ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ / INFORMATICS AND INFORMATION PROCESSES

DOI: https://doi.org/10.23670/IRJ.2024.142.6

РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО БИОМЕТРИЧЕСКИМ ДАННЫМ С ПОМОЩЬЮ ТЕХНОЛОГИИ БЛОКЧЕЙН И КОМПЬЮТЕРНОГО ЗРЕНИЯ

Научная статья

Утеев Г.[1], Гибадуллин Р.Ф.[2,] *
[1] ORCID : 0009-0001-8328-367X;
[2] ORCID : 0000-0001-9359-911X;
[1, 2] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (landwatersun[at]mail.ru)

Аннотация

В данной статье исследуется разработка децентрализованной системы верификации личности на основе биометрических данных с использованием технологии блокчейн и компьютерного зрения. Цель состоит в том, чтобы предоставить надежный и безопасный метод верификации личности, снижая риск идентификационного мошенничества или мошеннических транзакций. Благодаря сочетанию биометрических признаков, таких как распознавание лиц, отпечатков пальцев и сканирование радужки глаза, предлагаемая система способна обеспечивать высокую точность идентификации индивидуумов. Технология блокчейн обеспечивает децентрализацию и неизменяемость, гарантируя, что хранящиеся биометрические данные не могут быть изменены или удалены без согласия. Техники компьютерного зрения применяются для улучшения процесса извлечения и анализа биометрических данных, повышая эффективность и точность системы.

Для реализации системы идентификации личности использовались следующие методы и инструменты: блокчейн технология для децентрализованного и защищенного хранения биометрических данных в виде смарт-контрактов на основе Solidity; алгоритмы компьютерного зрения, такие как сверточные нейронные сети, для извлечения и сравнения биометрических характеристик изображений лиц; библиотека OpenPGP для асимметричного шифрования данных с использованием пары открытых и закрытых ключей; серверная часть на Python с использованием фреймворка FastAPI для обработки запросов и взаимодействия с блокчейном; клиентская часть на JavaScript с применением React для создания клиентского веб-приложения. Разработанное web-приложение совместимо со всеми современными браузерами и может быть легко интегрировано в существующие информационные системы.

Разработана новая децентрализованная система идентификации личности на основе блокчейна, компьютерного зрения и биометрических данных. Создан смарт-контракт на Solidity для надежного хранения зашифрованных биометрических данных в блокчейне Polygon. Реализовано веб-приложение на React и FastAPI для сбора и анализа изображений лиц с использованием библиотек компьютерного зрения. Обеспечена защита конфиденциальности данных при помощи асимметричного шифрования. Проведено комплексное тестирование всех компонентов системы, включая мок-тестирование сервера и смарт-контракта. Система продемонстрировала значительные преимущества по сравнению с альтернативным решением. Доступна демонстрационная версия системы для оценки возможностей идентификации в реальных условиях.

Разработанная в данной статье децентрализованная система идентификации личности на основе блокчейна и биометрических данных обладает рядом значительных преимуществ. Использование смарт-контрактов позволяет надежно и прозрачно хранить биометрические данные пользователей. Применение алгоритмов компьютерного зрения улучшает точность и скорость идентификации. Система обеспечивает высокий уровень безопасности данных благодаря криптографическим методам и контролю доступа. Разработанное решение демонстрирует значительные преимущества по сравнению с существующими системами идентификации. Внедрение системы возможно в различных сферах: финансы, медицина, госуслуги. Это позволит повысить защищенность персональных данных граждан и обеспечить их конфиденциальность. Дальнейшее развитие системы может включать расширение видов биометрических данных, оптимизацию алгоритмов и внедрение новых технологий, таких как Интернет вещей.

Ключевые слова: биометрия, блокчейн, идентификация, компьютерное зрение, децентрализация, криптография, безопасность.

DEVELOPMENT OF THE DECENTRALIZED BIOMETRIC IDENTITY VERIFICATION SYSTEM USING BLOCKCHAIN TECHNOLOGY AND COMPUTER VISION

Research article

Uteyev G.[1], Gibadullin R.F.[2,] *
[1] ORCID : 0009-0001-8328-367X;
[2] ORCID : 0000-0001-9359-911X;
[1, 2] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (landwatersun[at]mail.ru)

Abstract

Introduction. This article investigates the development of a decentralized biometrics-based identity verification system using blockchain technology and computer vision. The goal is to provide a reliable and secure method for identity verification, reducing the risk of identity fraud or fraudulent transactions. Through a combination of biometric attributes such as facial recognition, fingerprint and iris scanning, the proposed system is able to provide highly accurate identification of individuals. Blockchain technology provides decentralization and immutability, ensuring that the stored biometric data cannot be modified or deleted without consent. Computer vision techniques are applied to improve the process of extracting and analyzing biometric data, increasing the efficiency and accuracy of the system.

Materials and Methods. The following methods and tools were used to implement the system of personal identification: blockchain technology for decentralized and secure storage of biometric data in the form of smart contracts based on Solidity; computer vision algorithms, such as convolutional neural networks, for extraction and comparison of biometric characteristics of face images; OpenPGP library for asymmetric data encryption using a pair of public and private keys; server part on Python using FastAPI framework for processing of requests and in-application processing. The developed web-application is compatible with all modern browsers and can be easily integrated into existing information systems.

Results. Developed the new decentralized personal identification system based on blockchain, computer vision and biometric data. Created the smart contract on Solidity to securely store encrypted biometric data in the Polygon blockchain. Implemented a web application on React and FastAPI to collect and analyze facial images using computer vision libraries. Data confidentiality was protected using asymmetric encryption. Comprehensive testing of all components of the system, including mock testing of the server and smart contract was performed. The system demonstrated significant advantages compared to the alternative solution. The demo version of the system is available to evaluate the identification capabilities in real conditions.

Discussion and Conclusions. The decentralized personal identification system based on blockchain and biometric data developed in this paper has a number of significant advantages. The use of smart contracts allows reliable and transparent storage of users' biometric data. The use of computer vision algorithms improves the accuracy and speed of identification. The system provides a high level of data security due to cryptographic methods and access control. The developed solution demonstrates significant advantages over existing identification systems. Implementation of the system is possible in various spheres: finance, medicine, public services. It will increase the security of citizens' personal data and ensure their confidentiality. Further development of the system may include expansion of biometric data types, optimization of algorithms and introduction of new technologies, such as the Internet of Things.

Keywords: biometrics, blockchain, identification, computer vision, decentralization, cryptography, security.

Введение

Современное общество с каждым днём становится всё более технологичным и цифровым. Важнейшим аспектом этого процесса является вопрос идентификации личности. Традиционные методы идентификации, такие как пароли, PIN-коды и документы, уже не обеспечивают достаточный уровень безопасности и могут быть подвергнуты мошенничеству. В связи с этим возрастает интерес к разработке новых, более надёжных и удобных методов идентификации.

