ЛИТЕРАТУРА

1 Уэйншенк Сюзан. 100 главных принципов дизайна / Уэйншенк Сюзан. – Питер, 2013. – 272 с.

УДК 004.056

Студ. Ю. В. Ревинская, К. С. Бердник

Науч. рук. проф. П. П. Урбанович

(кафедра информационных систем и технологий, БГТУ)

РОЛЬ КРИПТОГРАФИИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Изначально криптография использовалась только для безопасного хранения или передачи документов. Сегодня область применения криптографии существенно расширилась. Основные изменения связаны с активным использованием асимметричных алгоритмов шифрования. Симметричное шифрование практикуется в основном для защиты сведений от несанкционированного доступа во время хранения.

Криптографический метод защиты самый надежный, так как охраняется непосредственно сама информация, а не доступ к ней. Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно.

Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма являются криптографически стойкими.

Сегодня на рынке представлено немало продуктов, предназначенных для безопасного хранения конфиденциальной информации с помощью криптографии. Анализ криптографических продуктов лучше всего начинать с реализованных в них алгоритмов шифрования. При этом предпочтение стоит отдавать таким, в которых реализованы известные технологии. Другой важной характеристикой является производительность. Очевидно, что процесс криптографического преобразования информации уменьшает скорость передачи и приема данных сервером и слишком длительные задержки могут привести к определенным трудностям.

Третий момент, на который необходимо обратить внимание при выборе криптографической защиты, связан с ключом шифрования. Значимы три фактора. Во-первых, длина ключа. Во-вторых, необходимо узнать, как именно осуществляется процесс создания ключей. В-третьих, способ хранения ключа шифрования.

При выборе криптографического ПО следует уделить особое внимание компании-разработчику. Практика показывает, что лучше приобретать продукты у известных фирм, которые давно присутствуют на рынке.

В связи с распространением такой информационной системы, как облачное хранилище данных, в котором информация хранится на многочисленных распределенных в сети серверах, первоочередной задачей является защита и сохранность размещенной информации.

Все существующие модели облачных вычислений подразделяется на три основных типа в зависимости от предоставляемого доступа, уровня безопасности и других возможностей: частные, общего пользования и гибридные (рисунок 1).

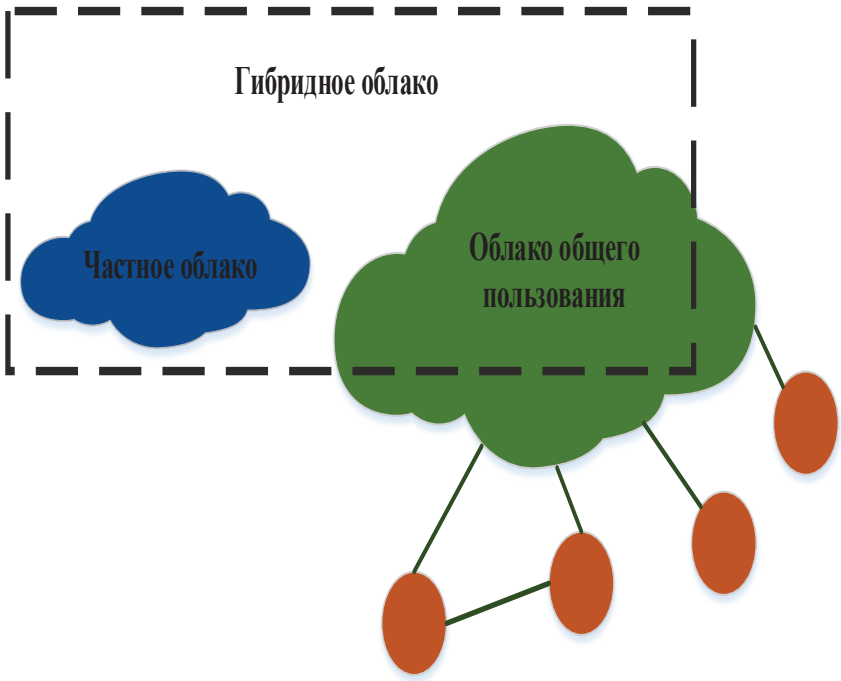

Рисунок 1 - Модели облачных вычислений

Архитектуруоблачныхвычисленийможноразделитьнасервисыинтеграции (IntegrationasaService, IaaS); платформы, предоставляемыеввидесервиса (PlatformasaService, PaaS);

программноеобеспечение, предоставляемоеввидесервиса (SoftwareasaService, SaaS) [1].

