ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції

20-21 листопада 2023 р.

Міністерство освіти і науки України

Вінницький національний технічний університет
Національна академія Державної прикордонної служби України
ім. Богдана Хмельницького
Вінницький національний медичний університет ім. М.І. Пирогова
КЗВО «Вінницька академія безперервної освіти»
КЗ «Сумський обласний інститут післядипломної педагогічної освіти»
Інститут комп'ютерних систем і технологій "Індустрія 4.0"
ім. П. Н. Платонова
Люблінська політехніка (Польща)
Університет Бельсько-Бяльський (Польща)

«ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП»

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної Інтернет-конференції
20-21 листопада 2023 р.

Суми/Віннця
НІКО/КЗВО «Вінницька академія безперервної освіти»
2023

УДК 004
ББК 32.97
Е50

Рекомендовано до видання Вченою радою КЗВО «Вінницька академія безперервної освіти» (протокол № 8 від 20.11.2023 р.)

Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2023 р. – Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2023. – 336 с.

ISBN 978-617-7422-23-4

Збірник містить матеріали Міжнародної науково-практичної Інтернет конференції «Електронні інформаційні ресурси: створення, використання, доступ. Матеріали збірника подано у авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей, Матеріали відтворюються зі збереженням змісту, орфографії та синтаксису текстів, наданих авторами.

УДК 004
ISBN 978-617-7422-23-4

ресурсів для навчання, оскільки модель може використовувати знання, отримані із більших та різноманітних наборів даних.

5. Основні точки [8].

У світі комп'ютерної графіки, точки [9], такі як очі, ніс, рот, підборіддя та контури обличчя, виступають, як основні елементи при розташуванні ключових точок. Ці важливі анатомічні деталі визначають унікальну геометрію обличчя та допомагають алгоритмам точно визначати положення та орієнтацію обличчя у просторі.

Ці елементи не лише надають базову інформацію про структуру обличчя, але й утворюють основу для вирішення більш складних завдань у сфері комп'ютерного зору. Розпізнавання емоцій, аналіз рухів та ідентифікація особливих рис обличчя стають можливими завдяки точному визначенню цих ключових точок.

Правила та алгоритми, які були описані раніше, використовуються для створення надійних та ефективних методів розташування ключових точок на обличчях людей.

Отже ця технологія може використовуватися в різних галузях, включаючи сферу розваг, розробку систем безпеки, медичні дослідження та багато інших областей. Відкриваючи нові перспективи для застосунків комп'ютерного зору, вона стає не лише інструментом вдосконалення технологічного прогресу, але й каталізатором для нових досліджень та інновацій.

Список використаної літератури

1. Матеріали та документація TensorFlow: [Електронний ресурс] – Режим доступу: https://www.tensorflow.org/tutorials/images/cnn;
2. " Курс "Convolutional Neural Networks" на Coursera: [Електронний ресурс] – Режим доступу: https://www.coursera.org/learn/convolutional-neural-networks;
3. Стаття "Ensemble Learning: A Comprehensive Guide" на Towards Data Science : [Електронний ресурс] – Режим доступу: https://towardsdatascience.com/ensemble-learning-a-comprehensive-guide-4f9d073f4e63;
4. Курс "Ensemble Learning in Python" на DataCamp [Електронний ресурс] – Режим доступу: https://www.datacamp.com/courses/ensemble-learning-in-python;
5. Стаття "Supervised Learning" на сайті Towards Data Science [Електронний ресурс] – Режим доступу: https://towardsdatascience.com/supervised-learning-2e2f7d78c63;
6. Документація TensorFlow на тему Transfer Learning [Електронний ресурс] – Режим доступу: https://www.tensorflow.org/tutorials/images/transfer_learning;
7. Стаття "A Comprehensive Introduction to Transfer Learning" на Machine Learning Mastery [Електронний ресурс] – https://machinelearningmastery.com/transfer-learning-for-deep-learning/;
8. Стаття "Facial Landmarks with OpenCV and Dlib" на PyImageSearch [Електронний ресурс] – Режим доступу: https://www.pyimagesearch.com/2018/04/02/faster-facial-landmark-detector-with-dlib/;
9. Стаття "Facial key point detection in Python with OpenCV" на Towards Data Science [Електронний ресурс] – Режим доступу: https://towardsdatascience.com/facial-key-point-detection-a-beginners-guide-c87a3d43cfb.

