Перевертун Д.Р. Развитие технологий биометрии в сфере аутентификации и защиты данных // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 9(35) с. 37–40

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

РАЗВИТИЕ ТЕХНОЛОГИЙ БИОМЕТРИИ В СФЕРЕ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ДАННЫХ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Технологии биометрии переживают быстрое развитие и становятся важным элементом современных систем аутентификации и защиты данных. В данной статье мы исследуем, как биометрические технологии меняют ландшафт кибербезопасности, предоставляя более надежные и удобные методы аутентификации, а также рассмотрим их преимущества и вызовы.

Ключевые слова: Биометрия, аутентификация, защита данных, сенсоры, биометрические данные, кибербезопасность.

DEVELOPMENT OF BIOMETRIC TECHNOLOGIES IN THE FIELD OF AUTHENTICATION AND DATA PROTECTION

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

Biometrics technologies are experiencing rapid development and are becoming an important element of modern authentication and data protection systems. In this article, we will explore how biometric technologies are changing the cybersecurity landscape by providing more reliable and convenient authentication methods, as well as consider their advantages and challenges.

Keywords: Biometrics, authentication, data protection, sensors, biometric data, cybersecurity.

С развитием цифровых технологий и увеличением объемов хранимых и обрабатываемых данных вопрос безопасности информации становится критически важным. Особенно актуальной становится проблема аутентификации, то есть проверки подлинности пользователей, чтобы предотвратить несанкционированный доступ к данным. В этой области технологии биометрии приходят на помощь и революционизируют методы аутентификации и защиты данных.[1]

Биометрия - это наука об измерении и анализе физических и поведенческих характеристик человека. В контексте аутентификации, биометрия используется для идентификации личности по уникальным физическим или поведенческим характеристикам. Эти характеристики включают в себя следующие [2-3]:

- Отпечатки пальцев: Уникальные узоры на пальцах, которые используются для аутентификации.
- Распознавание лица: Технологии, которые сканируют и анализируют черты лица, такие как форма глаз, носа и рта.
- Сканирование радужки глаза: Анализ уникального узора радужки для идентификации.
- Голосовая биометрия: Анализ особенностей голоса, таких как тембр и ритм, для аутентификации.

Поведенческая биометрия: Оценка поведения, такого как стиль печати на клавиатуре или походка, для определения личности.

Преимущества биометрии в аутентификации:

- Уникальность: Биометрические характеристики уникальны для каждого человека, что делает их идеальными для аутентификации.
- Удобство: Пользователям не нужно запоминать пароли или носить с собой ключи - их собственное тело служит ключом к данным.
- Надежность: Биометрические системы сложнее подделать или обойти, чем пароли или PIN-коды.
- Скорость: Процесс аутентификации по биометрическим данным может быть быстрым и эффективным.
- Улучшение безопасности: Биометрические данные могут быть использованы в сочетании с другими методами аутентификации, усиливая безопасность.

Несмотря на многочисленные преимущества, биометрия также имеет свои вызовы и ограничения:

- Приватность: Сбор и хранение биометрических данных вызывают вопросы о приватности и безопасности этих данных.
- Сканирование и сенсоры: Качество сканирования и качество сенсоров могут влиять на точность и надежность биометрических систем.
- Обратимость: В некоторых случаях биометричные характеристики могут быть обмануты, например, с помощью фотографии лица или записи голоса.
- Ложное срабатывание и отказ: Системы биометрии иногда могут допускать ошибки, срабатывая ложно или не срабатывая вовсе. [4-5]

Технологии биометрии представляют собой наиболее инновационные методы аутентификации и защиты данных, доступные в наше время. Их уникальность, удобство и надежность делают их неотъемлемой частью современных систем безопасности. Однако, внедрение биометрических решений также вызывает вопросы приватности и безопасности, которые требуют серьезного внимания и разработки соответствующих стандартов и законодательства.

Приватность и безопасность биометрических данных: Сбор и хранение биометрических данных представляют собой большую ответственность. Компании и организации, использующие биометрию, должны строго соблюдать нормы и законы о защите данных и приватности пользователей. Это включает в себя шифрование биометрических данных и установление строгих мер безопасности для их хранения и передачи.[6-7]

Сканирование и сенсоры: Точность и надежность биометрических систем часто зависят от качества сенсоров и оборудования. Например, камера, используемая для сканирования лица, должна быть способной различать живое лицо от фотографии. Развитие более совершенных сенсоров и технологий сканирования играет важную роль в повышении точности биометрических систем.

Обратимость и защита от мошенничества: Противники могут попытаться обойти биометрические системы, используя фотографии, записи голоса или другие мошеннические методы. Разработчики биометрических систем должны постоянно совершенствовать методы защиты от мошенничества, включая дополнительные проверки и двухфакторную аутентификацию.

В заключение, развитие технологий биометрии в сфере аутентификации и защиты данных обещает значительно улучшить безопасность и удобство в цифровом мире. Однако внедрение этих технологий требует осторожности, соблюдения принципов приватности и безопасности, а также постоянного совершенствования систем для обеспечения надежности и защиты данных пользователей. Биометрия представляет собой важное звено в современных стратегиях кибербезопасности и имеет потенциал изменить ландшафт аутентификации и защиты данных в будущем.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н. А., Мазепин П. С., Гришин Н. А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С.152-156.
7. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022.–№. 4.–С.51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N. A., Timofeev R. S. Comparison of training methods for convolutional neural networks //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.