пользователь об этом факте никак не узнает. Данные компаний о заказчиках, счётах, денежных оборотах, хранящиеся в облаке, могут быть подвержены утечке, вследствие чего компании могут оказаться в крайне плохом положении.

В качестве защиты данных в облачном хранилище поставлена задача создать расширение, которое способно шифровать данные при их загрузке в сервис, а также обратная операция – расшифровка данных при скачивании из сервиса. Пользователь задаёт ключ и алгоритм для шифрования. Для создания расширения выбран барузер Chrome, а в качестве сервиса облачного хранилища используется Dropbox. Основным алгоритмом шифрования выбран aes (симметричный алгоритм блочного шифрования), обеспечивающий высокую скорость шифрования данных. В данный момент реализовано:

- Шифрование данных при загрузке на сервис перетягиванием (draganddrop) файлов в облако;
- Расшифровка данных при скачивании с главной страницы сайта;
- Выбор алгоритма шифрования у пользователя;
- Сохранение ключа для шифрования пользователя.

Принцип работы расширения для защиты облака:

- При попытке загрузки в сервис (скачивании из сервиса) данных, запрос на загрузку будет отменён;
- Полученные данные шифруются выбранным алгоритмом шифрования ключом пользователя;
- Формируется запрос отправки/скачивания зашифрованных данных;
- Отправка запроса (загрузка/скачивание данных).

Основные преимущества расширения для защиты облака:

- работа на всех популярных операционных системах, таких как: Windows, Mac, Linux;
- поддержка русского языка – управлять расширением просто, а все функции понятны;
- ключ и алгоритм для шифрования имеется только на стороне клиента, таким образом, третьи лица практически теряют возможность получить доступ к данным пользователя.

Основные недостатки расширения:

- данные шифруются непосредственно перед отправкой или загрузкой, а не на лету. Таким образом необходимо ожидать шифрования(расшифровки) данных, а затем отправку или скачивание, вследствие чего теряется скорость работы с облачным хранилищем;
- программа может работать только в браузере Chrome версии 4.0 и выше.

В дальнейшем необходимо реализовать шифрование данных при загрузке на сервис через форму облачного хранилища, расшифровку данных при скачивании из формы открытого файла, создание вспомогательного окна процесса шифрования.

В целом при совершенствовании расширения необходимо сформировать адаптивность для различных барузеров (IE, Firefox, Opera) и возможность шифрования для других сервисов облачных хранилищ, таких как Google Диск, OneDrive, Яндекс.Диск.

Список использованных источников:

1. Статья Способ удобного шифрования данных в облаке (собственными средствами) // Habrahabr [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/241720/

2. Статья Шифрование данных в облаке, 2016: Исследование Gemalto и Ponemon [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Шифрование_данных_в_облаке

СТАТИСТИЧЕСКИЙ ПОДХОД К УПРАВЛЕНИЮ РЕСУРСАМИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Толкачёв А.В.

Куликов С.С. – к.т.н., доцент

В настоящее время облачная модель поставки и функционирования сетевых приложений и сервисов является доминирующей на рынке и продолжает демонстрировать стабильный рост. Использование методов статистического моделирования для управления ресурсами облачного вычислительного кластера может значительно повысить эффективность функционирования системы и минимизировать накладные расходы на балансировку нагрузки.

Облачные вычисления – подход, при котором ресурсы поставляются в виде услуги, могут быть сданы в аренду и предоставлены пользователям через сеть по запросу. Для максимально эффективной утилизации вычислительных ресурсов активно используются технологии виртуализации. Общая схема облачного вычислительного кластера приведена на рисунке 1.

В рамках одного физического сервера (хоста) при помощи специального программно-аппаратного комплекса (гипервизора) функционирует множество виртуальных машин, выступающих в качестве среды функционирования ПО. Гипервизоры связаны с системой мониторинга, ответственной за динамическое перераспределение нагрузки между физическими хостами. Трансфер виртуальной машины между хостами является достаточно ресурсоёмкой операцией, так как требует дополнительные сетевые ресурсы и вычислительные ресурсы для синхронизации [1]. Управление ресурсами, базирующееся на основе модели статистических предсказаний, позволяет минимизировать накладные расходы на миграцию виртуальных

машин между физическими хостами, избегая преждевременного перераспределения вычислительных мощностей, необходимость в которых обусловлена текущими показаниями мониторинга. Данный подход позволяет давать более объективную оценку текущей нагрузки на вычислительный кластер и предоставлять альтернативные схемы управления ресурсами с учётом наиболее вероятного изменения потребления ресурсов с течением времени [2, 3].

