Management, no. 3(2), pp. 141-148, 2012.

3. Николай Смирнов. “Облачные сервисы хранения корпоративного уровня”, журнал “Директор информационной службы”, no.8, 2014. – Режим доступа: http://www.osp.ru/cio/2014/08/13042503/ (дата обращения: 28.04.2016).

4. R. Seiger, S. Groß, A. Schill; SecCSIE: A Secure Cloud Storage Integrator for Enterprises; Proceedings of the 13th IEEE Conference on Commerce and Enterprise Computing (CEC), pp. 252-255, 2011.

5. Bessani A, Correia M, Quaresma B, Andre F, Sousa P. DepSky: dependable and secure storage in a cloud-of-clouds. Proceedings of the sixth conference on Computer systems, April 2011, pp. 31-46.

6. Brindha T, Shaji RS, Rajesh GP. A Survey on the Architectures of Data Security in Cloud Storage Infrastructure. International Journal of Engineering & Technology 2013; no. 5(2), 2013, pp. 1108-1114.

7. Lin H-Y, Tzeng WG. A secure erasure code-based cloud storage system with secure data forwarding. Parallel and Distributed Systems, IEEE Transactions on 2012, no. 23(6), 2012, pp. 995-1003.

8. Lo’ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd AlDosari.

A Secure Cloud Computing Model based on Data Classification, First International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2015), 2015, pp. 1153 – 1158.