Одним из таких методов является идентификация на основе биометрических данных. Биометрия представляет собой измерение и анализ уникальных физиологических или поведенческих характеристик человека. Биометрическая идентификация обеспечивает высокий уровень надежности и удобства, однако существующие системы обработки и хранения биометрических данных сталкиваются с проблемами безопасности, приватности и масштабируемости.

В последние годы активно развиваются блокчейн технологии, которые позволяют создавать децентрализованные, безопасные и неподконтрольные единому участнику системы. Блокчейн способен обеспечить надёжное и прозрачное хранение данных, что делает его перспективным инструментом для применения в системах идентификации на основе биометрии [1], [2].

Также растёт значимость компьютерного зрения, представляющего собой область искусственного интеллекта, способную обрабатывать и интерпретировать изображения и видео. Применение компьютерного зрения позволяет улучшить качество и точность биометрической идентификации, тем самым обеспечивая более надежное и быстрое распознавание личности.

Целью исследования является разработка децентрализованной системы идентификации личности на основе биометрических данных с использованием технологии блокчейн и компьютерного зрения для обеспечения высокой надежности и безопасности верификации личности, снижая риск идентификационного мошенничества и мошеннических транзакций.

Для достижения цели ставятся и решаются следующие задачи:

1) изучение и анализ существующих технологий биометрической идентификации и блокчейна;

2) разработка архитектуры системы, обеспечивающей децентрализованное хранение и безопасную обработку биометрических данных;

3) применение алгоритмов компьютерного зрения для обработки и анализа биометрических данных;

4) тестирование и оценка эффективности разработанной системы в сравнении с существующими решениями.

Новизна исследования заключается в создании децентрализованной системы идентификации личности, которая интегрирует технологии блокчейна и компьютерного зрения для повышения безопасности и эффективности идентификации личности.

Традиционные биометрические системы, такие как системы распознавания отпечатков пальцев и распознавания лиц, используемые в смартфонах (например, Touch ID и Face ID от Apple) [3], [4]. Эти системы обычно зависят от централизованного хранения данных, что потенциально увеличивает риск утечки данных при взломе централизованной базы данных. Системы единого входа (Single Sign-On, SSO) [5], [6], такие как Google Sign-In или

Facebook Login, которые упрощают процесс аутентификации для пользователей за счет использования одних и тех же учетных данных для доступа к различным сервисам. Несмотря на удобство, эти системы также подвержены риску централизованного хранения данных и проблемам приватности. Системы цифровой идентификации на основе блокчейна, такие как Estonia's e-Residency. Хотя эти системы используют блокчейн для обеспечения децентрализации и безопасности, они могут не в полной мере реализовывать возможности биометрической верификации и часто фокусируются на удостоверениях личности, а не на биометрических данных. Предлагаемый подход выделяется использованием блокчейн-технологии не только для децентрализованного хранения идентификационных данных, но и для управления доступом к биометрическим данным с помощью смарт-контрактов. Это обеспечивает: высокий уровень безопасности и приватности благодаря децентрализации и криптографическому шифрованию, биометрические данные защищены от несанкционированного доступа и утечек. Смарт-контракты позволяют пользователям самостоятельно управлять кто и в каких условиях может получить доступ к их биометрическим данным, обеспечивая при этом гибкость и автономию.

Таким образом, в отличие от существующих систем, предложенный подход обеспечивает дополнительный уровень защиты биометрических данных за счет децентрализации хранения и использования смарт-контрактов для контроля доступа к данным.

Материалы и методы

Биометрическая идентификация личности – это процесс распознавания индивидуальных особенностей человека на основе его физиологических или поведенческих характеристик. Биометрия позволяет создавать уникальные и надежные методы идентификации, обеспечивающие высокий уровень безопасности и минимизацию возможности подделки или кражи данных [7], [8].

Существует множество видов биометрических данных, которые могут быть использованы для идентификации личности, и они делятся на две основные категории: физиологические и поведенческие.

Физиологические биометрические данные:

1. Отпечатки пальцев: этот вид биометрии является одним из самых известных и широко распространенных. Отпечатки пальцев представляют собой уникальный рисунок папиллярных линий на подушечках пальцев, который не повторяется у разных людей и даже у близнецов. Системы распознавания отпечатков пальцев используются для контроля доступа, аутентификации в смартфонах и других устройствах.

2. Распознавание лица: технология распознавания лица анализирует уникальные черты лица, такие как форма и размер глаз, расстояние между глазами, форма и размер носа, контуры скул и рта. Распознавание лица используется в смартфонах, системах безопасности и контроля доступа, а также в области социальных сетей для автоматической маркировки фотографий.

3. Распознавание радужки глаза: радужка глаза – это цветная часть глаза, окружающая зрачок. У каждого человека радужка имеет уникальный узор, который не изменяется со временем и не зависит от внешних факторов. Распознавание радужки глаза считается одним из самых надежных видов биометрической идентификации и используется в сфере безопасности, контроля доступа и паспортного контроля.

4. Распознавание сетчатки: сетчатка – это тонкая пленка на задней стенке глаза, содержащая светочувствительные клетки. Кровеносные сосуды, расположенные внутри сетчатки, образуют уникальный узор, который может быть использован для идентификации личности. Распознавание сетчатки является одним из наиболее надежных и точных методов биометрической идентификации, однако его применение ограничено из-за необходимости специализированного оборудования и процесса считывания, который может быть некомфортным для пользователя.

5. Геометрия руки и лица: этот вид биометрии анализирует форму, размер и пропорции кисти руки или лица человека. Геометрия руки может использоваться для контроля доступа в зданиях, а геометрия лица может применяться в комбинации с другими методами распознавания лица.

Поведенческие биометрические данные:

1. Динамика почерка: этот вид биометрии анализирует особенности почерка человека, такие как форма и размер букв, наклон, скорость, давление письма и другие характеристики. Динамика почерка может использоваться для идентификации авторства документов и подписей.

2. Голосовая идентификация: голосовая биометрия определяет уникальные характеристики голоса человека, такие как тембр, высота, скорость и интонация. Голосовая идентификация может быть использована в телефонных системах, виртуальных помощниках и системах безопасности.

3. Распознавание походки: этот вид биометрии анализирует уникальные характеристики ходьбы человека, включая скорость, длину шага, угол наклона тела и общую динамику движений. Распознавание походки может применяться в системах видеонаблюдения и безопасности.

4. Динамика нажатия клавиш: эта биометрическая методика изучает особенности ввода данных с использованием клавиатуры, такие как скорость набора, сила нажатия клавиш и последовательность нажатий. Динамика нажатия клавиш может использоваться для аутентификации пользователей в онлайн-сервисах и системах безопасности.

5. Методы взаимодействия с сенсорными устройствами: этот вид биометрии оценивает способы, которыми пользователь манипулирует сенсорными устройствами, такими как смартфоны или планшеты. Данный вид биометрии может быть использован для аутентификации в мобильных.

