

كلية الهندسة

قسم الهندسة المعلوماتية

هندسة أمن النظم والشبكات الحاسوبية



## Secure Networked Software Architecture for University Electronic-Attendance Systems

بنية شبكية برمجية آمنة لنظام الحضور والتفقد الإلكتروني للجامعات

إعداد :

بيان محمد سفيان النصاري

تala فراس المسالمه

سوق علي الخشمان

باشراف:

م.محمد يامن الحلاق

بنيار - 2026

## الملخص

مع التطور المتتسارع في تقنيات التحول الرقمي واعتماد المؤسسات التعليمية على الأنظمة الذكية، برزت الحاجة إلى إيجاد حلول تقنية فعالة لمعالجة المشكلات المرتبطة بالأنظمة التقليدية لن فقد الحضور، مثل إهدر الوقت، وقابلية التلاعب، وعدم الدقة في تسجيل البيانات. يهدف هذا المشروع إلى تصميم وتنفيذ نظام تفقد حضور إلكتروني جامعي ذكي يعتمد على تقنية التعرف على الوجه (Face Recognition)، مدعوماً بنية شبكة وبرمجية متكاملة تضمن الدقة، السرعة، وأمن البيانات.

يقوم النظام المقترن على التقاط صور الطلبة داخل القاعات الدراسية باستخدام أجهزة مخصصة، ثم معالجة هذه الصور ومقارنتها مع قاعدة بيانات مركبة تحتوي على بيانات الوجوه المسجلة مسبقاً، ليتم تسجيل الحضور تلقائياً دون تدخل بشري. تم تصميم البنية البرمجية للنظام بحيث تضمن سهولة الإدارء، وقابلية التوسيع، والتكامل مع الأنظمة الجامعية الأخرى، في حين تم بناء بنية شبكة محاكية لبيئة جامعة حقيقة باستخدام أدوات محاكاة متقدمة تتيح ربط أجهزة القاعات مع الخادم центральный بشكل آمن وفعال

## Abstract

With the rapid advancement of digital transformation technologies and the increasing adoption of smart systems in educational institutions, there has been a growing need for effective technological solutions to address the limitations of traditional attendance methods. Conventional attendance systems, such as manual sign-in sheets or verbal roll calls, are often time-consuming, prone to human error, and vulnerable to manipulation. This project aims to design and implement a smart electronic attendance system for universities based on face recognition technology, supported by a secure and integrated network and software architecture.

The proposed system operates by capturing students' facial images within lecture halls and automatically matching them against a centralized database containing pre-registered facial data. Upon successful identification, attendance records are generated without human intervention. The software architecture of the system is designed to ensure scalability, reliability, and ease of management, while the network architecture is implemented to securely connect classroom devices to a central server, ensuring efficient data transmission and protection of sensitive information.

## Table of Contents

|          |   |
|----------|---|
| 7 .....  | 1.1 مقدمة الفصل   |
| 8 .....  | <u>1.2 المشكلة العلمية</u>                                      |
| 8.....   | 1.3 الهدف   |
| 9.....   | 1.4 أهمية المشروع   |
| 9 .....  | <u>1.5 المراجعة الأدبية</u>                                     |
| 9.....   | 1.5.1 تطور أنظمة فقد الحضور في المؤسسات التعليمية               |
| 9.....   | 1.5.2 أنظمة الحضور المعتمدة على التعرف على الوجه                |
| 10 ..... | 1.5.3 البنية البرمجية لأنظمة الحضور الذكية                      |
| 10 ..... | 1.5.4 البنية الشبكية وأمن أنظمة الحضور الإلكترونية              |
| 12 ..... | 1.6 التحديات  |
| 12 ..... | 1.7 التطبيقات العملية   |
| 14 ..... | الفصل الأول   |
| 15 ..... | 2.1 الأساس النظري   |
| 15 ..... | 2.2 التعرف على الوجه (Face Recognition)                         |
| 16 ..... | 2.3 كشف الوجه والتعرف عليه (Face Detection vs Face Recognition) |
| 17 ..... | 2.4 الأنظمة المعتمدة على واجهات البرمجة (API-Based Systems)     |
| 17 ..... | 2.5 البنية متعددة الطبقات (Three-Tier Architecture)             |
| 18 ..... | 2.6 منطقة العزل الشبكي(Demilitarized Zone – DMZ)                |
| 19 ..... | الفصل الثاني  |

## **مقدمة عامة**

---

|          |  |
|----------|--|
| 20 ..... | 3.1 نظرة عامة على الفصل                        |
| 21 ..... | 3.2 معمارية النظام                             |
| 22 ..... | 3.3 التقنيات والأدوات المستخدمة                |
| 24 ..... | 3.4 مكونات النظام (تفكيك الوحدات)              |
| 26 ..... | 3.5 تصميم قاعدة البيانات                       |
| 27 ..... | 3.6 خدمة التعرف على الوجه                      |
| 28 ..... | 3.7 عملية تسجيل الطالب (Enrollment)            |
| 29 ..... | 3.8 التحقق من الحضور (Verification)            |
| 29 ..... | 3.9 التفويض والتحكم بالوصول (Authorization)    |
| 30 ..... | 3.10 التدقيق والمحاسبة (Accounting & Auditing) |
| 31 ..... | 3.11 واجهات النظام ومسارات الصفحات وواجهات API |
| 31 ..... | 3.12 اعتبارات الأمان والخصوصية                 |
| 33 ..... | 3.13 سيناريو العرض العملي (Demo)               |
| 33 ..... | 3.14 القيود والتحسينات المستقبلية              |
| 33 ..... | 3.15 الخلاصة                                   |
| 37 ..... | الفصل الرابع                                   |
| 38 ..... | 4.1 نتائج البنية البرمجية للنظام               |
| 40 ..... | 4.2 نتائج البنية الشبكية والأمنية              |
| 41 ..... | 4.3 نتائج التسجيل المركزي للأحداث والتدقيق     |

|          |  |
|----------|--|
| 41 ..... | 4.4 مقارنة النتائج مع أهداف المشروع      |
| 41 ..... | 4.5 التحديات التي ظهرت أثناء التنفيذ     |
| 42 ..... | الخاتمة                                  |
| 43 ..... | قائمة المصطلحات                          |
| 44 ..... | قائمة الاختصارات (List of Abbreviations) |
| 45 ..... | References                               |



### 1.1 مقدمة الفصل

شهد قطاع التعليم العالي خلال السنوات الأخيرة تطوراً متسارعاً نتيجة التقدم الكبير في تقنيات المعلومات والاتصالات، الأمر الذي دفع الجامعات والمؤسسات التعليمية إلى تبني أنظمة إلكترونية حديثة تهدف إلى تحسين جودة العملية التعليمية والإدارية على حد سواء. وقد أصبح الاعتماد على الحلول الرقمية ضرورة ملحة لمواجهة التحديات المتزايدة المرتبطة بإدارة أعداد كبيرة من الطلبة، وضمان دقة البيانات، وتسريع الإجراءات الإدارية المختلفة. وبأinsi هذا التوجه ضمن إطار التحول الرقمي في التعليم العالي، الذي أشارت إليه عدة دراسات باعتباره عاملاً رئيسياً في تحسين كفاءة المؤسسات التعليمية ورفع مستوى الاعتمادية في خدماتها الأكademية والإدارية [1][2].

