БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ

Лактионов Е.Г.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Сороко Е.И. – кандидат эконом. наук, доцент

В статье рассмотрена технология биометрической аутентификации пользователя.

Целью работы является повышение эффективности обслуживания клиентов банка.

Для обеспечения надежной защиты пользовательских данных и проводимых операций банки модернизируют способы идентификации личности. На сегодняшний день ими предлагаются не только стандартные средства идентификации пользователя в системе, но и идентификация с помощью биометрических данных. Одним из ключевых методов идентификации пользователя на современных мобильных телефонах является идентификация посредством отпечатка пальца.

В настоящее время распознавание по отпечаткам пальцев выполняется достаточно быстро. Технология настолько усовершенствовалась, что время идентификации измеряется в долях секунды, а количество ложных срабатываний сократилось почти до нулевой отметки. Благодаря биометрии пользователь лично является уникальным ключом к устройству, приложению и безопасности платежей, что и обеспечивает высокий уровень защиты.

Распознавание человека по биометрическим данным – это автоматизированный метод идентификации на основе физиологических (являются физическими характеристиками и измеряются в определённые моменты времени) и поведенческих (представляют собой последовательность действий и протекают в течение некоторого периода времени) черт. Биометрическая аутентификация — это аутентификация пользователя по его уникальным биометрическим характеристикам. К таким характеристикам относятся отпечаток пальца, черты лица и другие.

В качестве двух основных характеристик любой биометрической системы можно использовать ошибки первого и второго рода. В области биометрии наиболее устоявшиеся понятия:

– FAR (False Acceptance Rate) — коэффициент ложного допуска, когда система предоставляет доступ нелигитимному пользователю;

– FRR (False Rejection Rate) — ошибочный отказ в доступе, когда лигитимный пользователь не получает доступ в систему [3].

В некоторых случаях использование биометрической аутентификации может ограничиваться необходимостью приобретения дорогостоящего оборудования. В таблице 1 приведены средние показатели для различных биометрических систем.

Таблица 1 – Характеристики биометрических систем

	Отпечатки пальцев	Геометрия лица	Радужная оболочка глаза
FAR, %	0,001	0,1	0,00001
FRR, %	0,8	7	0,10

Анализируя эти данные, можно придти к выводу, что аутентификация на основе рисунка радужной оболочки глаза является одним из самых надёжных биометрических методов. Безконтактный способ получения данных говорит о простоте использования и возможном внедрении в различные области.

Рассматриваемая система является модулем идентификации клиента банка, который позволяет аутентифицировать пользователя по шаблонам, например, по ПИН-коду или паролю, и с помощью дактилоскопических датчиков, встроенных в мобильные устройства.

При первом запуске приложения система генерирует пару ключей: публичный ключ и приватный ключ, которые помещаются в безопасное хранилище Android Keystore. Далее пользователю необходимо зарегистрироваться в банковской системе посредством ввода логина и пароля выданных банком. После этого клиентское приложение выполняет сетевой запрос на банковский сервер для получения ключа доступа, который будет передаваться в каждом последующем запросе как уникальный идентификатор пользователя. Этот ключ необходимо зашифровать и сохранить в настройках приложения.

Для упрощения идентификации пользователя имеется возможность привязать текущий логин и пароль к отпечатку пальцев пользователя, которые были зарегистрированы в системном Keystore ОС Android. Для привязки отпечатков необходимо перейти в личный кабинет пользователя и воспользоваться опцией “Регистрация быстрого входа”. В этот момент происходит привязка приватного ключа, сгенерированного при запуске приложения, к зарегистрированным ранее в системе отпечаткам.

Таким образом, чтобы получить зашифрованный ключ при последующем входе в приложение и расшифровать его для дальнейшего использования, пользователю не будет необходимо вводить логин и пароль, а будет достаточно лишь подтвердить свою личность посредством считывания отпечатков пальцев с датчиков устройства [10].

После расшифровки ключа приватным ключом, он передается на сервер банковской системы с запросом на данные. Далее система производит проверку на соответствие присланного ключа с ключами, хранящимися в базе данных банка. При обнаружении совпадения, клиентскому приложению возвращаются запрошенные данные.