На практике ключевым признаком при выборе одного из приведенных уровней облачной архитектуры является безопасность. Рынок облачных сервисов регулярно растет и расширяется, появляются, как и многие уязвимости нового уровня, так и средства защиты. Поэтому для защищаемой системы обычно определяют перечень классов угроз:

– защита периметра и разграничение сети. При использовании облачных вычислений защита более уязвимой части облака определяет общий уровень защищенности;

– динамичность виртуальных машин. Динамичность влияет на разработку целостности системы безопасности;

– уязвимости и атаки внутри виртуальной среды;

– защищенность данных и приложений. В облаке происходит процесс депериметризации. Чтобы сохранить защищенность, методы должны стать информационно-центричными;

– доступ системных администраторов к серверам и приложениям;

– несанкционированный доступ к среде виртуализации. Угроза возможна вследствие нарушения изоляции среды, предоставленной клиенту в рамках облачной услуги;

– защита бездействующих виртуальных машин;

– влияние традиционной безопасности на производительность.

На основе представленных угроз можно привести следующую классификацию основных типов атак [2]:

– традиционные атаки на ПО. Уязвимости операционных систем, модульных компонентов, сетевых протоколов, для защиты которых достаточно установить межсетевой экран, firewall, антивирус, систему предотвращения вторжений (IPS) и другие компоненты;

– функциональные атаки на элементы облака. Для каждой части облака необходимо использовать: для прокси — эффективную защиту от DoS-атак, для веб-сервера — контроль целостности страниц, для сервера приложений — экран уровня приложений, для системы управления базами данных — защиту от SQL-инъекций, для системы хранения данных — бэкапы (резервное копирование), разграничение доступа;

– атаки на клиента. Это такие атаки, как CrossSiteScripting, «угон» паролей, перехваты веб-сессий, «человек посередине» и

многие другие. Наиболее эффективной защитой является правильная аутентификация и использование шифрованного соединения (SSL) с взаимной аутентификацией;

– атаки на гипервизор. Это может привести к тому, что одна виртуальная машина сможет получить доступ к ресурсам другой;

– атака на виртуальные машины при их переносе с одного узла на другой;

– атаки на системы управления. Это может привести к появлению машин-невидимок. Решение: контроль доступа с определенных IP адресов или обязательное подключение через VPN.

Самой популярной моделью облачных вычислений являются SaaS-приложения. Однако такая модель является наименее защищенной в облачной инфраструктуре.Поэтому первоочередной проблемой, которая должна решаться при проектировании систем такого типа — безопасное хранение данных пользователей.

Для комплексного решения предложена концепция построения SaaS-систем, основанная на применении мультиарендной архитектуры с поддержкой версионности баз данных (БД), механизмом безопасной передачи информации между приложением-арендодателем и приложений-арендатором, а также управление доступом на основе токенов, ролей и привилегий.

Данные клиентов сохраняются в реляционной БД с поддержкой технологий внутреннего шифрования. При шифровании используется симметричный ключ, защищенный сертификатом, который хранится в загрузочной записи базы и доступен при ее восстановлении.

При авторизации пользователя в системе отсылается запрос приложению-арендодателю на получение строки подключения к своей БД. Для безопасной передачи данных по незащищенному каналу связи используется алгоритм, основанный на криптографическом протоколе Диффи-Хеллмана и ассиметричном алгоритме шифрования RSA.

Если в рамках функционирования SaaS-системы необходимо сохранять какую-либо информацию в облачном хранилище, то эти данные шифруются с помощью поточного шифра, например,RC4.

Данная концепция универсальна и может быть основой SaaS-системы любой тематики. Защита информации является не разовым мероприятием, а непрерывным процессом. Повышение производительности вычислительной техники и появление новых видов атак на шифры ведет к понижению стойкости известных

криптографических алгоритмов. Таким образом, используемые криптографические средства должны постоянно обновляться.

ЛИТЕРАТУРА

2 Макаров С.А. Облачные вычисления / С.А. Макаров. – Москва: LAP LambertAcademicPublishing, 2012. – 104 с.

3 Безопасность облачных вычислений [Электронный ресурс] / PCmag. – Режим доступа: http://q99.it/nMAhKZo. – Дата доступа 10.04.2017.

УДК 004.921

Студ. А.А Козловский

Науч. рук. проф. П.П.Урбанович

(кафедра информационных систем и технологий, БГТУ)

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ СБОРА, АНАЛИЗА И ИСПОЛЬЗОВАНИЯ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ОСНОВЕ СВЕТОДИОДНЫХ ДИСПЛЕЕВ

В связи с развитием информационных технологий, распространением беспроводного интернета и его доступности, для бизнеса наступила веха развития реализаций бизнес процессов, а также контроль их качества.

Так как у пользователей быстро растут требования к предлагаемым им сервисам, критически важными стали инструменты, позволяющие контролировать предлагаемый продукт, а также уменьшать время отклика от клиента к производителю и наоборот. Наиболее заинтересован в этом бизнес, построенный по модели SaaS – программное обеспечение как услуга, и производства, напрямую связанные с этим бизнесом [1].

С учетом изложенного, предложено решение, позволяющее значительно упростить управление, контроль, а также взаимодействие с клиентом при работе со светодиодными дисплеями. Данные дисплеи в основном используются в рекламных целях. Как правило, это один большой монитор, собранный из большого количества маленьких панелей, подключенных к специальному контроллеру, посылающему им необходимые сигналы (рисунок 1).