УДК 004.056.53

Хамоков А.А.
Сотрудник
Академия ФСО России
Россия, г. Орел
Мясин К.И.
Сотрудник
Академия ФСО России
Россия, г. Орел

ОПТИМИЗАЦИЯ СИСТЕМЫ КОНТРОЛЯ ИДЕНТИФИКАЦИОННОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ МЕТОДОВ

Аннотация. *В статье рассматриваются биометрическая система контроля доступа в зоны ограниченного доступа, основанная на индивидуальном распознавании лиц. Система верификации, система идентификации внедрены в помощь системе регистрации, в процессе регистрации необходимые данные собираются и обновляются в базе данных, чтобы помочь администратору обновить необходимую информацию. На основе этой обработки разрабатывается интегрированная защищенная система биометрического контроля доступа для зоны ограниченного доступа с приемлемым уровнем безопасности. В этом документе разрабатывается система контроля доступа, которая является эффективной и может должным образом идентифицировать отдельных лиц, а также экономически эффективной.*

Ключевые Слова – биометрия, распознавание лиц, система контроля доступа, верификация, система идентификации.

Annotation. *The article discusses a biometric access control system for restricted access zones based on individual facial recognition. The verification system, the identification system are implemented to help the registration system, during the registration process, the necessary data is collected and updated in the database to help the administrator update the necessary information. Based on this processing, an integrated secure biometric access control system is being developed for a restricted access zone with an acceptable level of security. This document develops an access control system that is efficient and can properly identify individuals, as well as cost-effective.*

Keywords: biometrics, facial recognition, access control system, verification and identification system.

ВВЕДЕНИЕ

Стратегии контроля доступа всегда были необходимостью в университетских городках. Всегда существовала необходимость ограничить доступ к чувствительным зонам и защитить ресурсы и активы в различных сценариях и местах, включая классные комнаты и специальные лаборатории. Мало того, в местных университетах произошли досадные инциденты, такие как кражи, вандализм в отношении имущества кампуса, взлом автомобилей и даже нападение со смертельным исходом. В данной статье представлена многофункциональная централизованная система контроля и управления доступом, использующая радиочастотные технологии и бесконтактные смарт-карты. Безопасность кампусов является основным кандидатом для таких технологий, поскольку природа кампусов обеспечивает легкий доступ к относительно большому количеству людей в одном месте. Предлагаемая система принесет пользу университетам, которые не имеют контроля доступа или развертывают автономную систему

в различных стратегических областях на своей территории. Автономные системы имеют ограничения в своих функциях, и одним из главных недостатков является их неэффективная способность отслеживать лиц, получивших доступ в комнаты, что затрудняет проведение расследований на территории кампуса. Справочное исследование для изучения различных технологий, таких как штрих-коды, QR-коды, Bluetooth, биометрия, RFID, бесконтактные смарт-карты и NFC, было проведено путем обзора соответствующих академических журналов, статей и онлайн-статей о технологиях. Исследования показали, что наилучшей возможной технологией для внедрения является бесконтактная смарт-карта. Основное внимание в этой статье уделяется проектированию и разработке системы централизованного контроля доступа (CAC) для cam-задач, таких как автоматизация посещения лекций, бронирование и планирование залов, а также проверка наличия мест в режиме реального времени. Необходимость принятия стратегий по проверке личности людей в нашем сегодняшнем мире невозможно переоценить. В настоящее время мы живем в эпоху, когда каждый должен быть бдительным и осознавать личность людей в своем окружении. Повторяющиеся проблемы безопасности и угроза фальшивых удостоверений личности в наших школах и обществе требуют от заинтересованных сторон целостного подхода к преодолению этой уродливой тенденции. Кража личных данных и изготовление поддельных документов достигают тревожных уровней во всем мире. Идентификация человека - это деликатное понятие, требующее оптимального рассмотрения на всех уровнях управления. Однако идентификация индивида началась давным-давно, когда людей идентифицировали по именам, племенным знакам, манере, в которой они выглядели, действовали, звучали (низкое ворчание по сравнению с пронзительным), даже по их запаху. Мы понимаем, что многие животные сегодня, например, собаки, зависят от своего носа, чтобы интерпретировать окружающую среду, и это включает в себя распознавание отдельных людей и различных существ. Поэтому