تُعد عملية نفاذ حضور الطلبة من العناصر الأساسية في النظام الأكاديمي الجامعي، لما لها من تأثير مباشر على تقييم التزام الطلبة بالمساقات الدراسية، ومتابعة انظامتهم داخل القاعات الدراسية، واتخاذ القرارات الأكاديمية المناسبة. إلا أن الأساليب التقليدية المستخدمة في تسجيل الحضور، مثل التوقيع اليدوي أو النداء الشفهي، تعاني من العديد من أوجه القصور، من أبرزها استهلاك وقت المحاضرة، وزيادة العبء الإداري على أعضاء الهيئة التدريسية، إضافة إلى احتمالية وقوع أخطاء بشرية أو حالات تلاعب وانتفال شخصية. وقد أكدت دراسات متعددة أن هذه الأساليب تفتقر إلى الدقة والموثوقية، خصوصاً في البيانات التعليمية ذات الأعداد الكبيرة من الطلبة [3][4].

ومع التطور الملحوظ في مجال الذكاء الاصطناعي ومعالجة الصور، برزت تقنيات القياسات الحيوية كحلول تقنية متقدمة لمعالجة هذه المشكلات، حيث تُعد تقنية التعرف على الوجه من أكثر هذه التقنيات شيوعاً وانتشاراً في الأنظمة التعليمية الحديثة. ويعود ذلك إلى ما توفره من سهولة في الاستخدام، ودقة عالية في التحقق من الهوية، وعدم الحاجة إلى تفاعل مباشر من المستخدم أو استخدام أدوات إضافية. وقد بينت دراسات حديثة أن أنظمة الحضور المعتمدة على التعرف على الوجه تسهم بشكل كبير في تقليل حالات التلاعب وتحسين موثوقية سجلات الحضور [5][6]. إلا أن هذه الدراسات تشير أيضاً إلى أن نجاح هذه الأنظمة يتطلب تصميم بنية برمجية منظمة ومتكلمة مع بنية شبكة آمنة، تضمن حماية البيانات الحساسة ومنع الوصول غير المصرح به، وهو ما يشكل الأساس العلمي لهذا المشروع [7][8].

## 1.2 المشكلة العلمية

تركز العديد من الدراسات على تطوير أنظمة حضور تعتمد على التعرف على الوجه من الناحية البرمجية، مع التركيز على دقة الخوارزميات وسرعة المعالجة [4]. إلا أن جزءاً كبيراً من هذه الأنظمة يتم نشره ضمن بيئات شبكية غير مدرورة، حيث يتم كشف خوادم التطبيقات أو قواعد البيانات مباشرة للمستخدمين، مما يزيد من المخاطر الأمنية ويجعل النظام عرضة للهجمات أو إساعه الاستخدام [5].

تتمثل المشكلة العلمية في الحاجة إلى تصميم نظام حضور إلكتروني لا يقتصر على دقة التعرف على الوجه فقط، بل يعتمد على بنية برمجية منتظمة ومتكلمة مع بنية شبكة آمنة تضمن الفصل بين المستخدمين والخدمات الحساسة، وتدعم مبدأ أقل صلاحية، وتتوفر قابلية التتبع والتدقيق [6].

## 1.3 الهدف

يهدف هذا المشروع إلى تصميم وتنفيذ بنية شبكة برمجية آمنة لنظام تفقد الحضور الإلكتروني في الجامعات، بما يحقق تكاملاً فعّالاً بين الجوانب البرمجية والشبكية للنظام. ويسعى المشروع إلى بناء نظام حضور إلكتروني يعتمد على تقنية التعرف على الوجه للحد من حالات التلاعب والاحتلال وضمان موثوقية تسجيل الحضور . كما يهدف إلى تصميم بنية برمجية خدمية (Service-Oriented Architecture) تعتمد على واجهات برمجية (APIs) لفصل واجهة المستخدم عن منطق النظام، بما يسهم في تحسين القابلية للتوسيع وسهولة الصيانة والتطوير المستقبلي .

ومن الناحية الشبكية، يهدف المشروع إلى تصميم بنية متعددة الطبقات (Three-Tier Architecture) تضمن عزل المستخدمين عن خوادم التطبيقات وقواعد البيانات الحساسة، وتعزز مستوى الأمان العام للنظام . ويشمل ذلك استخدام منطقة منزوعة السلاح (DMZ) كنقطة دخول وحيدة للنظام بهدف حماية الموارد الداخلية ومنع الوصول المباشر إليها . كما يسعى المشروع إلى تطبيق سياسات التحكم بالوصول باستخدام قوائم التحكم (Access Control Lists) وفق مبدأ أقل صلاحية (Least Privilege) للحد من سطح الهجوم وتقليل المخاطر الأمنية . إضافة إلى ذلك، يهدف النظام إلى دعم آليات التسجيل المركزي للأحداث

(Centralized Logging) بما يعزز قابلية المراقبة والتدقيق وتتبع الأنشطة، ويساعد في الكشف المبكر عن السلوكيات غير الطبيعية وتحليل الحوادث الأمنية المحتملة .

## 1.4 أهمية المشروع

تكمّن أهمية هذا المشروع في كونه يجمع بين ثلاثة مجالات رئيسية: الذكاء الاصطناعي، هندسة البرمجيات، وهندسة الشبكات. فقد أظهرت دراسات حديثة أن أنظمة التعرف على الوجه في التعليم تسهم في تحسين دقة وموثوقية تسجيل الحضور [13]، إلا أن غياب التصميم الشبكي الآمن يُعد من الأسباب الرئيسية لفشل هذه الأنظمة عند نشرها فعليًا [14].

كما يقدم المشروع نموذجًا أكاديميًّا وتطبيقيًّا يوضح أن تحقيق الأمان لا يعتمد فقط على استخدام أدوات أمنية متقدمة، بل يمكن تحقيقه من خلال التصميم الصحيح والتكامل بين البنية البرمجية والبنية الشبكية، وهو ما يعزز مفهوم الأمان القائم على المعمارية [15] (Architecture-Based Security).

## 1.5 المراجعة الأدبية

### 1.5.1 تطور أنظمة تفقد الحضور في المؤسسات التعليمية

شهدت أنظمة تفقد الحضور في المؤسسات التعليمية تحولاً ملحوظاً من الأساليب التقليدية اليدوية إلى الأنظمة الإلكترونية، وذلك بهدف تحسين دقة البيانات وتقليل الاعتماد على العامل البشري. فالطرق التقليدية مثل التوقيع اليدوي أو النداء الشفهي تستهلك وقتاً كبيراً من المحاضرات، كما أنها عرضة للأخطاء البشرية وحالات التلاعُب والانتهال، خاصة في الجامعات ذات الأعداد الكبيرة من الطلبة. وقد أظهرت الدراسات أن هذه الأساليب تؤدي إلى زيادة العبء الإداري على أعضاء الهيئة التدريسية، إضافة إلى صعوبة حفظ سجلات الحضور واسترجاعها وتحليلها بشكل فعال، مما دفع المؤسسات التعليمية إلى البحث عن حلول تقنية أكثر كفاءة لإدارة الحضور [1][2].