Каждый из этих видов биометрических данных имеет свои преимущества и недостатки, а также специфические области применения. Важно отметить, что комбинированный подход, включающий несколько видов биометрических данных, может значительно повысить надежность идентификации и уменьшить вероятность подделки или обмана системы [9]. В таблице 1 представлены основные преимущества и недостатки использования биометрической идентификации.

Таблица 1 - Преимущества и недостатки биометрических систем

DOI: https://doi.org/10.23670/IRJ.2024.142.6.1

Преимущества	Недостатки
Уникальность: биометрические данные, такие как отпечатки пальцев, радужка глаза, сетчатка и голос, являются уникальными для каждого человека, что делает их надежным средством идентификации.	Проблемы с приватностью: сбор и хранение биометрических данных может вызвать опасения в области защиты личной информации, поскольку эти данные являются уникальными и неизменными характеристиками индивида.
Трудность подделки: биометрические данные сложнее подделать или скомпрометировать по сравнению с традиционными методами идентификации, такими как пароли или ID-карты.	Возможность ошибок: хотя биометрические системы имеют высокий уровень точности, они также могут быть подвержены ошибкам, таким как ложные отклонения (когда законный пользователь не проходит идентификацию) или ложные принятия (когда неавторизованный пользователь проходит идентификацию).
Удобство: биометрическая идентификация обычно требует меньше времени и усилий со стороны пользователя, поскольку не требует запоминания паролей или носить с собой физические удостоверения личности.	Технические сложности: разработка и внедрение биометрических систем требует сложного оборудования и алгоритмов, что может увеличить затраты и время на их разработку и внедрение. Некоторые биометрические системы могут требовать специализированного оборудования для считывания данных, ограничивая их применение.
Большая точность: биометрические системы идентификации обеспечивают высокий уровень точности при сравнении биометрических данных, что снижает вероятность ложного срабатывания системы.	Влияние внешних факторов: некоторые биометрические системы могут быть чувствительными к внешним факторам, как освещение, температура или уровень шума, что может влиять на их точность и надежность.

При разработке и внедрении децентрализованной системы идентификации личности на основе биометрических данных, блокчейн и компьютерного зрения, важно учесть все эти преимущества и недостатки, чтобы создать надежную, безопасную систему идентификации.

Блокчейн является фундаментальным аспектом реализации децентрализованной системы (рис. 1) идентификации личности по биометрическим данным. Данная технология представляет собой децентрализованную, распределенную базу данных, которая состоит из блоков, содержащие информацию о транзакциях или событиях. Блоки связаны друг с другом криптографически, образуя цепочку блоков.

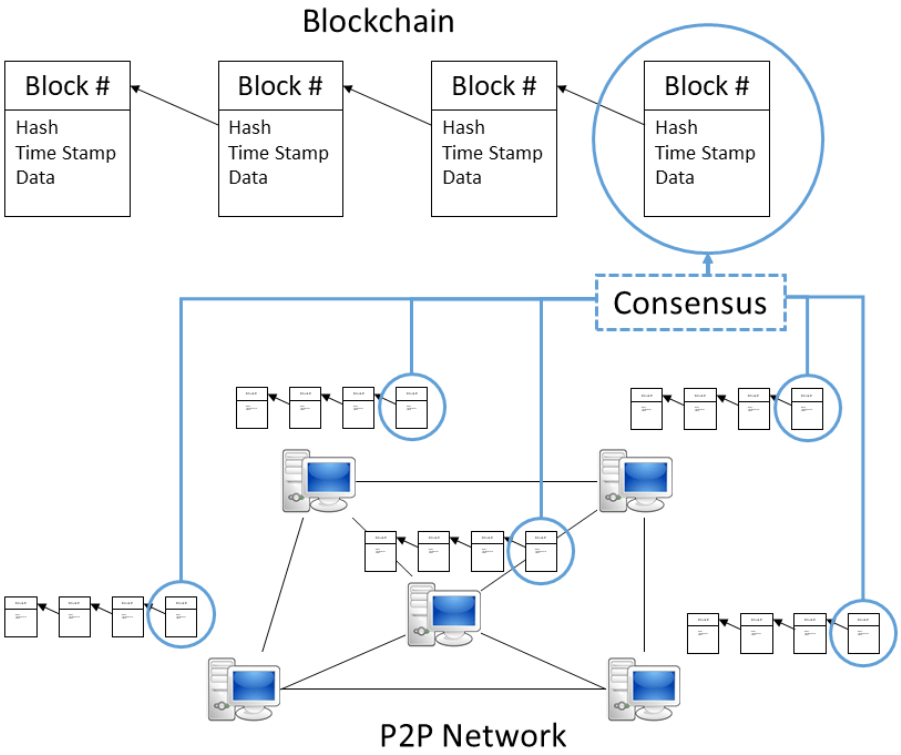

Рисунок 1 - Работа децентрализованной сети
DOI: https://doi.org/10.23670/IRJ.2024.142.6.2

Блокчейн идеален для идентификации личности из-за отсутствия центрального управления, устойчивости к атакам и гарантированной неизменности данных без согласия всех участников. Все транзакции публичны и верифицируемы. Данные защищены криптографией, что гарантирует безопасность, а биометрическая информация, такая как отпечатки и голос, может быть зашифрована и хранится в блокчейне [10].

Компьютерное зрение играет ключевую роль в реализации децентрализованной системы идентификации личности по биометрическим данным. Оно обеспечивает возможность обработки и анализа изображений и видео, содержащих биометрическую информацию, и использует эту информацию для идентификации личности с высокой точностью и скоростью. Кроме того, применение компьютерного зрения позволяет обеспечить безопасность и конфиденциальность данных, а также адаптироваться к изменяющимся условиям и потребностям пользователей.

Рассмотрим механизмы компьютерного зрения, которые используются в рамках данной научной работы для обработки и анализа биометрических данных.

Каскады Хаара – это алгоритм обнаружения объектов на изображениях, основанный на использовании признаков Хаара [11]. Он широко применяется для распознавания лиц на изображениях и видео, благодаря своей скорости и эффективности.

Scale-Invariant Feature Transform (SIFT) – это алгоритм извлечения и сопоставления ключевых точек, который обеспечивает инвариантность масштаба, вращения и изменения освещенности. SIFT может быть применен для сравнения отпечатков пальцев и других текстурных признаков [12].

Speeded-Up Robust Features – это улучшенная версия алгоритма SIFT, которая обеспечивает более быстрое извлечение и сопоставление ключевых точек с сохранением инвариантности масштаба и вращения [13].

Histogram of Oriented Gradients (HOG) – это метод извлечения текстурных признаков, основанный на анализе гистограмм направленных градиентов. HOG может быть использован для анализа изображений лиц, отпечатков пальцев и других текстурных объектов [14].

Глубокое обучение и сверточные нейронные сети (convolutional neural networks, сокращенно CNN) – это класс алгоритмов машинного обучения, основанный на применении сверток и пулинга для извлечения иерархических признаков изображений. CNN широко используются в задачах компьютерного зрения, таких как распознавание объектов, классификация изображений и семантическая сегментация [15].