необходимость разработки способа физической идентификации индивида становится важной. Безопасность обеспечивает способ защиты жизни и имущества, гарантируя, что люди и их ценности находятся в безопасности. Следовательно, обеспечение безопасности при прохождении через ворота становится очень важным, чтобы избежать проблем в нашей среде. В отличие от доступа в компьютерную систему или веб-приложение (например, электронная почта), для доступа через ворота требуется разрешение на вход / выход из объекта, такого как здания, лаборатории, склады и т.д. Здесь контроль доступа отвечает не только за аутентификацию и предоставление доступа (что является его основной обязанностью), он включает сбор информации о том, кто и что имело доступ к объекту, когда, по какой причине (если возможно) и когда человек покинул объект и т.д. Таким образом, в этой работе подчеркивается и рекомендуется необходимость надлежащей идентификации пользователя, которому предоставлен доступ к различным объектам, например, больницам, конференц-залам и зонам ограниченного доступа вокруг университетов (например, библиотека, лаборатории, офисы, серверная комната (отдел ИКТ)) и т.д.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

Управление доступом - это структура, которая позволяет эксперту контролировать доступ к зонам и активам в данном физическом объекте или к данным на базе ПК (логическим). Доступ можно подразделить на два типа:

1. Контроль физического доступа может быть адекватным в условиях, когда всем пользователям системы требуется доступ к большинству данных в ней. В условиях, когда не все активы данных в системе должны быть одинаково доступны для всех клиентов, необходим постепенный точный контроль.

2. Логический контроль доступа повышает безопасность, обеспечиваемую физическим контролем доступа, действуя в качестве дополнительной

защиты от несанкционированного доступа к ресурсам системы или их использования. Это также может увеличить контроль физического доступа, обеспечивая включенную точность, поскольку различные клиенты могут выполнять различные функции.

Биометрию можно рассматривать как науку, основанную на точной математике, использующую строгие процессы измерения для определения личности человека; это одна из надежных систем контроля доступа. В отличие от измерения закономерностей физической активности человека, биометрия обнаруживает закономерности в различных особенностях тела. Распознавание голоса и лиц становится таким же популярным, как отпечатки пальцев. Когда вы говорите, что внедрили средства биометрии для того, чтобы физическое лицо имело доступ к вашему дому, офисам и зданиям компании, это означает, что вы внедрили считыватель, который измеряет искажения лица, это означает, что считыватель измеряет искажения лица, изгиб пальцев или голосовые факторы, чтобы инструменты контроля доступа знали, что человек, требующий входа, - это человек с искренним доступом, а не противник. Биометрические системы контроля доступа могут устранить слабые места использования первых двух факторов (имя пользователя и пароль) или просто обеспечить дополнительный уровень безопасности. Некоторые коммерческие отрасли серьезно зависят от биометрии, включая ее как часть 2-факторной аутентификации. Без оговорок я могу сказать, что биометрия - это надежный и незаменимый механизм безопасности для коммерческого и бытового применения, особенно для развитых сообществ и компаний. Биометрические данные могут использоваться различными способами для корректировки характера или потребностей компании или фирмы. Распознавание на ладони - это еще одна форма биометрии. В свете этого в была представлена работа, проделанная над основанной на деталях системой распознавания palmtop для системы автоматического открывания и запирания дверей. Биометрическое распознавание - это развивающаяся и

многообещающая область с большим коммерческим размахом. Это чрезвычайно надежная система идентификации источника, поскольку она основана на том, кто мы есть, а не на том, чем 3 мы обладаем. Эти характеристики уникальны для отдельных лиц, следовательно, могут быть использованы для проверки или идентификации личности. Биометрические данные можно разделить на два класса:

1). Физиологический – распознавание лиц, отпечаток пальца, геометрия рук, распознавание радужной оболочки глаза.

2). Поведенческий – голос, подпись.

Распознавание лиц и голоса. В биометрии системы распознавания лиц и голоса являются одной из новых биометрических мер, они являются самыми безопасными мерами аутентификации, связанными с тем, кем является пользователь (личность пользователя). Для целей сравнения использование PIN-кодов и паролей - это учетные данные для аутентификации, которые известны пользователю, а токены - это учетные данные, которыми владеет пользователь. Каждое лицо имеет множество уникальных ориентиров и узлов, то есть различных точек и высот, составляющих лицевые структуры. Некоторые качества лица, которые оцениваются с помощью программного обеспечения для распознавания лиц, - это расстояние между глазами, ширина носа, глубина глазных впадин, форма скул и длина линии подбородка. Эти узлы, которые измеряются, представлены кодами, известными как отпечаток лица в базе данных. Фреймворки распознавания лиц используют несколько процедур для проверки характеристик человека. Шаги заключаются в следующем:

1. Обнаружение: Получение изображения может быть выполнено путем цифрового сканирования имеющегося паспорта или фотографии или с

помощью цифровой камеры для получения фотографии человека в реальном времени.

