Биометрические системы контроля доступа. Преимущества распределенных систем и облачных решений. Стационарный биометрический комплекс в составе распределенной облачной системы

Махнева О. А.

Махнева Ольга Александровна / Makhneva Olga Aleksandrovna - начальник группы разработки,
отдел программных продуктов,
АО «Ланит Партнер», г. Хабаровск

Аннотация: *в данной статье представлен новый способ построения систем контроля доступа на базе узла биометрического терминала собственной разработки и облачных технологий. Проведен анализ двух типов построения систем контроля доступа, плюсы и минусы каждой из них, а так же обзор технологических решений, количественных и качественных показателей. Выработан способ снижения затрат на создание мощных систем с большим объемом данных за счет двух технологий НОУ ХАУ, увеличивающих мощностные и скоростные показатели системы.*
Ключевые слова: *биометрия, биометрический терминал, СКУД, облачные технологии.*

Вопрос безопасности всегда остро поставлен в обществе. Обеспечение ее с помощью современных систем контроля управления доступом является одним из наиболее востребованных решений. В этой области именно биометрические технологии, а именно распознавание личности по отпечаткам пальцев, сетчатке глаза, лицу, голосу и другие, занимают первое место. К сожалению, данные технологии пока еще не получили достаточного распространения в нашей стране.

При разработке решения авторы ставили следующие задачи:

- разработка стационарного биометрического комплекса, входящего в состав частного облака;
- реализация технологии параллельного использования процессоров;
- виртуальное объединение памяти двух терминалов;
- реализация возможностей по подключению к «облаку» (облачные технологии).

Для создания открытой облачной системы безопасности разработано специализированное оборудование, позволяющее создавать облачные системы безопасности. Для построения узлов облачной сети может быть использовано следующее оборудование:

- узел биометрической идентификации;
- узел кластера системы безопасности;
- узел системы дистанционного контроля и управления.

Узел биометрической идентификации отпечатков пальцев

Для решения задачи быстрой идентификации отпечатков пальцев с использованием туманных технологий создан специализированный биометрический терминал (узел системы безопасности). Технические характеристики биометрического терминала (узла системы безопасности) приведены в таблице 1.

Таблица 1. Технические характеристики биометрического терминала

Параметр	**Значение**
Количество шаблонов отпечатков пальцев	2000
Время распознавания, *t [сек.]*	$t \leq 1$
Время обучения, *t [сек.]*	$t \leq 7$
Количество отпечатков пальцев для 1 пользователя системы	10
Количество терминалов, объединяемых в туманную сеть	не ограничено
Коммуникационные интерфейсы:	
Интерфейс RS485	1
Температура эксплуатации	-20 С +45С

Количество шаблонов отпечатков для одного терминала невелико - это минус. Однако данный терминал и сама биометрическая панель может работать при достаточно низких температурах, что актуально на территории РФ. А поскольку данное решение предполагает создание распределенной вычислительной системы, то показатели количества шаблонов становятся не важными для масштабных и больших систем. Скорость распознавания и количество шаблонов увеличивается с ростом количества терминалов, объединенных в одну сеть.

Для подключения в сеть биометрические терминалы снабжены следующими периферийными интерфейсами:

- Ethernet 100 BaseT;

- CAN BUS

Терминал снабжен специализированным датчиком отпечатков Шведской компании Fingerprints AB [2], который позволяет корректно считывать рисунок папиллярного узора с загрязненной поверхности пальца, сохраняя при этом высокую степень вероятности корректного распознавания.

Состав оборудования и функции основных блоков узла биометрической идентификации показаны в таблице 2.

Таблица 2. Состав и функции основных блоков биометрического терминала

Наименование блока	Функции
Микроконтроллер Texas Instruments Tiva 129TMC	Управление блоками терминала
Оптическое реле	Управление внешними устройствами (электромагнитными замками)
Перепрограммируемое запоминающее устройство	Хранение прикладного кода программы управления узлом биометрической идентификации
Биометрический процессор	Хранение шаблонов отпечатков пальцев, обеспечение процедур биометрической идентификации
Сенсор отпечатков пальцев	Формирование электронного представления рисунка папиллярного узора

Узел биометрической идентификации предназначен для проведения процедур биометрической идентификации с использованием рисунка папиллярного узора пальца. Узел может быть размещен в местах, где требуется ограничение доступа в целях недопущения несанкционированного проникновения на охраняемую территорию. Узел может быть установлен на двери помещения, проходной и т. д. Поскольку в составе узла биометрической идентификации имеются электронные реле, узел может управлять практически любым внешним оборудованием. В частности, к узлу может быть подключены:

- электромагнитные замки;
- электромеханические замки;
- устройства контроля и индикации факта открытия двери.

Поскольку в составе узла биометрической идентификации имеются сетевые интерфейсы Ethernet и CAN, узел может являться частью системы безопасности офисного помещения, жилого дома или промышленной площадки, опасного производственного объекта. При этом возможна реализация следующих функций:

- дистанционное оповещение о фактах прохода (электронная почта, SMS, текстовое сообщение с использованием сервисов социальных и общедоступных сетей);
- размещение протокола о фактах прохода в базах данных;
- дистанционное блокирование отдельных пользователей;
- формирование политики доступа в охраняемую зону, включая указание время прохода, дни недели.
- управлением произвольным внешним оборудованием.