Трансформеры и архитектура Vision Transformer – это модели машинного обучения, основанные на механизме внимания [16]. ViT – это разновидность трансформеров, разработанная специально для задач компьютерного зрения. Они показали высокую эффективность в распознавании объектов, сегментацию изображений и других задач. ViT может быть использован для извлечения и сопоставления биометрических признаков, таких как лица, отпечатки пальцев и голосовые характеристики.

Optical Flow – это метод оценки движения объектов на видео путем анализа изменения яркости пикселей между кадрами [17]. В контексте биометрической идентификации Optical Flow может быть использован для анализа движений губ и голосовых характеристик в процессе говорения.

В рамках данной работы комбинация этих алгоритмов и методов компьютерного зрения позволяет обеспечить высокую точность в задачах идентификации.

Архитектура предлагаемой децентрализованной системы идентификации личности по биометрическим данным с использованием блокчейн и компьютерного зрения состоит из трех основных узлов:

1. Узел смарт-контракта (Smart-Contract Solidity) отвечает за хранение зашифрованных персональных данных пользователей в блокчейн. Смарт-контракты обеспечивают надежное и безопасное хранение данных, а также контроль доступа к ним. Доступ к узлу смарт-контракта имеет только сервер, что обеспечивает дополнительный уровень защиты данных.

2. Узел сервер (FastAPI Python) отвечает за обработку запросов от клиентов, взаимодействие с базой данных и идентификацию пользователей на основе биометрических данных. Сервер использует компьютерное зрение для анализа и распознавания лиц, а также взаимодействует с узлом смарт-контракта для получения и обновления данных. FastAPI обеспечивает быстродействие и высокую производительность серверной части системы.

3. Узел клиент (JavaScript React) представляет собой веб-приложение, в котором пользователи вводят свои биометрические данные и PIN-коды. Здесь происходит шифрование данных и генерация публичных и приватных ключей на основе лица и PIN-кода для взаимодействия с данными (шифрование и дешифрование). Пользователи могут также выдавать или отзывать доступ к своим данным для различных компаний и организаций через узел клиент.

Такая архитектура системы, изображенная на рисунке 2, позволяет разделить ответственность между разными узлами и обеспечить надежную, безопасную и эффективную работу системы идентификации.

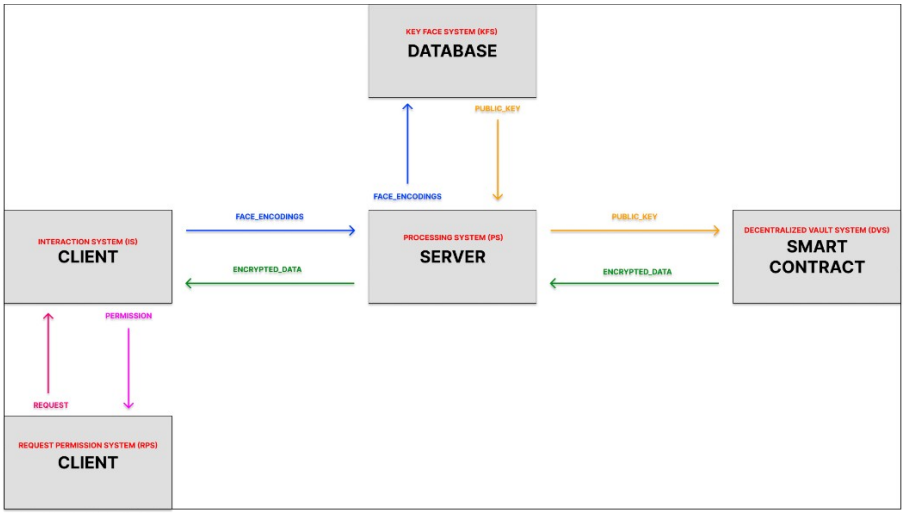

Рисунок 2 - Архитектура взаимодействий отдельных систем

DOI: https://doi.org/10.23670/IRJ.2024.142.6.3

Разделение архитектуры на три узла позволяет легко масштабировать и модифицировать каждый из узлов независимо друг от друга, что облегчает обновление системы и добавление новых функций. Кроме того, децентрализация системы через блокчейн обеспечивает прозрачность и контроль над данными, что является важным аспектом для пользователей и организаций.

В рамках предлагаемой системы идентификации личности были использованы следующие библиотеки для разработки алгоритма идентификации на основе компьютерного зрения:

1. На клиенте (React): библиотека face-api.js была использована для обработки биометрических данных пользователя в виде изображений лица (рис. 3). Face-api.js является набором инструментов компьютерного зрения, основанных на TensorFlow.js, который предоставляет функции для распознавания лиц, определения ориентации лица, обнаружения ключевых точек лица и генерации дескрипторов лица для сопоставления и идентификации.

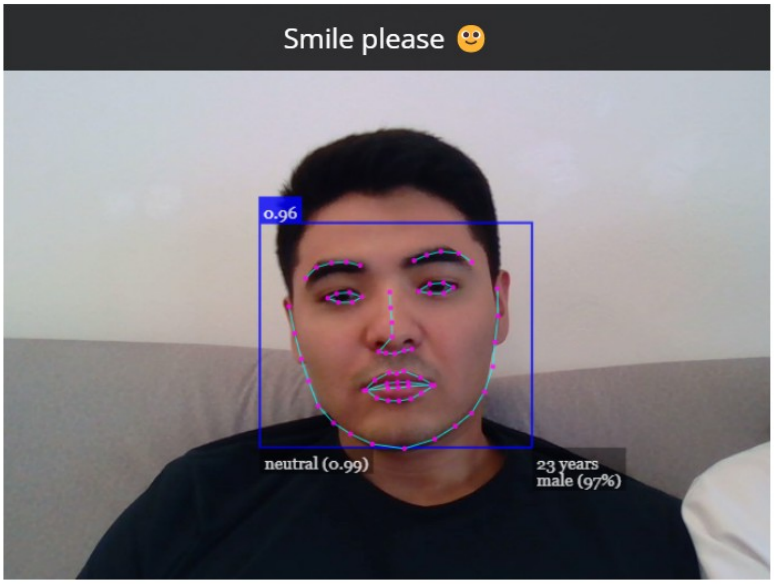

Рисунок 3 - Работа библиотеки face-api.js
DOI: https://doi.org/10.23670/IRJ.2024.142.6.4

2. На сервере (FastAPI): библиотека face-recognition была использована для обработки и сравнения биометрических данных, полученных от клиента. Face-recognition является высокоуровневой библиотекой на языке Python, которая облегчает работу с функциями распознавания лиц и предоставляет инструменты для обучения, сравнения и идентификации лиц на основе изображений [18].