### 1.5.2 أنظمة الحضور المعتمدة على التعرف على الوجه

مع التقدم في مجال الذكاء الاصطناعي ومعالجة الصور، برزت تقنيات القياسات الحيوية كحلول فعالة لمعالجة مشكلات أنظمة الحضور التقليدية، وتُعد تقنية التعرف على الوجه من أكثر هذه التقنيات استخداماً في البيانات التعليمية. ويعود ذلك إلى قدرتها على التحقق من هوية الأفراد دون الحاجة إلى أدوات إضافية أو تفاعل مباشر من المستخدم، مما يقلل من حالات التلاعُب والانتهال. وقد

## الفصل الأول

بيّنت دراسات عديدة أن أنظمة الحضور المعتمدة على التعرف على الوجه تسهم في تحسين موثوقية تسجيل الحضور ورفع دقتها، خصوصاً في القاعات الدراسية الذكية، إلا أنها أشارت أيضاً إلى وجود تحديات تتعلق بالإضاءة وزوايا التصوير وجودة الكاميرات. [5][4][3]

### 1.5.3 البنية البرمجية لأنظمة الحضور الذكية

تؤكد الأدبيات المتعلقة بـهندسة البرمجيات على أهمية تصميم بنية برمجية واضحة ومنظمة عند تطوير الأنظمة الذكية، لما لذلك من دور في تحسين القابلية للصيانة والتوسّع وضمان استقرار النظام. وتشير الدراسات إلى أن اعتماد معماريّات برمجية خدمية تعتمد على واجهات برمجية (APIs) يسهم في فصل واجهة المستخدم عن منطق الأعمال، ويتيح سهولة التكامل مع أنظمة أخرى مستقبلاً. كما أن هذا النوع من البنى البرمجية يساعد في تطبيق ضوابط أمنية بشكل أفضل، خاصة عند التعامل مع بيانات حساسة مثل البيانات البيومترية، وهو ما يجعل البنية البرمجية عنصراً أساسياً في نجاح أنظمة الحضور الإلكترونية. [6][7].

### 1.5.4 البنية الشبكية وأمن أنظمة الحضور الإلكترونية

تشير الأدبيات في مجال أمن المعلومات إلى أن نجاح الأنظمة الإلكترونية لا يعتمد على الجانب البرمجي فقط، بل يتطلّب أيضاً تصميم بنية شبكيّة آمنة تضمن حماية الموارد والخدمات الحساسة. ويُعد التقسيم الشبكي وعزل المكونات الداخلية من المبادئ الأساسية للحد من المخاطر الأمنية، حيث تسهم البنى متعددة الطبقات في تقليل سطح الهجوم ومنع الوصول غير المصرح به. كما تؤكّد الدراسات على أهمية استخدام مناطق منزوعة السلاح (DMZ) كنقطة دخول وحيدة للأنظمة، وتطبيق سياسات التحكم بالوصول وفق مبدأ أقل صلاحية، إضافة إلى دور التسجيل المركزي للأحداث في تعزيز المراقبة والتدقّيق والاستجابة للحوادث الأمنية. [10][9][8].

جدول 1: أهم مقالات الدراسة في أنظمة تفقد الحضور الإلكتروني

| SL.No. | Pub Year | Author(s)   | Title   | Pub Title  |
|--------|----------|---|---|--|
| 1      | 2024     | Ashish Jadhav; Dhwaniket .Kamble; Santosh B ;Rathod; Sumita Kumar Mohammad Dalwai | Attendance management system using face recognition | IAES Int. Journal of Artificial Intelligence               |
| 2      | 2024     | K. Lavanya; N. Akalyaa .S. Archana; J Pushpakala                                  | Face Recognition-Based Attendance System            | Shanix International Journal of Arts, Science Humanities & |

## الفصل الأول

|    |      |   |  |  |
|----|------|---|--|--|
| 3  | 2025 | Siti Aisyah   | Development of a Smart Attendance System Using Face Recognition Technology       | ICISTech Journal   |
| 4  | 2024 | ;Kamal G. Oladele Edidiong J. Iseh; Jamal .O. Oladele; Pawan R Bhaladhare                     | AI-Based Face Recognition Attendance System                                      | International Journal of Innovative Research in Multidisciplinary Professional Studies (IJIRMPS) |
| 5  | 2023 | Phul Babu Jha; Arjun ;Basnet; Biraj Pokhrel Bishnu Pokhrel; Gopal Kumar Thakur; Surya Chhetri | An Automated Attendance System Using Facial Detection and Recognition Technology | Apex Journal of Business and Management  |
| 6  | 2025 | ;Divyanshu Bhardwaj Nikita; Vernika; Aarush Gupta; Tanya Chauhan                              | Smart Attendance System Using Face Recognition with OpenCV                       | Journal of Mobile ,Computing & Communication Mobile Networks                                     |
| 7  | 2024 | S. A. Feroze  | The Facial Recognition Technology in Academic Attendance                         | International Journal of Innovative Technology and Management                                    |
| 8  | 2022 | .J. Patel et al   | Facial Recognition Attendance System with Anti-Spoofing                          | Multimedia Tools and Applications  |
| 9  | 2023 | .R. Kumar et al   | Privacy-Aware Face Recognition Attendance System                                 | IEEE Access  |
| 10 | 2023 | .M. Alqahtani et al   | AI-Based Attendance System for Higher Education                                  | Education and Information Technologies   |
| 11 | 2024 | .Y. Zhang et al   | Robust Face Recognition in Uncontrolled Environments                             | Computer Vision and Image Understanding  |
| 12 | 2024 | .S. Rose et al  | Zero Trust Architecture for Distributed Web Applications                         | ACM Computing Surveys  |

# الفصل الأول

## 1.6 التحديات

تشير الدراسات الحديثة إلى أن أنظمة تفقد الحضور الإلكتروني المعتمدة على تقنية التعرف على الوجه تواجه مجموعة من التحديات التقنية والعملية عند تطبيقها في البيئات التعليمية الواقعية. من أبرز هذه التحديات تغير ظروف الإضاءة داخل القاعات الدراسية، حيث أوضحت بعض الدراسات أن ضعف الإضاءة أو عدم تجانسها يؤدي إلى انخفاض جودة الصور الملتقطة، مما يؤثر سلباً على دقة نماذج التعرف على الوجه، خاصة في البيئات غير المضبوطة. كما تُعد زوايا التصوير المختلفة وحركة الطلبة أثناء الدخول أو الجلوس من العوامل التي تزيد من صعوبة استخراج الخصائص البيومترية بدقة.

## 1.7 التطبيقات العملية

خلال السنوات الأخيرة، ولا سيما منذ عام 2020، شهدت أنظمة تفقد الحضور الإلكتروني المعتمدة على تقنية التعرف على الوجه تطوراً ملحوظاً في التطبيقات العملية داخل المؤسسات التعليمية، حيث ركزت العديد من الدراسات على تحويل النماذج النظرية إلى أنظمة قابلة للتطبيق في البيئات الجامعية الواقعية. وقد أظهرت هذه التطبيقات قدرة عالية على أتمتة عملية تسجيل الحضور بدقة وكفاءة، مع تقليل الاعتماد على الأساليب التقليدية التي تعاني من التلاعيب والأخطاء البشرية.

في هذا السياق، طُبّقت أنظمة الحضور المعتمدة على التعرف على الوجه في القاعات الدراسية الذكية، حيث يتم التقاط صور الطلبة تلقائياً عند دخولهم القاعة أو أثناء المحاضرة، ثم معالجتها باستخدام نماذج تعلم عميق لاستخراج الخصائص البيومترية ومقاربتها مع قواعد البيانات المخزنة مسبقاً. وأسهم هذا الأسلوب في تسريع عملية تسجيل الحضور، وتقليل الوقت المهدور، ورفع موثوقية السجلات الأكademie.

كما امتدت التطبيقات العملية لهذه الأنظمة لتشمل البيانات الجامعية واسعة النطاق، مثل الامتحانات الإلكترونية والتحقق من هوية الطلبة، إضافة إلى دمجها مع أنظمة إدارة التعلم والمنصات التعليمية. وأظهرت الدراسات أن الجمع بين تقنيات معالجة الصور، ونماذج التعرف المقدمة، والبني البرمجية الآمنة، يساهم في توفير حلول عملية قابلة للتوسّع، مع الحفاظ على خصوصية البيانات وحمايتها، مما يجعل هذه الأنظمة مناسبة للتطبيق الفعلي في مؤسسات التعليم العالي.

