УДК 62-529

ИСПОЛЬЗОВАНИЕ ПИРИНГОВЫХ ТЕХНОЛОГИЙ ДЛЯ СОЗДАНИЯ СЕТИ ОТКРЫТЫХ ДАННЫХ С ДАТЧИКОВ

Манаенко В.Н. (Университет ИТМО)
Научный руководитель – к.т.н., Капитонов А.А.
(Университет ИТМО)

Решение задачи доверия к данным, полученным от независимых участников распределенной одноранговой сети. Сценарий построения децентрализованной открытой сети данных от датчиков.

Введение. Потребность в открытой информации возник как ответная реакция с одной стороны на скандалы с утаиванием критичной информации (например, знаменитый скандал с выбросами автомобилей Фольксваген в 2015), а с другой стороны — как желание профессионального сообщество защититься от необоснованной критики и конспирологии (например, утечка переписки климатологов в 2009). В России с 2011 года действует проект «Народный мониторинг», который позволяет людям подключать свои датчики к общей системе. Но такой подход влечет за собой большую нагрузку на центр управления и все ещё не решает озвученную выше проблему. При создании открытой сети независимых участников без единого центра контроля неизбежно возникнет вопрос доверия к данным, публикуемым всеми участниками.

Основная часть. Суть предлагаемого решения представляет собой открытую пиринговую одноранговую сеть, защищенную криптографией и распределенным реестром с одной стороны и автоматикой с другой. Существуют различные сценарии сбора и последующей обработки данных. В данной работе предлагается остановится на сборе экологических данных и данных о погоде. Фундаментом решения проблемы доверия, на наш взгляд, выступает автоматизация сбора данных, то есть минимизация человеческого фактора, и организация связи между автономными устройствами и публичными и защищенными базами данных. Здесь и далее предполагается, что мы работаем с известным датчиком и знаем, как получать с него данные. Предлагаемая схема работы включает в себя одноплатный компьютер и один или несколько датчиков. Компьютер подключен к сети интернет и имеет непрерывный доступ к нему. Данные могут быть собраны по требованию или по установленному расписанию. На одноплатном компьютере установлено программной обеспечение, предлагаемое здесь в качестве решения. При установке ПО, на компьютере генерируется секретный и публичный ключи. В последствии они используются для создания цифровой подписи. На этом этапе мы уже можем отличать от какого датчика были получены данные. Дальше пакет данных упаковывается в распределенное хранилище, в результате мы получаем хеш данных. Как известно, работа хеш функций такова, что при любом изменении исходных данных, получаемый хеш изменяется кардинально. Третьим этапом защиты данных является помещение полученного хеша в распределенный реестр. Это обеспечивает его неизменность во времени, согласно особенностям работы распределенных реестров.

Выводы. Описанная выше схема защиты данных была апробирована на производстве химического препарата. Критическим показателем выступала концентрация активного вещества. Во время производства продукта, из партии выбирался образец, проходил проверки, эти данные попадали в систему защиты данных, хеш публиковался в открытом распределенном реестре и печатался на упаковке. Таким образом, автоматизация на этапе производства и невозможность изменить данные после выпуска продукта повышают доверие будущих клиентов.

Манаенко В.Н. (автор) Подпись

Капитонов А.А. (научный руководитель) Подпись