На клиенте с помощью face-api.js пользовательское изображение лица обрабатывается, определяются ключевые точки лица и генерируется дескриптор лица. Этот дескриптор лица затем шифруется с использованием публичного и приватного ключа, созданных на основе лица и PIN-кода пользователя. Зашифрованный дескриптор лица и публичный ключ отправляются на сервер FastAPI для дальнейшей обработки и сопоставления.

На сервере с использованием библиотеки face-recognition дескрипторы лиц пользователей извлекаются из базы данных блокчейна и сравниваются с полученным зашифрованным дескриптором лица от клиента. Если выявляется совпадение, сервер идентифицирует пользователя и предоставляет доступ к соответствующим данным или сервисам, соблюдая необходимые меры безопасности и приватности. В случае успешной идентификации сервер отправляет подтверждение обратно на клиентскую сторону, где пользователю предоставляется доступ к запрашиваемым данным или функциям.

Важным аспектом разработки системы является обеспечение безопасности и приватности пользовательских данных. В рамках системы были приняты следующие меры для защиты информации:

1) использование библиотеки OpenPGP на клиентской стороне (React) для шифрования пользовательских данных с помощью асимметричного шифрования на основе публичных и приватных ключей обеспечивает безопасную передачу данных между клиентом, сервером и смарт-контрактами;

2) публичные и приватные ключи генерируются на основе лица и PIN-кода пользователя. Это позволяет пользователям самостоятельно контролировать доступ к своим данным, поскольку только они обладают необходимой информацией для расшифровки данных.

Зашифрованные данные пользователя хранятся на смарт-контракте в блокчейн, что обеспечивает их децентрализованное и надежное хранение, данные остаются неприкосновенными и не могут быть изменены без соответствующих разрешений (рис. 4).

Рисунок 4 - Визуализация хранения данных на смарт-контракте
DOI: https://doi.org/10.23670/IRJ.2024.142.6.5

В случае необходимости предоставления доступа к своим данным другому пользователю, исходный пользователь может зашифровать свои данные с использованием публичного ключа получателя. Таким образом, только получатель сможет расшифровать данные с помощью своего приватного ключа, что обеспечивает конфиденциальность информации и контроль над ее распространением.

Серверная часть системы (FastAPI) также обеспечивает безопасность обработки и передачи данных между клиентами и смарт-контрактами, используя соответствующие механизмы аутентификации, авторизации и шифрования [19].

Таким образом, предлагаемая система идентификации личности направлена на обеспечение высокого уровня безопасности и приватности пользовательских данных, благодаря использованию асимметричного шифрования, генерации ключей на основе биометрических данных, децентрализованного хранения информации в блокчейне и контролируемому пользователем доступе к данным.

Результаты исследования

Для обеспечения децентрализованного хранения и обработки биометрических данных на языке программирования Solidity был создан смарт-контракт, предназначенный для работы в сети Polygon.

Сеть Polygon была выбрана в качестве платформы блокчейна из-за своих преимуществ, таких как низкие комиссии, высокая скорость транзакций и возможность масштабирования. Регистрационный идентификатор смарт-контракта изображен на рис. 5. Эти характеристики делают Polygon подходящей для разработки и реализации системы идентификации личности на основе блокчейна.

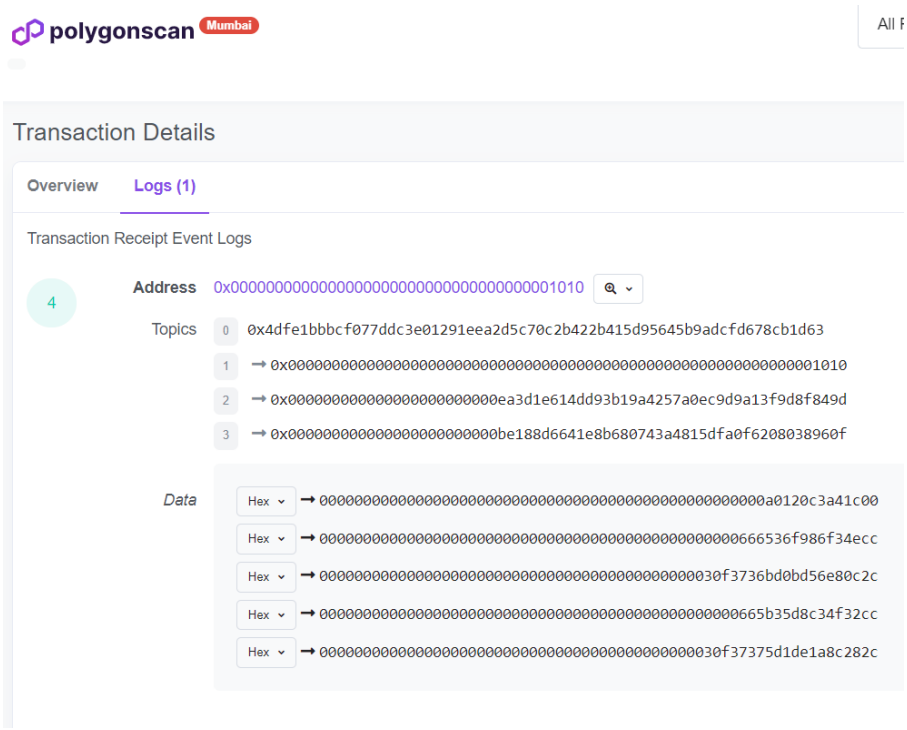

Рисунок 5 - Регистрация смарт-контракта в сети Polygon
DOI: https://doi.org/10.23670/IRJ.2024.142.6.6

В системе реализовано хранение зашифрованных биометрических данных пользователей (изображения лиц и отпечатки пальцев), а также связанных с ними метаданных, таких как хэши и публичные ключи (рис. 6).

Рисунок 6 - Пример хранения зашифрованных данных в Polygon
DOI: https://doi.org/10.23670/IRJ.2024.142.6.7

Созданы функции для добавления, обновления и удаления пользовательских данных с соответствующими механизмами контроля доступа и аутентификации (рис. 7).

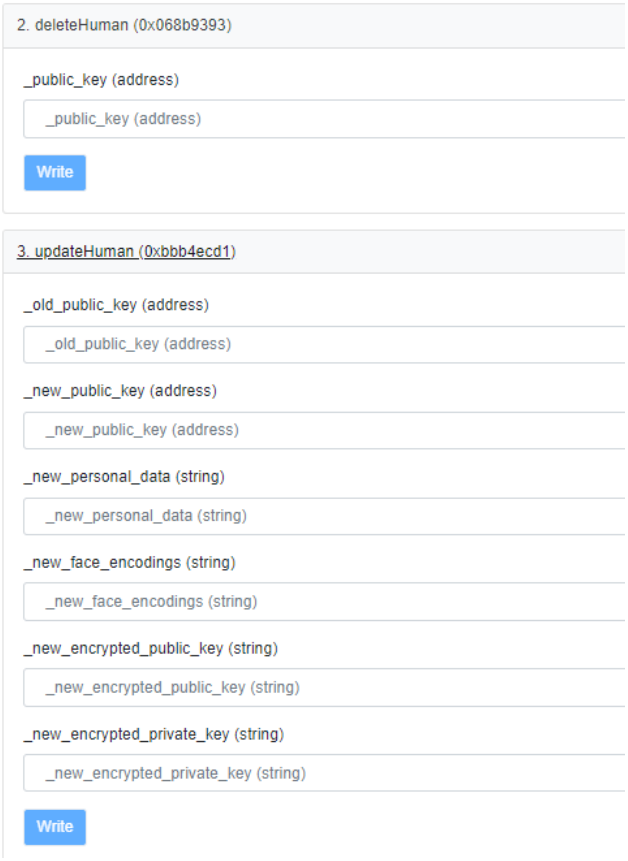

Рисунок 7 - Пример удаления и обновления данных
DOI: https://doi.org/10.23670/IRJ.2024.142.6.8

Обработка транзакций, связанных с предоставлением и отзывом доступа к данным между пользователями и организациями, происходит с использованием асимметричного шифрования и публичных ключей.