ПРУС Б.В., РАКИТЯНСЬКА Г.Б.,
Вінницький національний технічний університет

ШИФРУВАННЯ ТА БЕЗПЕКА ЗБЕРЕЖЕННЯ ДАНИХ У FLUTTER ДОДАТКАХ

Анотація: У статті розглянуто важливі аспекти шифрування та безпеки збереження даних в мобільних додатках, розроблених з використанням Flutter.

Ключові слова: Мобільний додаток, безпека даних, шифрування, збереження даних, Flutter.

Abstract: The article discusses important aspects of encryption and security of data storage in mobile applications developed using Flutter.

Keywords: Mobile app, data security, encryption, data retention, Flutter.

Вступ

У світі мобільних додатків безпека даних стала однією з найважливіших тем. Мобільні додатки використовуються для здійснення фінансових операцій, обміну особистими повідомленнями, зберігання особистих фотографій та багато іншого. Точно так само, як і зі звичайними комп'ютерами, безпека даних у мобільних додатках має вирішальне значення. Користувачі довіряють додаткам значну кількість особистої та конфіденційної інформації, такої як паролі, фінансові дані, локація та контакти [1]. Тому розробники повинні забезпечити належний рівень захисту цих даних.

Flutter [2] від Google з відкритим кодом швидко став одним із найпопулярніших інструментів розробки для створення кросплатформних мобільних додатків. У цій статті ми розглянемо, який захист вбудовано в мобільні програми Flutter, і порекомендуємо додаткові рівні, які можна використати для мобільних проектів.

Виклад основного матеріалу

Захист даних користувачів - це не лише їх право, але й обов'язок розробників. Невдача у забезпеченні належного рівня безпеки може призвести до серйозних наслідків, таких як витік конфіденційних даних, порушення приватності та втрата довіри користувачів. Це може також призвести до правових проблем і фінансових втрат [3]. Тож від надійності та безпеки даних залежить не лише успіх додатка, а й репутація розробника.

Шифрування є одним з головних засобів захисту даних у мобільних додатках. Шифрування полягає в перетворенні даних в такий спосіб, щоб вони стали нерозбірливими для сторонніх осіб без спеціального ключа [4]. У Flutter-додатках для забезпечення безпеки даних можна використовувати різні методи шифрування, такі як Advanced Encryption Standard (AES) або Rivest–Shamir–Adleman (RSA).

Локальні дані, які зберігаються на пристрої користувача, повинні бути шифровані. Наприклад, паролі, токени доступу, конфіденційні дані або кешована інформація повинні бути зашифрованими, щоб надійно захистити їх від несанкціонованого доступу [3].

Мобільні платформи, такі як Android і iOS, надають розробникам інструменти для забезпечення безпеки даних у мобільних додатках. У розробників є можливість використовувати системні API для збереження особистих даних користувачів в захищених областях пам'яті пристрою [4]. Наприклад, в Android можна використовувати Android Keystore для збереження ключів і токенів безпечно, а в iOS - Secure Enclave для сховища ключів. Flutter-додаток може взаємодіяти з цими системними рішеннями для забезпечення безпеки даних.

У Flutter можна використовувати пакети, такі як encrypt [5] або pointycastle [6], для реалізації шифрування даних. Для кожного типу даних, які потрібно зберегти, слід використовувати належний метод шифрування і зберігання ключів в надійному сховищі.

Під час передачі даних через мережу також необхідно використовувати шифрування, щоб захистити їх від перехоплення. Використовуйте захищені протоколи, такі як HTTPS, для забезпечення шифрованого з'єднання між клієнтом і сервером [7]. У Flutter це можна реалізувати за допомогою пакету http [8], який підтримує HTTPS-з'єднання.

Ключі і токени доступу - це важливі компоненти безпеки даних. Вони не повинні зберігатися відкрито на пристрої користувача або відправлятися по мережі в незашифрованому вигляді. Для їх захисту можна використовувати ключові сховища або безпечні місця для збереження [9].

API ключі використовуються для автентифікації додатків на віддалених серверах. Вони дозволяють додатку звертатися до зовнішніх ресурсів, таких як веб-служби або API, та отримувати доступ до ресурсів на сервері. Важливо надійно зберігати API ключі та не використовувати їх у відкритому вигляді. Їх можна зберігати в змінних середовища, які не входять до вихідного коду додатка, або в безпечних сховищах, які недоступні іншим додаткам на пристрої користувача.

Токени доступу (Access Tokens): Токени доступу використовуються для автентифікації користувачів і надання їм доступу до захищених ресурсів в додатку або на сервері. Наприклад, токени доступу використовуються для авторизації користувачів в соціальних мережах або для

доступу до особистих даних на сервері. Токени повинні бути збережені безпечно та шифровані. Крім того, слід використовувати методи автентифікації з використанням токенів, такі як OAuth, щоб забезпечити безпеку та прозорість взаємодії з ресурсами [10].