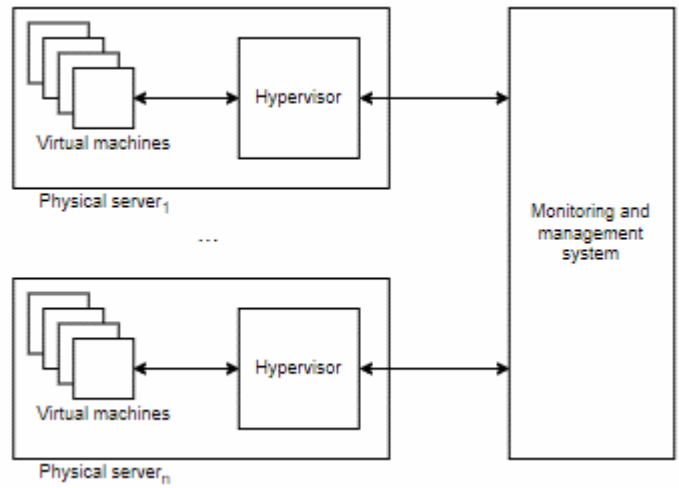

Рис. 1 – Общая схема облачного вычислительного кластера

Использование статистических предсказаний в процессе управления облачными ресурсами так же упрощает соблюдение соглашения об уровне предоставления услуг (англ. ServiceLevelAgreement, SLA). Статистическое планирование использования ресурсов позволяет предварительно резервировать дополнительные вычислительные мощности для поддержания метрик доступности и функционирования сервиса (время доступа, общая доступность и т.п.) на заявленном уровне [2].

Список использованных источников:

1. Ворожцов А.С., Тутова Н.В., Тутов А.В. Динамическое распределение вычислительных ресурсов центров обработки данных // T-COMM: Телекоммуникации и транспорт. – 2016. – Том 10. - №7. – С.47-51

2. Resource Central: Understanding and Predicting Workloads for Improved Resource Management in Large Cloud Platforms. [Электронный ресурс] – Режим доступа: https://www.microsoft.com/en-us/research/publication/resource-central-understanding-predicting-workloads-improved-resource-management-large-cloud-platforms/

3. Michael Borkowski, Stefan Schulte, Christoph Hochreiner Efficient Resource Management Technique for Performance Improvement in Cloud Computing // IEEE/ACM 9th International Conference on Utility and Cloud Computing. – 2016.

ДЕНОРМАЛИЗАЦИЯ КАК СРЕДСТВО УЛУЧШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ БАЗ ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Хадарович П.В.

Медведев С.А. – к.т.н., доцент

В настоящее время количество высоконагруженных приложений неизменно увеличивается. Чтобы справиться с возрастающей нагрузкой, производится либо улучшение аппаратной части машины, обрабатывающей запросы пользователей, либо добавление нескольких новых машин для обработки запросов. Но применение некоторых методов оптимизации производительности баз данных, позволит улучшать аппаратную часть или внедрять новые машины значительно реже. Денормализация является одним из таких методов. При ее грамотном применении, можно существенно увеличить скоростьобработки данных, что в свою очередь, уменьшит время обработки запросов.

Денормализация – намеренное преобразованиеструктуры базы данных в состояние, которое не соответствует критериям нормализации баз данных. Архитектура базы данных, соответствующая критериям нормализации, способствует ее улучшенному пониманию и дальнейшему сопровождению. Но при больших объемах данных, данный подход может существенно снизить производительность обработки данных. В таких случаях, денормализация способна уменьшить время обработки данных.

Применение денормализации имеет смысл тогда, когда происходит потеря производительности по следующим причинам:

- в запросе присутствует слишком много операций объединения таблиц. В таких случаях, производится