Реализовано взаимодействие с серверной частью системы (FastAPI) для получения и обработки запросов от клиентов и передачи данных между клиентами, сервером и смарт-контрактами.

Для сбора и обработки биометрических данных пользователей было разработано приложение, основанное на клиентской части системы (React). Оно обеспечивает удобный интерфейс для ввода и обработки биометрических данных, а также взаимодействие с сервером и смарт-контрактами.

Запрос эмоций пользователя для обеспечения подлинности биометрических данных и исключения возможности использования фотографий, пользователю предлагается проявить две эмоции – грусть и радость. Это позволяет убедиться в том, что данные получены в реальном времени (рис. 8).

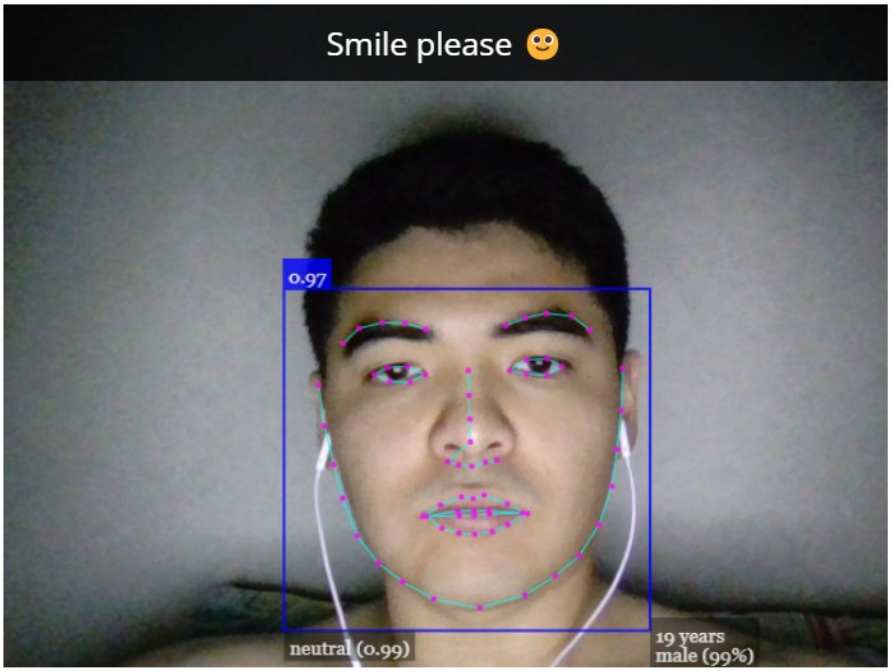

Рисунок 8 - Пример запроса прохождения эмоционального теста
DOI: https://doi.org/10.23670/IRJ.2024.142.6.9

Для сбора биометрических данных приложение использует библиотеку face-api.js для распознавания и анализа лица пользователя, формируя массив face_encodings, представляющий уникальные характеристики лица (рис. 9).

Рисунок 9 - Пример получения уникальных характеристик лица
DOI: https://doi.org/10.23670/IRJ.2024.142.6.10

Обработка данных при получении массив face_encodings передается на сервер (рис. 10), где с помощью библиотеки face-recognition происходит сопоставление с хранимыми данными других пользователей для определения идентификации пользователя.

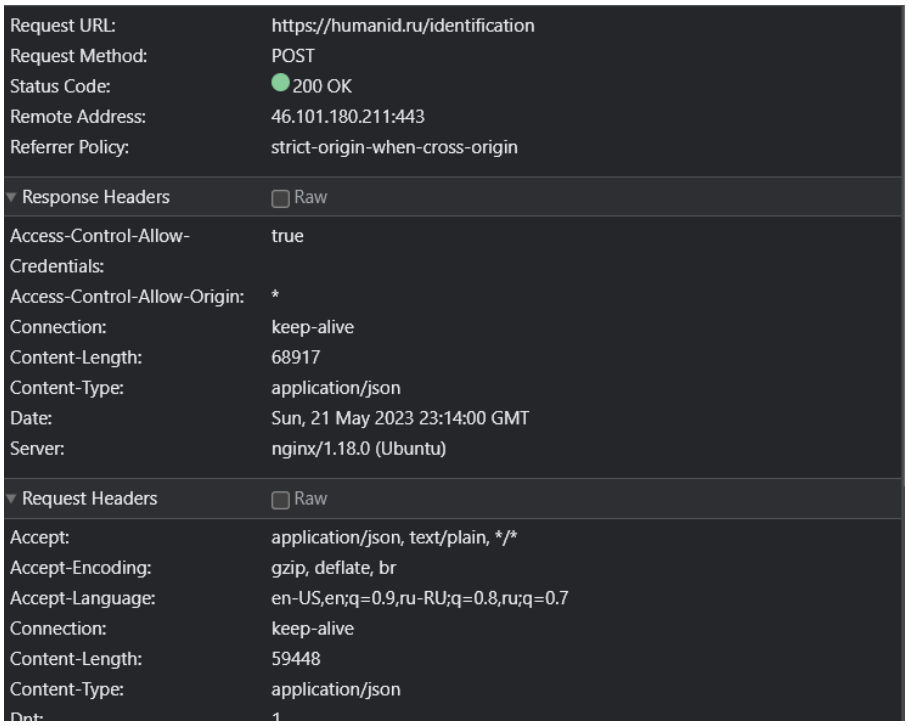

Рисунок 10 - Отправка данных на сервер
DOI: https://doi.org/10.23670/IRJ.2024.142.6.11

Шифрование и передача данных происходит после успешной идентификации, пользовательские данные шифруются с использованием библиотеки OpenPGP и передаются на сервер для дальнейшего взаимодействия со смарт-контрактом (рис. 11).