Для забезпечення безпеки даних також важливо правильно реалізувати процес аутентифікації користувачів. Необхідно використовувати сучасні методи аутентифікації, такі як двофакторна аутентифікація, входження за допомогою відбитків пальців або розпізнавання обличчя, щоб запобігти несанкціонованому доступу.

Загальна безпека даних у мобільних додатках - це процес, який постійно розвивається та оновлюється. Використовуючи вищезазначені практики та ресурси, ви зможете підтримувати найвищий стандарт безпеки в ваших Flutter-додатках і надавати користувачам впевненість у збереженні їхніх даних.

Висновки

Шифрування та безпека збереження даних в Flutter-додатках є критично важливими аспектами розробки. Захист даних користувачів повинен бути високого рівня, і розробники повинні вкласти зусилля в забезпечення безпеки локальних і переданих даних. Використовуючи належні методи шифрування, безпечні сховища для ключів і токенів, а також правильні методи аутентифікації, ви можете створити надійний та безпечний Flutter-додаток, якому користувачі можуть довіряти.

Список використаних джерел

1. Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse. (2015). The Mobile Application Hacker's, 18.
2. Flutter [Електронний ресурс] – режим доступу: https://flutter.dev Дата звернення: 28 жовтня 2023.
3. Timothy Speed, Darla Nykamp, Mari Heiser, Joseph Anderson. (2013). Mobile Security: How to Secure, Privatize, and Recover Your Devices, 20-23, 56-58.
4. Himanshu Dwivedi, Chris Clark, (2012) Mobile Application Security, 16, 40, 68.
5. Encrypt [Електронний ресурс] – Режим доступу: https://pub.dev/packages/encrypt Дата звернення: 28 жовтня 2023.
6. Pointycastle [Електронний ресурс] – Режим доступу: https://pub.dev/packages/pointycastle Дата звернення: 28 жовтня 2023.
7. Introduction to HTTP and HTTPS [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/azure/rtos/netx-duo/netx-duo-web-http/chapter1 Дата звернення: 28 жовтня 2023.
8. Http [Електронний ресурс] – Режим доступу: https://pub.dev/packages/http Дата звернення: 28 жовтня 2023.
9. Understanding OAuth2 Landscape [Електронний ресурс] – Режим доступу: https://sagarag.medium.com/understanding-oauth2-landscape-1b80cc9ed303 Дата звернення: 28 жовтня 2023.
10. Aaron Parecki (2012), OAuth 2.0: The Definitive Guide 156-160.

ПРУС О.В., МАЙДАНЮК В.П.,
Вінницький національний технічний університет

WEBASSEMBLY: ІНТЕГРАЦІЯ ТА ІННОВАЦІЇ У ПОБУДОВІ ГРАФІКІВ ТА ІНТЕРАКТИВНИХ ВЕБ-ІНТЕРФЕЙСІВ

Анотація: Стаття розглядає роль та важливість WebAssembly (Wasm) у побудові графіків та інтерактивних інтерфейсів на веб-сторінках. WebAssembly надає можливості оптимізації та виконання високоякісного коду на веб-платформі, що робить його потужним інструментом для розробки веб-додатків. Стаття аналізує основні аспекти використання WebAssembly у графіці та інтерактивних інтерфейсах, а також надає огляд фреймворків і бібліотек для роботи з Wasm. Висвітлюються найкращі практики та інноваційні рішення для покращення веб-графіки та інтерактивності.

Ключові слова: WebAssembly, Wasm, графіка, інтерактивність, веб-інтерфейси, фреймворки, бібліотеки, оптимізація, інновації, веб-розробка, візуалізація, віртуальні інтерфейси, графічний дизайн.

ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ: СТВОРЕННЯ, ВИКОРИСТАННЯ, ДОСТУП:

Збірник матеріалів
Міжнародної науково-практичної Інтернет-конференції
20-21 листопада 2023 р.

Редактор С.А.Пойда, М.С. Ніколаєнко
Комп'ютерне верстання С.А.Пойда, М.С. Ніколаєнко

Підписано до друку 15.11.2023 Гарнітура Times New Roman
Формат 60х84/16 Папір офсетний
Друк цифровий Ум. друк. арк. 19,4
Тираж 300 пр. Зам. № 2/23

Видавництво НІКО
м.Суми, вул.Харківська, 54
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи України
серія СМв № 044
від 15.10.2012
E-mail: ms.niko@i.ua
Телефон для замовлень: +38(066) 270-64-68