ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ СИСТЕМАХ

Шаповалов И.В., Добрынин И.С.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. ТКС, тел. (057) 702-55-92
E-mail: Shapovalovstd@gmail.com

Cloud computing is a fast developing technology in which information is stored and processed on the remote servers. Security of the information, which is stored and processed in cloud systems, is important part of this new technology. According to social analysis, security of the information and trusting to the service providers are the most important problems of cloud computing. This work represents methods of securing data, which is stored in the cloud.

В связи с тем, что в облачных системах вся информация хранится и обрабатывается на стороне провайдера услуг, необходимо обеспечить ее конфиденциальность, целостность и доступность. Очень остро на данный момент стоит вопрос доверия провайдерам облачных услуг, что, в свою очередь, отстраняет многих потенциальных пользователей от использования облачных технологий. В данной работе представлены методы обеспечения конфиденциальности информации, обрабатываемой центром обработки данных (далее ЦОД), а так же управление доступом к данной информации.

На данный момент для защиты информации в ЦОД применяется шифрование, при этом информация шифруется на стороне провайдера. Однако для работы с ней необходимо проихводить обратную операцию – расшифрование. При этом доступ к информации может быть получен посторонними лицами, так как от ЦОД информация передается уже в открытом виде, хотя и с использованием различных протоколов защиты информации. Так же возможены злоумышленные действия со стороны ЦОД. В таком случае злумышленнику не придется проводить сложную атаку, так как вся ключевая информация хранится в датацентрах.

Для предотвращения подобных атак в данной работе предлагается использование посредника. Под посредником будем подразумевать сервер, установленный на стороне клиента, который будет производить шифрование и расшифрование данных.

Принцип работы представленной модели заключается в следующем:

1. Клиент проходит аутентификацию на сервере-посреднике.
2. Клиент при помощи посредника обращается к провайдеру услуг для загрузки информации на виртуальный сервер, расположенний на стороне провайдера.
3. Посредник производит шифрование передаваемых данных. При этом ключевая информация может как храниться на сервере-посреднике, так и выделяться при аутентификации клиента на сервере-посреднике..
4. Зашифрованная информация отправляется на сервер провайдера.

При применении данной модели провайдеру передается уже зашифрованная информация, что предотвращет атаки инсайдеров на хранящуюся в датацентрах информацию. Однако при этом нарушается клиент-серверная модель, от клиента требуются затраты на сервер-посредник Так же, для работы с посредником удаленно, необходима организация защищенного канала между клиентом и сервером-посредником. Применение данной модели целесообразно в случае использования облачных серверов организациями с большим числом пользователей. Однако необходимо помнить, что при увеличении числа пользователей возрастает нагрузка на сервер-посредник. Стоит заметить, что аутентификация производится два раза, первый раз – клиент аутентифицируется на сервере-посреднике, и второй раз – сервер-посредник аутентифицируется на сервере услуг.

Второй метод отличается от первого отсутствием сервера-посредника. При этом используется приложение, встраеваемое в браузер. При этом так же происходит аутентификация в приложении. Принцип работы данной модели практически не отличается от принципа работы предыдущей, за исключением того, что клиент через приложение производит обращения к серверу провайдера. При использовании данной модели отсутствует

необходимость в сервере-посреднике и, соответственно, и в установлении защищенного канала между клиентом и посредником. Однако при использовании данной модели нагрузка ложится на локальные машины клиента. К тому же из-за необходимости аутентификации в приложении необходимо обеспечить репликацию учетных записей с разных клиентских машин. Так же, в отличии от предыдущей модели, в которой аутентификация была централизованной, в данной модели она децентрализованна.

Оба этих метода объеденяет то, что инициатива обеспечения защиты информации исходит со стороны клиента, и провайдер в этом никакого участия не принимает.

Третий метод требует инициативы как от клиента, так и от провайдера услуг. В нем так же используется приложение. Только в данной модели оно не просто производит аутентификацию и шифрование и расшифрование данных. Данное приложение представляет собой API виртуального сервера, с помощью которого происходит аутентификация на самом сервере, а не в приложении, как в предыдущем случае. Шифрование и расшифрование происходит на машине клиента, что позволяет исключить возможность раскрытия конфиденциальной информации злоумышленниками.

Для шифрования информации, передаваемой в ЦОД, в данной модели рекомендуется использование потоковых шифров или блочных шифров в режиме OFB. Эти шифры обеспечивают должную защиту и при этом возможность изменения данных клиентом. При этом ключи шифрования хранятся на машине клиента или, в случае использования сервера-посредника, выделяются из аутентификационных данных. Однако при этом следует учесть, что преобразования аутентификационных данных для выделения ключей должны отличаться от преобразований для проведения аутентификации, а именно – для выделения хэшей для проведения аутентификации, так как в этом случае злоумышленник может получить ключ сразу, не проводя криптоанализа.

Аутентификация в приложении, за исключением API, может выполнятся по принципу простого объявления аутентификационных данных. Для API аутентификация выполняется по протоколу CHAP, Kerberos или другому протоколу, в котором аутентификационные данные не передаются в открытой форме. Метод аутентификации в данном случае выбирает провыйдер услуг. При аутентификации на сервере-посреднике возможна аутентификация при помощи протокола PAP, в том случае, если аутентификация происходит внутри локальной сети организации и не допускает удаленного соединения. В случае удаленного доступа необходима аутентификация, исключающая передачу аутентификационных данных в открытом виде.

Предложенные в работе методы позволяют обеспечить конфиденциальность инфрмации, хранящейся и обрабатываемой в ЦОД. Данные методы предполагают частичный перенос нагрузки с серверов провайдера на сервер-посредник или на рабочие машины клиента. Данные методы слегка отступают от концепции облачных вычислений, которая предполагает, что вся обработка информации происходит на стороне провайдера, однако обеспечиваемая защита данных превосходит появившуюся нагрузку. Использование предложенных методов позволит защитить информацию не только от злоумышленников в сети, но и от самих провайдеров, которые так же могут использовать ее в своих целях. При применении данных методов отпадает вопрос о доверии провайдерам ценной информации, что повысит спрос на их услуги и даст толчек дальнейшему развитию концепции облачных вычислений, так как, обратившись к социальным исследованиям на тему проблем облачных вычислений, можно увидеть, что безопасность и доверие провайдеру облачных услуг стоит там на первых местах.

Литература:

1. Защита и контроль доступа к информации. [Электронный ресурс] / Techdays.com. Онлайн семинары по современным технологиям. – Режим доступа: URL: http://www.techdays.ru/videos/3157.html/ - 08.12.2010г. – Загл. с экрана.