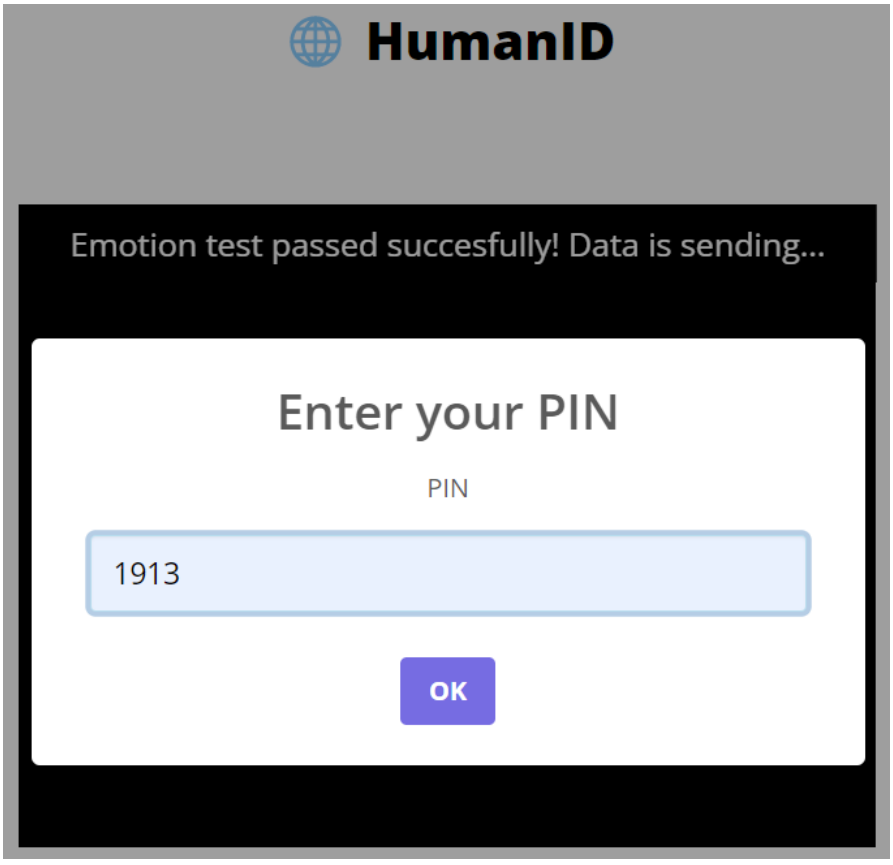

Рисунок 11 - Попытка расшифровки данных с помощью ПИН-кода
DOI: https://doi.org/10.23670/IRJ.2024.142.6.12

Для обеспечения качества и надежности разработанной системы идентификации личности по биометрическим данным были проведены комплексные тесты всех ее компонентов. Тестирование включало в себя проверку функциональности, производительности, безопасности и корректности взаимодействия между узлами системы.

На этапе тестирования серверной части использовались мок-тесты для проверки работы FastAPI сервера (рис. 12, рис. 13). Мок-тесты (mock tests) – это специальный вид тестирования программного обеспечения, при котором заменяются реальные объекты и зависимости тестируемого кода на заглушки. Данный вид тестирования позволяет изолировать функциональность сервера от внешних зависимостей, что обеспечивает более точное и надежное тестирование. С помощью мок-тестов проверялись различные сценарии работы сервера, обработка запросов и взаимодействие с базой данных.

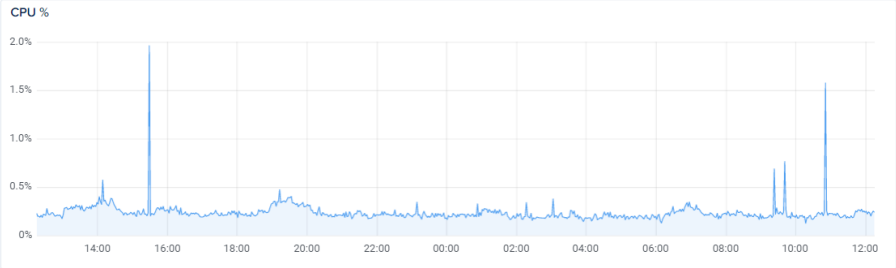

Рисунок 12 - Нагрузка центрального процессора на сервере при тестировании идентификации 1000 пользователей
DOI: https://doi.org/10.23670/IRJ.2024.142.6.13

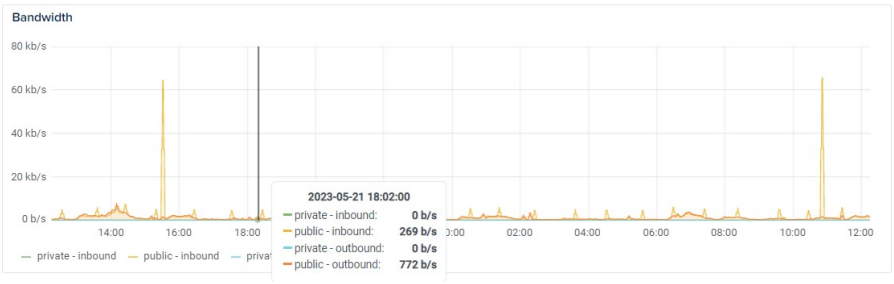

Рисунок 13 - Пропускная способность при тестировании идентификации 1000 пользователей
DOI: https://doi.org/10.23670/IRJ.2024.142.6.14

Для тестирования смарт-контракта на языке Solidity также использовались мок-тесты (рис. 14). Они позволяют проверить логику работы смарт-контракта, его взаимодействие с блокчейн-сетью и корректность хранения биометрических данных [20]. На этапе тестирования клиентской части системы, разработанной на React, использовались тесты веб-компонентов. Это позволило проверить корректность работы пользовательского интерфейса, взаимодействие с сервером и обработку пользовательских данных.

Рисунок 14 - Результаты тестирования транзакций на смарт-контракте
DOI: https://doi.org/10.23670/IRJ.2024.142.6.15

В ходе исследования было проведено сравнение разработанной системы идентификации личности с альтернативным решением – DigitalID [21]. Результаты сравнения систем представлены в таблице 2.

Данное сравнение разработанная выявило ряд значительных преимуществ разработанной системы идентификации личности перед альтернативным решением. Для апробации разработанной системы с перспективой ее широкого применения в различных отраслях, где требуется надежная идентификация пользователей и защита их персональных данных, следует перейти по ссылке [22].

Таблица 2 - Результаты сравнения систем

DOI: https://doi.org/10.23670/IRJ.2024.142.6.16

Параметры	HumanID	DigitalID
Время обработки и идентификации пользователя на основе компьютерного зрения	0,3 секунды	0,6 секунд
Время обработки и передачи запросов между узлами системы	0,5 секунд	0,9 секунд
Время исполнения смарт-контрактов и записи данных в блокчейн	2 секунды	–
Использование децентрализованной блокчейн технологии для хранения данных	Да, основана на сети Polygon	–
Управление пользователями доступом к их данным	Пользователи имеют полный контроль над своими данными и могут управлять доступом по своему усмотрению	Пользователи имеют ограниченный контроль над своими данными

Заключение

В статье освещены принципы разработки децентрализованной системы идентификации личности по биометрическим данным с использованием технологии блокчейн и компьютерного зрения. Основные результаты, полученные в ходе исследования, можно сформулировать следующим образом:

1. Подтверждена актуальность разработки новой системы идентификации на основе биометрических данных и технологии блокчейн.

