Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

УДК 004.056.5

Матюк

Дмитрий Владимирович

Подсистема защищенного удаленного хранения данных для приложений в SaaS-модели

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-31 80 10 Теоретические основы информатики

Научный руководитель

Захаров В. В.

Кандидат технических наук

Минск 2015

Введение

Современные корпорации сталкиваются с бурным ростом объемов данных, необходимых для их повседневной работы. Этот рост вызван потребностью постоянно иметь в пределах досягаемости финансовую, маркетинговую, техническую, статистическую и другую информацию для оперативного реагирования на изменения рыночной ситуации, поведение конкурентов и клиентов.

Для хранения данных применяются различного рода хранилища, сети хранения данных, массивы накопителей на жестких дисках. Организация собственного хранилища, особенно для компании, работающей на большой территории, является затратным мероприятием, требующим не только наличия дорогого оборудования, но и грамотного персонала.

В настоящее время облачные хранилища являются одним из перспективных путей развития информационных технологий. Количество предлагаемых сервисов и их пользователей неуклонно растёт. Облачные хранилища широко используют для хранения частной и корпоративной информации, в том числе и конфиденциальной, что предъявляет определенные требования к обеспечению информационной безопасности таких систем.

Однако, как показывают опросы, 86% IT-специалистов не доверяют облачным хранилищам важные корпоративные данные. Основными причинами недоверия пользователей считаются:

- поставщики облачных услуг стараются свести к минимуму свою ответственность;
- скудность предоставляемой информации о внутренней защищенности;
- отсутствие возможности узнать географическое место положения данных.

Общая характеристика работы

Диссертация посвящена разработке подсистемы защищенного удалённого хранения данных для приложений в SaaS-модели.

В настоящее время облачные хранилища являются одним из перспективных путей развития информационных технологий. Однако, производители, в большинстве случаев, не предоставляют подробной информации об организации защиты хранимой информации, в некоторых случаях пользователям хранилища не предоставляют даже криптографических механизмов для

обеспечения конфиденциальности и целостности их данных, поэтому анализ защищенности конфиденциальных данных в существующих сервисах и предложение путей совершенствования системы защиты является важной научно-прикладной задачей.

Целью диссертационной работы является разработка прототипа подсистемы защищенного удалённого хранения данных отвечающего следующим требованиям:

- подсистема должна быть реализована в виде SaaS-сервиса;
- подсистема должна быть защищена от утери и повреждения данных;
- подсистема должна обеспечить конфиденциальность данных.

Согласно цели диссертационной работы были поставлены следующие задачи:

- анализ современных методов обеспечения информационной безопасности;
- разработать варианты использования системы;
- сформулировать требования к разрабатываемому прототипу;
- разработать API взаимодействия с хранилищем;
- спроектировать архитектуру прототипа системы;
- проанализировать механизмы безопасности системы;
- реализация клиентского приложения, для демонстрации серверного функционала.

Объект: облачные сервисы как хранилища информации.

Предмет: особенности организации и функционирования сервиса, защита данных размещенных на удаленных серверах.

Методы:

- изучение существующей литературы по безопасному хранению данных;
- создание хранилищаданных;
- создание клиентского приложения для демонстрации серверного функционала;
- создание алгоритмов шифрования данных на стороне клиента
- создание APIдля взаимодействия с сервисом.

Содержание работы.Диссертация состоит из введения, четырех глав, заключения, списка использованных источников из 38 наименований, содержит 75 страниц машинописного текста, включая 14 рисунков, 1 таблица, 1 приложение.

В диссертации проводятся анализы:

- существующих подходов по обеспечению одновременной и стабильной работы множества пользователей с минимизацией рисков потери данных;
- современных методов применяющихся для защиты данных.

Проведенные анализы необходимы, для формирования требований к системе. На основании требований к системе выбирается технология взаимодействия с хранилищем и создается спецификация системы.

Реализация системы включает в себя выбор средств разработки и написание сервиса защищенного удаленного хранения данных.

Завершающей частью диссертации является анализ возможных путей развития сервиса.

Заключение

В магистерской диссертации выполнен анализ современных методов применяющихся для защиты данных при передаче, между узлами глобальной сети, и долговременном хранении. Так же был проведен анализ существующих подходов по обеспечению одновременной и стабильной работы множества пользователей с минимизацией рисков потери данных.

На основании проведенных анализов были сформулированы требования к системе и реализован сервис хранения конфиденциальных данных.

Разработанный сервис позволяет хранить конфиденциальные данные в зашифрованном виде. Владелец данных способен управлять доступом к ним, наделяя других пользователей правами доступа. Шифрование информации осуществляется как на стороне клиента, так и на стороне сервера. Создано клиентское приложение демонстрирующее работу сервиса хранения данных.

Перспективным направлением развития защищенности сервиса является выявление аномалий поведения пользователей, для предотвращения несанкционированного доступа третьих лиц к учетным записям. Для реализации данного функционала могут быть использованы нейронные сети. Использование нейронной сети позволит обучать систему индивидуально под каждого пользователя. Аудит действий пользователя в системе должен быть использован в качестве входных данных нейронной сети. Использование нейронной

сети позволяет дообучать ее, адаптируясь под плавные изменения в поведении пользователя.

Так же перспективными направлениями развития сервиса являются:

- разработка функциональности по восстановлению удаленных данных;
- доработка пользовательского интерфейса;
- усовершенствование алгоритмов шифрования данных на стороне клиента;
- усовершенствование алгоритмов генерации криптографических ключей;
- реализовать функционал администратора по управлению пользователями.

Публикации, связанные с темой диссертации:

Захаров В.В., Матюк Д.В. Популярные облачные хранилища и пути повышения их защищенности. Материалы XVII межд. научно-практической конференции «Наука и образование в условиях социально-экономической трансформации общества», г. Минск-2014.