2. Выравнивание: Как только система распознавания лиц (FRS) обнаруживает лицо, она определяет положение различных атрибутов лица, таких как голова, расстояние между глазами и носом, размер лица, поза и т.д. голова должна быть повернута на определенный градус в сторону камеры.

3. Представление: FRS преобразует шаблон лица в уникальный код. Этот код присваивает набор цифр шаблону reach, чтобы представлять характеристики лиц, с которыми сталкиваются люди.

4. Сопоставление: сопоставление лиц выполняется с использованием различных размеров изображения, если изображение, загруженное в FRS, выполнено в 3D, а системная база данных содержит 3D-изображения, то проблем с сопоставлением лиц не возникнет. Но некоторые проблемы, с которыми сталкивается база данных FRS, связаны с 2D-визуализацией. Но недавно исследователи нашли решение этой проблемы, преобразовав 3D-изображения в 2D. то есть, когда будет получено 3D-изображение, система будет извлекать и измерять разные точки, например, внутренний слой глаза, внешний слой глаза, кончик носа. Если эти измерения будут сделаны, к нему будет применен алгоритм для преобразования его в 2D-формат. Затем FRS может выполнить действие сопоставления лиц.

РЕЗУЛЬТАТ И ОБСУЖДЕНИЕ

Безопасность, которая была важным аспектом организации, должна восприниматься всерьез. В документе разрабатывается система контроля доступа, которая является эффективной и может надлежащим образом идентифицировать отдельных лиц, экономически эффективной. Была создана новая система аутентификации, которая может проверять, кто и что входит через пропускные ворота, также сотрудник службы безопасности

школьной системы может иметь полную запись в журнале о том, кто входил в школьные помещения / лаборатории и в какое время. Результат, полученный системой, будет более точным, если для конкретного человека будет сохранено больше черт лица. Изображения были записаны в разных положениях, причем у каждого человека было по 5 изображений. Максимальная точность системы достигается, когда контролируются все параметры и количество фотографий составляет не менее 5. Этот результат показывает, что высокая точность системы достигается, если окружающая среда контролируется как при регистрации, так и в точке верификации, и если в системе сохраняется большое количество черт лица.

ЗАКЛЮЧЕНИЕ

Система контроля доступа может принести множество преимуществ многим организациям, в том числе сделать кампус более умным и безопасным пространством. В этом документе обсуждалось, как максимально эффективно использовать данные, собранные системой контроля доступа, для интеграции нескольких полезных функций и сервисов с точки зрения хранимых данных. Тот факт, что система управления основана на Интернете, делает ее очень гибкой, поскольку в систему можно легко включить дополнительные функции. Выбор смарт-карт и использование распознавание лиц в качестве учетных данных пользователя - это не только стратегия безопасности, позволяющая сократить время ожидания, но и позволяющая использовать будущие приложения, требующие безопасных транзакций. Многофункциональная смарт-карта, несомненно, облегчила бы бремя студентов и сотрудников, которым приходится носить с собой несколько разных карт одновременно. Система, однако, по-прежнему довольно проста и поэтому подвержена таким хитростям, как посещаемость прокси -сервера и проблемы с тайлгированием. Для устранения таких недостатков систему можно было бы дополнить распознаванием лиц и биометрией. Цель цель статьи -

обеспечить безопасные средства контроля доступа для организации, и я считаю, что если система будет управляться и использоваться эффективно, жизнь, имущество и школьные помещения будут более защищены.

Использованные источники:

1. Дюк В., Самойленко А. Data mining. Учебный курс. СПб.: Питер, 2001. 368 с.

2. Чубукова И. А. Data mining. М.: Бином, 2008. 384 с.

3. Технологии анализа данных: DataMining, VisualMining, TextMining, OLAP / Барсегян, Куприянов, Степаненко, Холод, Под ред. Барсегяна А. А. 2 изд. СПб.: БХВ-Петербург, 2007. 336 с.

4. Башмаков А. И., Дудко Я. В. Алгоритм обнаружения и анализа нештатных ситуаций // Информатика, вычислительная техника и управление. Ижевск: Системная инженерия. Научно-теоретический журнал, 2015. С. 100-104.

5. Гитис Л. Х. Кластерный анализ в задачах классификации, оптимизации и прогнозирования. М.: МГГУ, 2001. 103 с.

6. Дубровин Б. А., Новиков С. П., Фоменко А. Т. Современная геометрия методы и приложения: учебное пособие для физико-математических специальностей университетов. М.: Наука, 1986. 759 с.

7. Hand D., Mannila H. and Smyth P., 2001. Principles of Data Mining. London: MIT Press. P. 197-201.

Информация о себе: alkham007@mail.ru