## الفصل الأول

---

---

## الفصل الأول

## 2.1 الأساس النظري

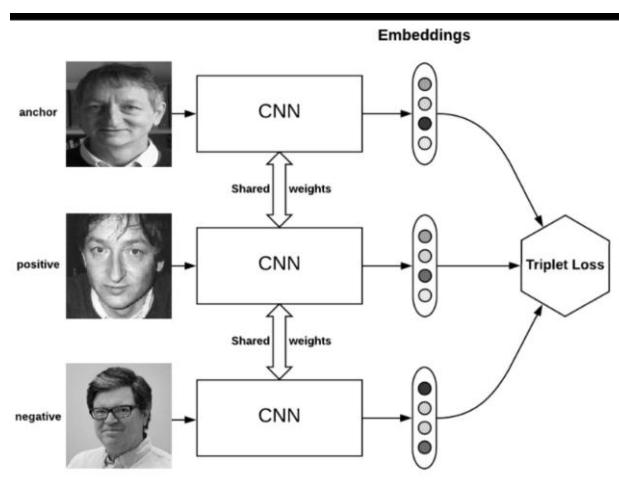
يهدف هذا الفصل إلى تقديم الإطار النظري والمفاهيمي الذي يقوم عليه تصميم وتنفيذ نظام تفقد الحضور الإلكتروني المقترن، وذلك من خلال استعراض مجموعة من المفاهيم الأساسية في مجالات التعرف على الوجه، وهندسة البرمجيات، وأمن الشبكات. ويُعد هذا الفصل أساساً علمياً لفهم البنية البرمجية والبنية الشبكية للنظام قبل الانتقال إلى الجوانب التطبيقية والتنفيذية في الفصول اللاحقة.

كما يركّز الفصل على توضيح العلاقة التكاملية بين التقنيات البرمجية والمفاهيم الشبكية والأمنية، ودورها في تحقيق نظام حضور إلكتروني يتمتع بالدقة، والاعتمادية، وحماية البيانات الحساسة.

## 2.2 التعرف على الوجه (Face Recognition)

يُعد التعرف على الوجه أحد تقنيات القياسات الحيوية التي تعتمد على الخصائص الفизيائية الفريدة لوجه الإنسان للتحقق من الهوية. وتقوم هذه التقنية على تحليل ملامح الوجه واستخراج مجموعة من الخصائص الرقمية التي تمثل بصمة فريدة لكل شخص، ثم مقارنتها مع بيانات مخزنة مسبقاً في قاعدة بيانات.

وقد أسمى التطور الكبير في نماذج التعلم العميق في تحسين دقة أنظمة التعرف على الوجه بشكل ملحوظ، خاصة في التعامل مع التغيرات في الإضاءة، وتعبيرات الوجه، وزوايا التصوير. ويُعد هذا النوع من التقنيات مناسباً لأنظمة تفقد الحضور في الجامعات، نظراً لكونه غير تلامسي ولا يتطلب تفاعلاً مباشراً من المستخدم.



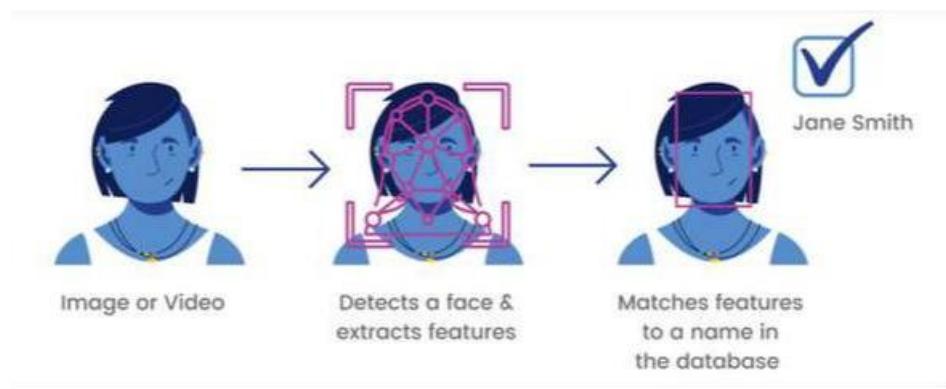
الشكل (1.1): المخطط العام لأآلية عمل نظام التعرف على الوجه

## Face Detection vs Face ( كشف الوجه والتعرف عليه ) 2.3

### (Recognition)

تمر أنظمة التعرف على الوجه بمرحلتين أساسيتين تختلفان من حيث الوظيفة والدور. تتمثل المرحلة الأولى في كشف الوجه، وتهدف إلى تحديد موقع الوجه داخل الصورة أو الفيديو دون التعرف على هوية الشخص. أما المرحلة الثانية فهي التعرف على الوجه، والتي ترتكز على تحديد هوية الشخص من خلال مقارنة الخصائص المستخرجة مع قاعدة البيانات.

ويُعد الفصل بين هاتين المرحلتين أمرًا ضروريًا في تصميم الأنظمة الذكية، حيث يسمح باستخدام خوارزميات متخصصة لكل مرحلة، مما يؤدي إلى تحسين الكفاءة العامة للنظام وزيادة دقتها.



الشكل (1.2): الفرق بين كشف الوجه والتعرف على الوجه

### 2.4 الأنظمة المعتمدة على واجهات البرمجة (API-Based Systems)

تشير الأنظمة المعتمدة على واجهات البرمجة (APIs) إلى نمط معماري يسمح بتبادل البيانات والخدمات بين مكونات النظام المختلفة من خلال واجهات محددة وواضحة. ويسهم هذا الأسلوب في فصل واجهة المستخدم عن منطق الأعمال، مما يعزز قابلية الصيانة والتطوير.

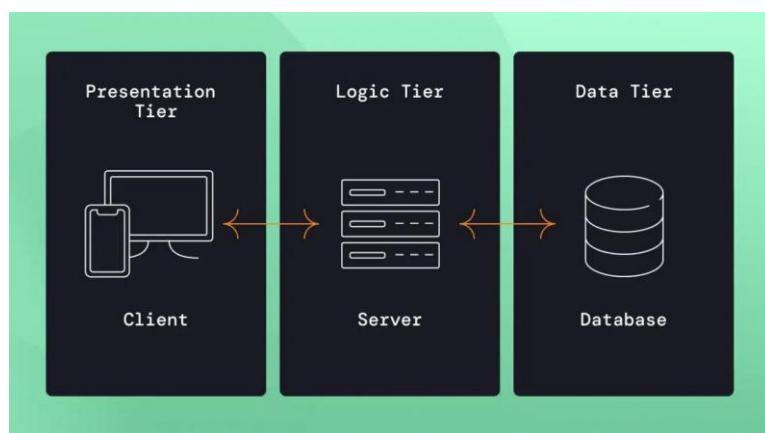
في نظام تقدّم الخدمة الإلكتروني، تُستخدم واجهات البرمجة لربط واجهة المستخدم بخدمات التعرف على الوجه وقواعد البيانات وأنظمة المصادقة، مما يحقق بنية مرنة وقابلة للتَوسيع.

### 2.5 البنية متعددة الطبقات (Three-Tier Architecture)

تعتمد البنية متعددة الطبقات على تقسيم النظام إلى ثلاثة طبقات رئيسية:

طبقة العرض، وطبقة التطبيق، وطبقة البيانات. ويساعد هذا التقسيم على تنظيم النظام بشكل أفضل، وتقليل الاعتماد المباشر بين مكوناته، وتعزيز مستوى الأمان.