Частным случаем применения вялятся использованием узла биометрической идентификации для построения систем учета рабочего времени. При построении подобной системы не требуется включение в состав системы персональных компьютеров и серверов — функции устройства для хранения данных может выполнять узел системы безопасности, выполненный на базе микрокомпьютера Beagle Bone Black. В составе узла системы безопасности, имеется встроенное программное обеспечение управления базами данных, позволяющее хранить и обрабатывать информацию о пользователях системы, времени прохода через охраняемую точку и т. д. в форме не реляционных баз данных.

Узел кластера системы безопасности

Для развертывания системы разработан специализированный программно-аппаратный узел безопасности. Узел выполняет следующие функции:

- контроль и управление специализированными узлами биометрической идентификации;
- управление административными базами данных пользователей системы безопасности;
- управление внешним оборудованием (реле, датчики и др.)
- кластеризация данных системы безопасности в целях обеспечения отказоустойчивости системы хранения и обработки данных.

Фактически разработанный узел кластера системы безопасности является альтернативой дорогостоящим узлам построенных на базе специализированных серверов. Предлагаемое решение имеет следующие преимущества:

- сниженные требования к потребляемой мощности (максимальное потребление не более 10 Вт);
- уменьшенные размеры узла (120х 170 мм) и вес, допускающие установку практически в любом месте, без необходимости выделения отдельного помещения (серверной комнаты);

- открытое программное обеспечение на основе ядра операционной Debian;
- автоматический встроенный контроль электропитания.

Группа узлов кластера объединяется в кластер системы безопасности и образует облако системы безопасности.

Узел системы безопасности представляет собой разработанную в рамках данной НИР специализированную материнскую плату, на которую устанавливается малогабаритный компьютер Beagle Bone Black [3].

Характеристики компьютера Beagle Bone Black приведены в таблице 3.

Таблица 3. Состав и характеристика блоков компьютера Beagle Bone Black

Наименование блока	**Характеристика**
Микропроцессор Texas Instruments AM335x ARM Cortex A8	Тактовая частота - 1GHz
Flash память	4 Gb
Оперативная память	512 Mb DDR3
Сетевой интерфейс	CANBUS, Ethernet 100BaseT, Serial Port
Входы-выходы общего назначения	40

Узел кластера системы безопасности предназначен для развертывания в составе территориально распределенной системы безопасности и позволяет:

- осуществлять поддержку облачных и туманных вычислений;
- выполнять роль узла биометрической идентификации;
- хранить базу данных пользователей системы биометрической идентификации;
- хранить базу данных оборудования системы безопасности;
- хранить базу данных о событиях системы безопасности (факты нарушения периметра охраны, успешная и не успешная идентификация, срабатывание датчиков охранной и пожарной сигнализации);
- управлять подключенными по сети узлами биометрической идентификации;
- управлять подключенным по сети оборудованием системы безопасности (датчиками охранной и пожарной сигнализации).

Узел кластера системы безопасности может быть использован как основа для построения систем безопасности в любой сфере. Универсальность узла системы безопасности, построенного на базе ARM процессора, обусловлена универсальностью платформы ARM — на базе данной платформы строятся многочисленные системы различных сферах деятельности.

Узел кластера системы безопасности рассматривается, прежде всего, как альтернатива государственным средствам обеспечения безопасности. Как известно государственные структуры пытаются создать системы безопасности, обеспечивающие сохранение жизни и здоровья граждан в масштабах всего государства.

Однако указанные меры по созданию глобальных систем являются низкоэффективными. Главная причина неэффективности существующих систем безопасности — чрезмерная централизация и глобализация технических решений. Что приводит к экстенсивному наращиванию ресурсов для обеспечения безопасности — увеличению количество операторов, осуществляющих слежение за безопасностью, видеокамер, устройств слежения и так далее.

Подобные глобальные решения являются экономически нецелесообразными.

Разработанный комплекс узел кластера системы безопасности позволяет существенно сократить расходы на создание подобных систем, повысить эффективность за счет использования облачных технологий, использования оборудования невысокой стоимости.

Основная идея состоит в использовании принципа децентрализации - дорогостоящее оборудование централизованных центров безопасности, включая центры МЧС, необходимо заменить на децентрализованную распределенную информационную систему, построенную на базе разработанного оборудования. При этом за счет агрегации вычислительной мощности процессоров, объединенных в облаке и туманной сети возможно построение отказоустойчивой системы высокой вычислительной мощности. Невысокая стоимость оборудования, а также поддержка практически всех коммуникационных интерфейсов и стандартов (включая Ethetnet, Wifi, Zigbee и т. д.) позволяет развернуть узлы систем безопасности в жилых, офисных и промышленных помещениях. При этом задача создания единого информационного пространства и распределенной системы безопасности решается с использованием программного обеспечения с открытым исходным кодом, что позволяет использовать программные компоненты распределенной системы любыми производителями аппаратных и программных средств.