2. Рассмотрены теоретические основы биометрической идентификации, технологии блокчейн и компьютерного зрения, что позволило определить основные принципы и алгоритмы для разработки системы.

3. Спроектирована архитектура системы, состоящая из трех узлов: смарт-контракт, сервер и клиент. Определены функциональные требования к системе и выбран подходящий тип блокчейна для ее реализации.

4. Разработан алгоритм идентификации на основе компьютерного зрения, обеспечивающий безопасность и приватность данных пользователей.

5. Реализована система, включающая создание смарт-контрактов для хранения и обработки биометрических данных, разработку приложения для сбора и обработки данных, а также интеграцию компьютерного зрения для идентификации личности.

6. Проведено тестирование системы, оценка ее производительности, масштабируемости, безопасности и приватности. Система продемонстрировала ряд преимуществ перед альтернативным решением.

Разработанная децентрализованная система идентификации личности обладает значительным практическим потенциалом и может быть использована в различных сферах, таких как финансы, здравоохранение, образование и правоохранительные органы. Предлагаемое в статье решение прокладывает путь для дальнейшего развития инновационных технологий в области цифровой идентификации.

Конфликт интересов

Не указан.

Рецензия

Кацко С.Ю., Сибирский государственный университет геосистем и технологий, Новосибирск, Российская Федерация

DOI: https://doi.org/10.23670/IRJ.2024.142.6.17

Conflict of Interest

None declared.

Review

Katsko S.Y., Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

DOI: https://doi.org/10.23670/IRJ.2024.142.6.17

Список литературы на английском языке / References in English

1. Zheng Z. Blockchain challenges and opportunities: A survey / Z. Zheng, S. Xie, H. N. Dai et al. // International journal of web and grid services. — 2018. — Vol. 14. — Iss. 4. — P. 352–375.

2. Tasatanattakool P. Blockchain: Challenges and applications / P. Tasatanattakool, C. Techapanupreeda // 2018 International Conference on Information Networking (ICOIN). — 2018. — P. 473–475.

3. Tolosana R. Increasing the robustness of biometric templates for dynamic signature biometric systems / R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia et al. // 2015 International Carnahan Conference on Security Technology (ICCST). — Taiwan. — 2015. — P. 229–234. DOI: 10.1109/CCST.2015.7389687

4. Moganeshwaran R. Fingerprint-fingervein multimodal biometric authentication system in field programmable gate array / R. Moganeshwaran, M. Khalil Hani, M. Annuar Suhaini // 2012 IEEE International Conference on Circuits and Systems (ICCAS). — Kuala Lumpur. — 2012. — P. 237–242. DOI: 10.1109/ICCircuitsAndSystems.2012.6408317

5. Huang T. Research on Single Sign-on Technology for Educational Administration Information Service Platform / T. Huang, F. Guo // 2021 3rd International Conference on Computer Communication and the Internet (ICCCI). — Nagoya. — 2021. — P. 69–72. DOI: 10.1109/ICCCI51764.2021.9486813

6. Chitpinityon S. New Approach for Single Sign-on Improvement using Load Distribution Method / S. Chitpinityon, M. Tossa // 2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C). — Bangkok. — 2021. — P. 44–47. DOI: 10.1109/RI2C51727.2021.9559786

7. Elhoseny M. Multimodal biometric personal identification and verification / M. Elhoseny, A. Elkhateb, A. Sahlol et al. // Advances in Soft Computing and Machine Learning in Image Processing. — 2018. — P. 249–276.

8. Vega A. P. Biometric personal identification system based on patterns created by finger veins / A. P. Vega, C. M. Travieso, J. B. Alonso // 3rd IEEE International Work-Conference on Bioinspired Intelligence. — 2014. — P. 65–70.

9. Shen W. Automated biometrics-based personal identification / W. Shen, T. Tan // Proceedings of the National Academy of Sciences. — 1999. — Vol. 96. — P. 11065–11066.

10. Li X. A survey on the security of blockchain systems / X. Li, P. Jiang, T. Chen et al. // Future generation computer systems. — 2020. — Vol. 107. — P. 841–853.

11. Cuimei L. Human face detection algorithm via Haar cascade classifier combined with three additional classifiers / L. Cuimei, Q. Zhiliang, J. Nan et al. // 2017 13th IEEE International Conference on Electronic Measurement Instruments (ICEMI). — 2017. — P. 483–487.

12. Cruz-Mota J. Scale invariant feature transform on the sphere: Theory and applications / J. Cruz-Mota, I. Bogdanova, B. Paquier et al. // International journal of computer vision. — 2012. — Vol. 98. — P. 217–241.

13. Bay H. Speeded-up robust features (SURF) / H. Bay, A. Ess, T. Tuytelaars et al. // Computer vision and image understanding. — 2008. — Vol. 110. — P. 346–359.

14. Surasak T. Histogram of oriented gradients for human detection in video / T. Surasak, I. Takahiro, C. H. Cheng et al. // 2018 5th International conference on business and industrial research (ICBIR). — 2018. — P. 172–176.

15. Lavin A. Fast algorithms for convolutional neural networks / A. Lavin, S. Gray // Proceedings of the IEEE conference on computer vision and pattern recognition. — 2016. — P. 4013–4021.

16. Yuan Y. Hrformer: High-resolution vision transformer for dense predict / Y. Yuan, R. Fu, L. Huang et al. // Advances in Neural Information Processing Systems. — 2021. — Vol. 34. — P. 7281–7293.

17. Barron J. L. Performance of optical flow techniques / J. L. Barron, D. J. Fleet, S. S. Beauchemin et al. // Proceedings 1992 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. — 1992. — P. 236–237.

18. Zhao W. Face recognition: A literature survey / W. Zhao, R. Chellappa, P. J. Phillips et al. // ACM computing surveys (CSUR). — 2003. — Vol. 35. — P. 399–458.

19. Bansal P. Study on integration of FastAPI and machine learning for continuous authentication of behavioral biometrics / P. Bansal, A. Ouda // 2022 International Symposium on Networks, Computers and Communications (ISNCC). — 2022. — P. 1–6.

20. Sharma Y. An authentication model for online transactions using biometric security / Y. Sharma, H. Gupta, S. K. Khatri // 2019 4th International Conference on Information Systems and Computer Networks (ISCON). — 2019. — P. 7–11.

21. Chalaemwongwan N. A practical national digital ID framework on blockchain (NIDBC) / N. Chalaemwongwan, W. Kurutach // 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). — 2018. — P. 497–500.

22. Humanid_app. — URL: https://github.com/Gi3a/humanid_app (accessed: 02.09.2023).