وتُعد هذه البنية مناسبة لأنظمة الحضور الجامعية التي تتطلب إدارة عدد كبير من المستخدمين، مع ضمان حماية قواعد البيانات من الوصول المباشر.

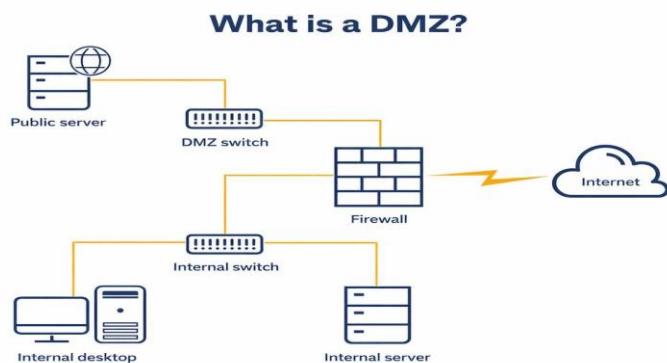


(الشكل(1.3): البنية متعددة الطبقات (Three-Tier Architecture )

### 2.6 منطقة العزل الشبكي (Demilitarized Zone – DMZ)

تشير منطقة العزل الشبكي (DMZ) إلى طبقة وسيطة تُستخدم لعزل الخوادم التي تتعامل مع المستخدمين الخارجيين عن الشبكة الداخلية. وتُعد DMZ من المفاهيم الأساسية في تصميم الشبكات الآمنة، حيث تقلل من مخاطر الوصول غير المصرح به إلى الموارد الحساسة.

في نظام الحضور الإلكتروني، تُستخدم DMZ كنقطة دخول وحيدة لواجهات البرمجة والخدمات، مما يعزز مستوى الحماية ويحد من انتشار الهجمات داخل الشبكة.



الشكل (1.4): نموذج بنية شبكة باستخدام DMZ

---

## الفصل الثاني

يوثق هذا الفصل المعمارية البرمجية التي تم تطبيقها في مشروع "نظام الحضور الجامعي المعتمد على التعرف على الوجه". يركز الفصل على كيفية تقسيم النظام إلى وحدات متنقلة (**Modules**)، وكيفية تفاعل الواجهات الأمامية مع واجهات (**ONNX** عبر REST API) في **ArcFace**، **Django**، وكيف يتم تشغيل محرك التعرف على الوجه (**Embedding Face**) وربطه بهوية الطالب. كما يوضح الفصل آليات التحقق من إنتاج تمثيل عددي للوجه (**Embedding Face**) وربطه بهوية الطالب. كما يوضح الفصل آليات التحقق من الصلاحيات داخل القاعات (**Audit Logs**) وآلية حفظ سجلات التدقيق (**Authorization**) لدعم مبدأ المحاسبة (**Accounting**) وإمكانية تتبع الأحداث.

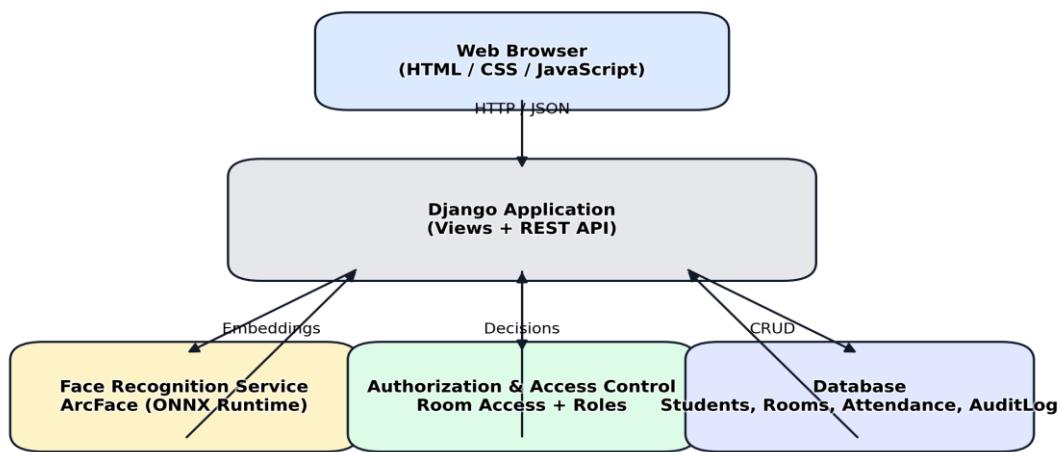
### 3.1 نظرة عامة على الفصل

يوفر النظام مسار عمل متكامل لإدارة الحضور داخل الجامعة. يبدأ المسار من تسجيل طالب جديد (**Enrollment**) عبر التقاط صورة/إطار من الكاميرا، ثم استخراج الـ **Embedding** وتخزينه في قاعدة البيانات. بعد ذلك، عند تنفيذ عملية التحقق داخل قاعة محددة (**Live Scan**)، يقوم النظام باستخراج الـ **Embedding** من الصورة الحالية ومقارنته مع القوالب المسجلة للطلاب، ثم يطبق سياسة الصلاحيات الخاصة بالقاعة (هل هذا الطالب مسموح له بالدخول لهذه القاعة/الجسسة؟). في النهاية يتم إنشاء سجل حضور منظم (**Attendance Record**) وإضافة سجل تدقيق (**Audit Log**) يتضمن نتيجة العملية ومعلوماتها.

من الناحية الهندسية، تم تصميم النظام كبنية معيارية (**Modular Design**) بحيث تكون كل وظيفة رئيسية معزولة قدر الإمكان. هذا التقسيم يسهل تطوير النظام واختباره، ويجعل توسعه لاحقاً أكثر أماناً ووضوحاً. كما تم تضمين عناصر "المصادقة + التفويض + المحاسبة" (**AAA**) من خلال: التتحقق من هوية المستخدم عند الحاجة، تقييم صلاحية الطالب لدخول قاعة معينة (**Authorization**)، وتسجيل كل العمليات الأمنية المهمة مثل تسجيل الطالب، محاولات التتحقق، وأي محاولة وصول غير مصرح بها.

### 3.2 معمارية النظام

يتبع النموذج الأولي معمارية طبقية تفصل بين: طبقة العرض (Web Pages)، وطبقة منطق الأعمال (Django Views/APIs)، وخدمات التعرف على الوجه، ووحدة التحكم بالوصول. يتم تبادل البيانات بين المتصفح وتطبيق Django عبر HTTP/JSON، بينما يتم استدعاء محرك ArcFace داخلياً لاستخراج الـ Embedding. يوضح الشكل 2.1 نظرة شاملة على المكونات الأساسية ومسارات الاتصال بينها.



الشكل 2.1 : نظرة عامة على بنية النظام

تم تطوير النظام باستخدام Django REST Framework مع Django Python لواجهات الـ API. أثناء العرض التجريبي يتم تشغيل الخادم محلياً عبر `python manage.py runserver`، ويقوم المتصفح باستدعاء الصفحات ومسارات الـ API لجلب البيانات وتحديث لوحة التحكم (Dashboard) بشكل دوري.

### 3.3 التقنيات والأدوات المستخدمة

يعرض هذا القسم التقنيات الأساسية التي اعتمد عليها التنفيذ. يشمل ذلك: **Django/DRF** لإنشاء واجهات الويب وواجهات الـ **API**، قاعدة بيانات **SQLite** (في النسخة التجريبية)، مكتبات تشغيل النماذج عبر **ONNX** **HTML/CSS/JavaScript** لاستخراج تمثيل الوجه. كما تم استخدام **ArcFace Runtime**، ومعيار **getUserMedia** في الواجهات، وبالأخص للوصول إلى الكاميرا ضمن المتصفح.