Ключ доступа имеет ограниченное время жизни. При каждой следующей авторизации банк генерирует новый ключ доступа, тем самым увеличивая защищенность данных от злоумышленников.

Описанная схема идентификации пользователя представлена на рисунке 1.

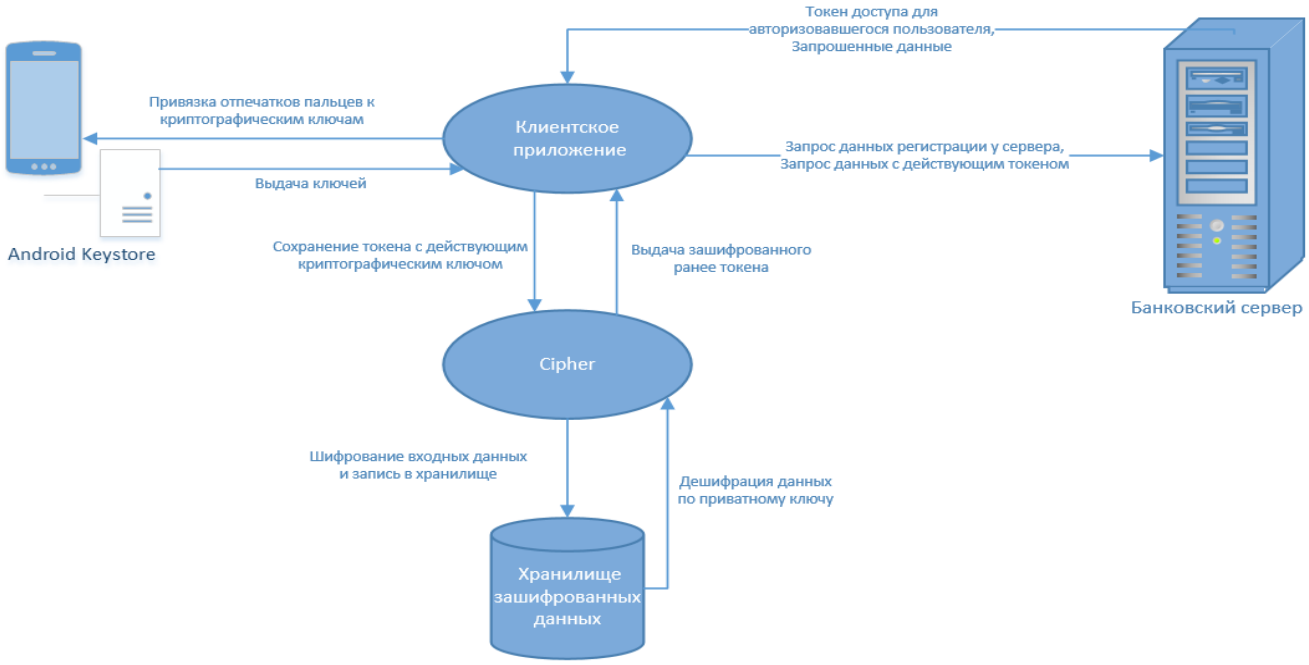

Рисунок 1 - Общая схема процесса идентификации клиента банка

Реализован модуль идентификации клиента банка. Выявлено, что идентификация пользователя посредством сканера отпечатков пальца происходит значительно быстрее, чем идентификация посредством ввода секретных данных. Также пользователю нет необходимости запоминать сложный пароль, поэтому количество ошибок авторизации существенно сокращается, как и сокращается количество запросов в банковские службы на восстановления паролей.

Список использованных источников:

1. Гинце, А. А. Биометрические технологии: мифы и реальность / А.А. Гин-це // Инсайд. – 2005. – № 1. – С. 59–63.

2. Bery, J. The history and development of fingerprinting / J. Bery // Advances in Fingerprint Technology.-1990. – pp. 1-38.

3. Мальцев А.В. Современные биометрические методы идентификации [Электронный ресурс]: [статья] / А.В. Мальцев. – Москва, 2011. – Режим доступа: http://habrahabr.ru/post/126144/