Разработанный узел кластера системы безопасности позиционируется как интеграционное устройство, позволяющее на его основе адаптировать в систему безопасности любые датчики охранной,

пожарной сигнализации, датчики состояния окружающей среды (температура, загазованность, уровень радиации и т. д.).

Использование данного устройства имеет еще одно значительное достоинство — применение указанного оборудования в качестве узла системы безопасности позволяет полностью отказаться от создания облачной инфраструктуры, требующей выделения помещений для установки группы серверов.

Концепция туманных технологий поддерживается правительством РФ. 01 июля 2016 года правительство РФ поручило Минкомсвязи и Минпромторгу и другим ведомствам подготовить инфраструктуру «туманных вычислений» (по данным сайта www.rbk.ru [1]).

Реализация концепции туманных вычислений с использование узлов биометрической идентификации

Узлы биометрической идентификации имеют ограничение на количество зарегистрированных на узле пользователей. Текущее ограничение составляет 2000 пользователей. Для преодоления указанных ограничений компанией разработано гибридное устройство, совмещающее в себе функции узла биометрической идентификации и узла системы безопасности. Данное оборудование оснащено 2-мя процессорами биометрической идентификации.

Концепция туманных вычислений предложена компанией Cisco Systems в начале 2000 годов и предполагает использование вычислительной мощности группы устройств, которые размещены на объектах управления и контроля. Основная идея основана на том, что большую часть времени процессоры этих устройств простаивают, поскольку используют ресурсы в течение непродолжительного времени. Однако большое количество недорогих процессоров, размещенных на различных объектах, составляют значительную вычислительную мощность. Неиспользуемая вычислительная мощность может быть направлена на выполнение операций, требующих значительных вычислительных ресурсов. Такой операцией является процедура распределенной биометрической идентификации большой группы людей. При этом вычислительная мощность (процессоры) не собираются в одном центра, образуя облачную структуру, а остаются на месте установки. Каждый из процессоров участвует в выполнении запросов территориально-распределенной биометрической идентификации. Такой способ использования вычислительных ресурсов называется туманной сетью.

Подобное решение дает следующие преимущества:

- минимально возможная стоимость, поскольку развертывание туманной сети не требует организации облака и построения отдельных вычислительных центров.
- высокие показатели отказоустойчивости и живучести, поскольку невозможно вывести из строя систему, размещенную на значительной территории.
- высокие показатели производительности, поскольку в процедуру идентификации одновременно выполняют большое количество вычислительных устройств (биометрических процессоров), работающих параллельно.

Предлагаемая идея распределенной биометрической идентификации с использованием туманной сети имеет недостаток — система требует абсолютно надежных каналов связи, соединяющих узлы туманной сети.

Для преодоления указанного недостатка разработано и создано специализированное устройство, являющееся, по сути, узлом биометрической идентификации без датчика отпечатка пальцев. Устройство позиционируется как узел системы безопасности, в который устанавливаются до 2-х процессоров биометрической идентификации с возможностью идентификации до 4000 пользователей. Узел системы безопасности способен дублировать биометрические данные 2-х узлов биометрической идентификации. Таким образом, система распределенной биометрической идентификации может функционировать в 2-х режимах:

- в режиме туманной сети, режим не требует установки дополнительного оборудования;
- в смешанном режиме облачно-туманной сети, при котором базы данных биометрических терминалов дублируются с использованием дополнительных узлов биометрической идентификации.

Благодаря описанной и реализованной архитектуре решения появилась возможность добиться улучшенных показателей производительности в части:

1. количества отпечатков пальцев в системе,
2. скорости распознавания отпечатков пальцев,
3. безопасности хранения отпечатков пальцев в виде математического представления и отсутствия хранения персональных данных,
4. безопасность решения из-за отсутствия централизованной базы – в случае выхода из строя одного терминала, остальные продолжают работу.

Таким образом, один терминал, который не обладает высокими показателями по сравнению с аналогами, но в составе распределенной вычислительной системы его показатели растут в разы, пропорционально увеличению количества узлов системы. Таким образом, для малых компаний мы сможем добиться недорогого и надёжного решения, а для крупных соответствующих показателей, не

оказывающих влияние на стоимость за счет наращивания мощностей или удорожания технологии. Чем больше требуется терминалов, тем быстрее и большее количество сотрудников они могут обслуживать.

Литература

1. РБК. [Электронный ресурс]. Режим доступа: www.rbk.ru (дата обращения: 24.04.2015).
2. Сайт компании FINGERPRINTS. [Электронный ресурс]. Режим доступа: https://www.fingerprints.com/products/productsarea-sensor (дата обращения: 18.12.2016).
3. Сайт BeagleBone Black, раздел документации. [Электронный ресурс]. Режим доступа: https://cdn-shop.adafruit.com/datasheets/BBB_SRM.pdf (дата обращения: 18.12.2016).