## الفصل الثاني

الجدول 2.1: مجموعة التقنيات (تنفيذ النموذج الأولي)

| Layer                 | Technology                        | Purpose   |
|-----------------------|-----------------------------------|---|
| Backend Web Framework | Django                            | Routing, views, templates, ORM, admin panel                   |
| API Layer             | Django REST Framework             | JSON endpoints, authentication mechanisms, request validation |
| ML Inference Runtime  | ONNX Runtime                      | Execute ArcFace embedding model efficiently on CPU/GPU        |
| Face Embedding Model  | ArcFace                           | Generate discriminative face embeddings for matching          |
| Database              | Relational DB (SQLite/PostgreSQL) | Persistence for students, rooms, attendance, audit logs       |
| Frontend              | HTML/CSS/JavaScript               | Enrollment page, live scan view, dashboard updates            |
| Administration        | Django Admin                      | Create rooms, manage enrollments, inspect logs, debug data    |

### 3.4 مكونات النظام (تفكيك الوحدات)

من أجل قابلية الصيانة والتنظيم، قُسم النظام إلى وحدات واضحة، بحيث تتكامل هذه الوحدات عبر واجهات محددة. الهدف من هذا التقسيم هو تقليل الترابط (Coupling) وزيادة التماسك (Cohesion) بحيث يمكن تطوير كل جزء دون كسر بقية الأجزاء. يوضح الجدول 2.2 نظرة سريعة على هذه الوحدات ومسؤولياتها.

- المصادقة وملفات المستخدم (User Profiles & Authentication): إدارة حسابات المستخدمين (مثل Admin/Teacher)، تسجيل الدخول، وإدارة بيانات الملف الشخصي الأساسية، مع إمكانية الاعتماد على جلسات الويب أو Tokens عند استخدام واجهات API.
- إدارة الطلاب (Student Management): حفظ هوية الطالب (الرقم الجامعي والاسم) وربطها ب قالب الوجه المخزن (Embedding Vector) الذي يمثل بصمة الوجه الرقمية.
- إدارة القاعات والصلاحيات (Access Management & Room): تعريف القاعات (Rooms) وسياسات الوصول المرتبطة بها، أي تحديد الطالب المسموح لهم بالدخول إلى قاعة معينة (ويمكن توسيعها لتشمل جلسات مقرر محددة).
- محرك الحضور (Attendance Engine): تنسيق خطوات التحقق: التقاط الإطار من الكاميرا، استخراج الـ Embedding، المقارنة مع القوالب المسجلة، دمج نتائج التعرف مع سياق القاعة، ثم كتابة سجل حضور في قاعدة البيانات.
- التدقيق والمحاسبة (Accounting & Auditing): تسجيل الأحداث ذات الحساسية الأمنية مثل محاولات تسجيل طالب، محاولات تحقق ناجحة/فشلية، ومحاولات وصول غير مصرح بها. هذه السجلات تدعم تتبع "من قام بماذا، ومتى، ومن أي عنوان IP، وما هي النتيجة".
- الواجهة الأمامية ولوحة التحكم (Frontend Dashboard): توفير صفحات سهلة الاستخدام للعرض التجريبي: صفحة تسجيل طالب، صفحة التتحقق المباشر (Live Scan)، ولوحة Dashboard لعرض سجلات الحضور وتحديثها دورياً.

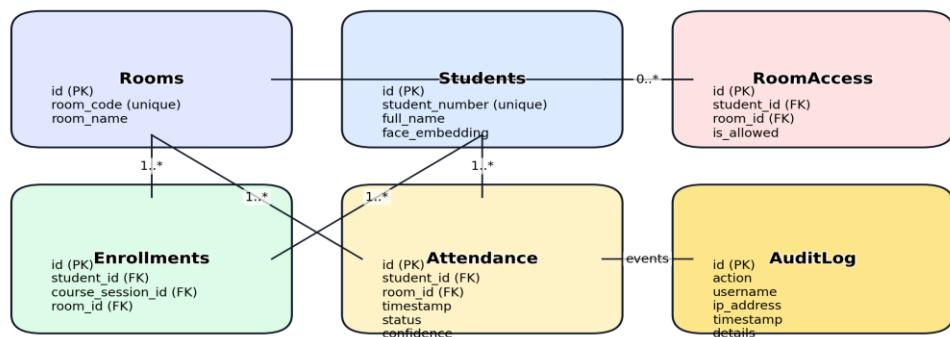
الجدول 2.2: المكونات الرئيسية ومسؤولياتها في Django

## الفصل الثاني

| Component              | Typical File(s)      | Key Responsibilities  |
|------------------------|----------------------|---|
| Models                 | models.py            | Define Students, Rooms, Enrollments, RoomAccess, Attendance, AuditLog |
| Views (Pages)          | views.py + templates | Render dashboard, enrollment page, live scan page                     |
| Views (APIs)           | views.py / api views | Enrollment API, verification API, attendance list API                 |
| Serializers/Validators | serializers.py       | Validate inputs (student data, images, parameters)                    |
| Face Service           | face_service/*       | Load ONNX model, extract embeddings, cosine similarity                |
| Authorization          | authorization.py     | Decide if student is allowed in target room/session                   |
| Auditing               | accounting.py        | Write structured audit events for accountability                      |

### 3.5 تصميم قاعدة البيانات

يعتمد النظام على مخطط علقي (Relational Schema) يربط بين: الطلاب، القاعات، جلسات المقررات (Course Sessions)، وسجلات الحضور والتنفيذ. يهدف هذا التصميم إلى ضمان التكامل المرجعي (Referential Integrity) وإتاحة الاستعلامات المهمة، مثل: عرض حضور طالب ضمن فترة زمنية، أو عرض جميع عمليات الدخول المحاولة لقاعة معينة. يوضح الشكل 2.4 العلاقات الأساسية بين الجداول.



الشكل 2.4: تصميم قاعدة البيانات وعلاقات الجداول

يحتفظ جدول **Students** بمعلومات الطالب الأساسية و قالب الوجه (**face\_embedding**). بينما يعرف جدول **Rooms** القاعات وأковادها (مثل **LAB-101**). ويستخدم جدول **Enrollments/RoomAccess** لربط الطالب بالقاعات أو الجلسات المسموح بها، أما جدول **Attendance** فيحفظ نتيجة كل عملية تحقق (الحالة، الوقت، القاعة، ونسبة الثقة). أخيراً، يسجل جدول **AuditLog** أحداث النظام لأغراض التتبع والمحاسبة.

الجدول 2.3: الجداول الأساسية والحقول الرئيسية

| Table       | Key Fields   | Notes   |
|-------------|--|---|
| Students    | student_number, full_name, face_embedding          | Face embedding stored as a vector/blob/encoded list |
| Rooms       | room_code, room_name                               | Used to tag events by physical location             |
| Enrollments | student_id, room_id, course_session_id             | Maps student to room/session context                |
| RoomAccess  | student_id, room_id, is_allowed                    | Explicit allow/deny rules (can override defaults)   |
| Attendance  | student_id, room_id, timestamp, status, confidence | Status {IN,OUT,FORBIDDEN}                           |
| AuditLog    | action, username, ip_address, timestamp, details   | Immutable security trail                            |

### 3.6 خدمة التعرف على الوجه

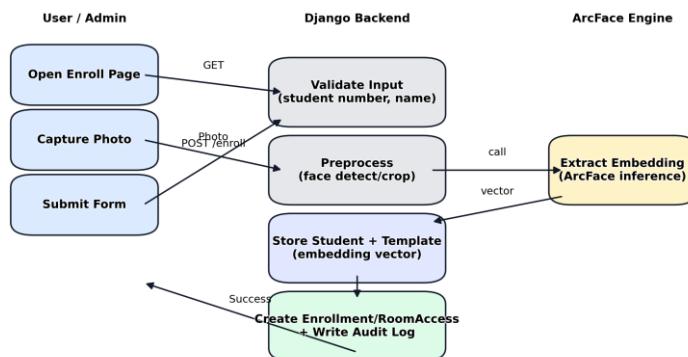
تعتمد عملية التعرف على الوجه على استخراج تمثيل عدي ثابت الطول (**Embedding**) لكل وجه. في مرحلة التسجيل، تُلتقط صورة واضحة لوجه الطالب ثم تمر عبر النموذج **ArcFace** ( بصيغة **ONNX** ) لإنتاج **Embedding**. يتم تخزين هذا المتجه في قاعدة البيانات وربطه بمعرف الطالب. هذا الأسلوب يسمح بالمطابقة لاحقًا عبر مقارنة المتجهات بدل الاعتماد على الصورة الخام.

في مرحلة التحقق، يتم استخراج **Embedding** من الإطار الحالي ثم حساب مقياس التشابه (**Similarity**) مع قواليب الطالب المسجلة. إذا تجاوزت أعلى درجة تشابه عتبة (**Threshold**) محددة، يعتبر الطالب معرفًا (**Recognized**). بعد التعرف، تطبق سياسة الوصول: إذا كان الطالب ضمن قائمة المسموح لهم لقاعة/جلسة معينة، ثُسجّل الحالة **IN**، وإذا كان معروفاً لكنه غير مخول للقاعة ثُسجّل الحالة **FORBIDDEN**. أما إذا لم يتم الوصول لعتبة التعرف فتعامل الحالة كـ **OUT** أو **Unknown** وفق سياسة النظام.

من أجل موثوقية النتائج، يفرض النظام قيوداً أثناء التسجيل مثل: وجود وجه واحد فقط في الإطار، إضاءة مناسبة، وعدم وجود اهتزاز كبير. كما تتم معالجة الحالات الاستثنائية مثل فشل التقاط الصورة أو عدم وجود وجه واضح، مع تسجيل الحدث في **AuditLog** لإظهار سبب الفشل.

### 3.7 عملية تسجيل الطالب (Enrollment)

تُنفذ عملية التسجيل عبر صفحة **Enrollment** في الواجهة. عند إدخال رقم الطالب والاسم، يطلب المتصفح صلاحية الوصول للكاميرا ثم يلتقط صورة عند الضغط على **Take Photo**. ترسل الصورة إلى **Django API Take Photo**، الذي يستدعي محرك **ArcFace Embedding** لاستخراج الـ **embedding** ويخرّنه في جدول **Students**. يوضح الشكل 2.2 تسلسل الخطوات من المتصفح وحتى تخزين القالب.

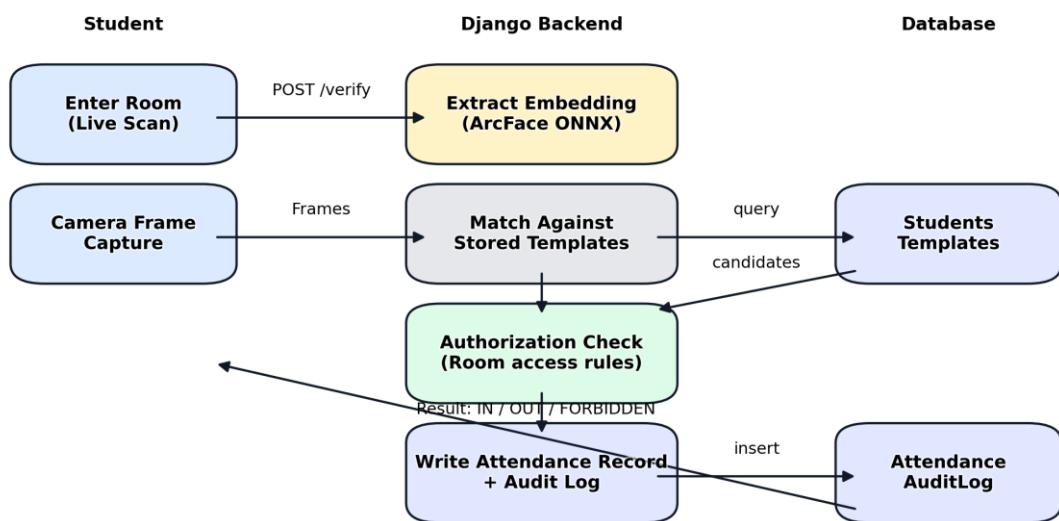


الشكل 2.2: تسلسل عملية التسجيل

لربط الطالب بقاعة محددة (تجربة التفريض)، يتم إنشاء قيد في **Enrollment** أو **RoomAccess** يحدد أن هذا الطالب مسموح له بالدخول إلى قاعة معينة مثل **Lab 1 (LAB-101)**. يمكن تنفيذ ذلك عبر لوحة **Django Admin** خلال العرض التجاري: بعد إنشاء الطالب، نضيف علاقته **RoomAccess** تشير إلى **RoomAccess** والقاعة (وحلّة السماح).

### 3.8 التحقق من الحضور (Verification)

عملية التحقق (Verification) تتم من خلال صفحة Live Scan المرتبطة بقاعة القاعة الحالية (Room). يتم إدخال الكاميرا بشكل دوري وإرساله إلى مسار API مخصص للتحقق. يستخرج النقاط إطار (Frame) من الكاميرا ويشكل دورياً ويُرسل إلى مسار API مخصص للتحقق. يتم إنشاء Embedding للإطار ثم يبحث عن أفضل تطابق مع الطلاب المسجلين. بعد ذلك يطبق سياسة الوصول الخادم على Embedding لبناء نتائج التحقق (مسحوق/غير مسحوق) ثم يُعرضها في الواجهة. يوضح الشكل 2.3 هذا التسلسل.



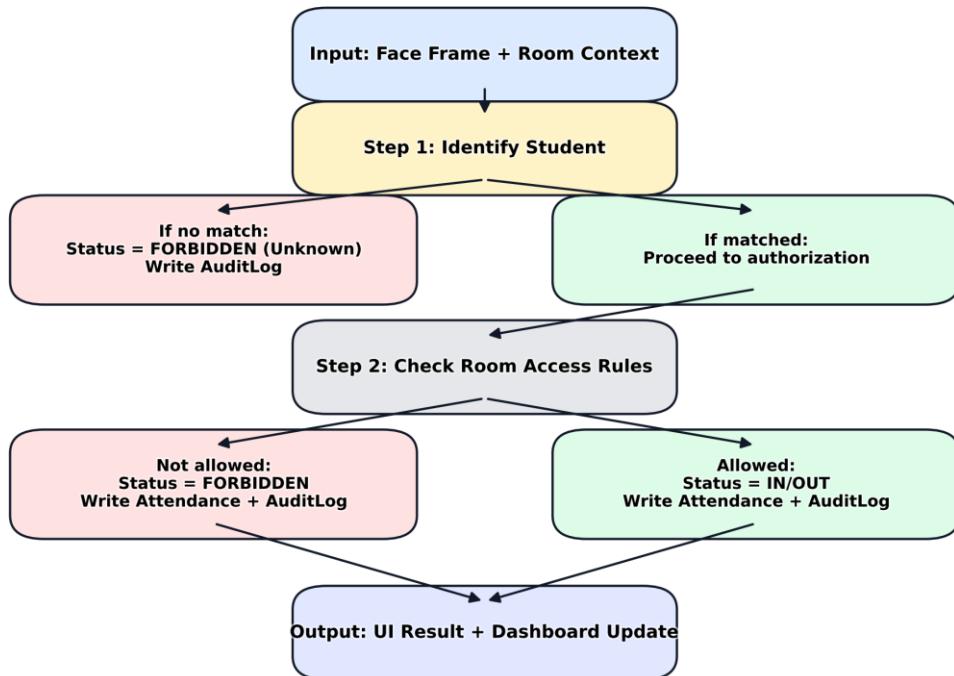
الشكل 2.3: تسلسل التتحقق من الحضور

بعد اتخاذ القرار، ينشئ النظام سجل حضور جديد يحتوي على: الطالب (إن وجد)، القاعة، الوقت، الحالة Dashboard (Confidence) (IN/OUT/FORBIDDEN). يتم تحديث لوحة API لعرض السجل اليومي وتلخيص النتائج.

### 3.9 التفويض والتحكم بالوصول (Authorization)

يطبق النظام مبدأ التحكم بالوصول عبر قواعد واضحة تربط هوية الطالب بسياق القاعة/الجلسة. بمعنى آخر، التعرف على الوجه وحده لا يكفي لإثبات السماح بالدخول؛ بل يجب أن يكون الطالب "محولاً" لهذه القاعة وفق البيانات المخزنة. لهذا

السبب تم فصل منطق التعرف (Recognition) عن منطق الصلاحيات (Authorization) لضمان اتساق القرار وسهولة تدقيقه.



الشكل 2.5: مخطط تدفق قرار التقويض

عند التحقق، إذا تم التعرف على الطالب ثم تم إيجاد قيد RoomAccess يسمح له بالدخول، تكون النتيجة IN. أما إذا تم التعرف على الطالب لكن لا يوجد سماح لهذه القاعة، تكون النتيجة FORBIDDEN وتحسب كمحاولة غير مصراً بها. هذا الفصل بين "التعرف" و"التقويض" يحمي النظام من سيناريوهات مثل تعرف صحيح ولكن في قاعة خاطئة.

### 3.10 التدقيق والمحاسبة (Accounting & Auditing)

يمثل التدقيق (Auditing) جزءاً أساسياً في النظام، لأنّه يوفر سجلاً زمنياً لجميع الأحداث المهمة. ويستخدم هذا السجل أثناء العرض لإثبات ما تم تفديده عملياً: إنشاء طالب جديد، محاولات تحقق ناجحة، ومحاولات مرفوضة.

يتضمن سجل التدقيق عادة حقولاً مثل: نوع العملية (action)، اسم المستخدم أو الطالب، عنوان IP، الطابع الزمني (timestamp)، وتفاصيل إضافية (details) مثل رقم القاعة أو سبب الفشل. يساعد ذلك في التحليل الجنائي (Forensics) واستكشاف الأخطاء وتحسين الضبط.

### 3.11 واجهات النظام ومسارات الصفحات وواجهات API

يعتمد النظام على تنظيم واضح لمسارات الصفحات (Pages) ومسارات الـ API داخل auth\_app/urls.py، مع استخدام أسماء مسارات (...=name) لتمكين الدوال {url %} داخل القوالب. خلال التطوير ظهرت مشكلة NoReverseMatch بسبب الإشارة إلى اسم مسار غير موجود (مثل 'face')، وتم حلها بتوحيد أسماء المسارات في urls.py وتحديث القوالب لاستخدام الأسماء الصحيحة (مثلاً: 'attendance', 'enroll', 'verify').

الجدول 2.4: أمثلة على نقاط النهاية المستخدمة في النموذج الأولي

| Category            | Endpoint (example) | Method | Purpose  |
|---------------------|--------------------|--------|--|
| Dashboard           | /                  | GET    | Main dashboard view                                      |
| Enrollment Page     | /enroll-page/      | GET    | UI for registering a new student                         |
| Live Scan Page      | /attendance/       | GET    | UI for camera-based verification                         |
| Enroll API          | /auth/enroll-face/ | POST   | Submit photo + student metadata to create template       |
| Verify API          | /auth/verify-face/ | POST   | Submit photo/frame to identify student and record status |
| Attendance List API | /auth/attendance/  | GET    | Return recent attendance records as JSON (filterable)    |
| Admin               | /admin/            | GET    | Administrative management interface                      |

### 3.12 اعتبارات الأمان والخصوصية

على الرغم من أن النموذج الحالي تجريبي، إلا أن تصميمه أخذ بعين الاعتبار مجموعة من ضوابط الأمان الأساسية. يشمل ذلك حماية مسارات الإدارية، فرض صلاحيات الوصول للعمليات الحساسة، وتسجيل كل الأنشطة المهمة. يستعرض هذا القسم أهم اعتبارات الأمانة والخصوصية التي تم الالتزام بها أثناء التنفيذ.

## الفصل الثاني

للمستخدمين المؤثوقين فقط، وإمكانية توسيع Authentication (Django Admin): تقييد لوحة الإدارة عند الحاجة API لمسارات الـ JWT/Token والنظام لاحقاً لاستخدام

، Authorization (RoomAccess/Enrollments): تطبيق قواعد وصول دقيقة لكل قاعة عبر التفويض (Authorization)، بحيث لا تُقبل عملية دخول إلا إذا كانت مطابقة لهوية الطالب ومطابقة لسياسة القاعة.

(AuditLog): تخزين التدقيق (Auditing)، مما يسهل المراجعة IP لكل حدث حساس مع بيانات السياق وقت/نتيجة، واكتشاف السلوك غير الطبيعي.

وضمان التكامل المرجعي بين Data Integrity (Foreign Keys): الاعتماد على علاقات سلامة البيانات (Data Integrity) للطلاب والقاعات وسجلات الحضور.

(Admins/Teachers): فصل الأدوار بين المستخدمين Least Privilege، مبدأ أقل الصلاحيات (Least Privilege). وحصر التعديلات المباشرة في البيانات الحساسة ضمن لوحة الإدارة فقط.

الجدول 2.5: ضوابط الأمان المطبقة أو التي تم النظر فيها

| Control                  | Where Implemented    | Notes  |
|--------------------------|----------------------|--|
| Authentication           | Django/DRF           | Admin/operator must log in; tokens may protect APIs    |
| Room-based authorization | authorization module | Denies access if student not permitted in room         |
| Audit logging            | accounting module    | Logs enrollment, verification, configuration changes   |
| Thresholding             | face service         | Rejects low-confidence matches to reduce false accepts |
| Separation of concerns   | architecture         | Keeps ML logic separate from web and database logic    |

### 3.13 سيناريو العرض العملي (Demo)

لتنفيذ عرض عملي واضح، يمكن اتباع السيناريو التالي: (1) إنشاء قاعة داخل النظام (Lab) إن لم تكن موجودة. (2) تسجيل طالب جديد عبر صفحة Enrollment والتقاط صورة واضحة. (3) ربط الطالب بالقاعة عبر إضافة (4) فتح صفحة Live Scan وتحديد القاعة Lab 1 ثم تنفيذ RoomAccess (Allowed=True). التحقق. (5) ملاحظة ظهور السجل في Dashboard مع الحالة IN والثقة. (6) لإثبات التفويض، يمكن إزالة FORBIDDEN، مع وجود سجل تدقيق يثبت محاولة دخول RoomAccess غير مصرح بها.

توفر لوحة Admin Django وسيلة فعالة لإظهار البيانات المخزنة أثناء العرض. يمكن من خلالها استعراض الطالب المنشأ (Students)، التتحقق من وجود الـ face\_embedding محفوظاً، مراجعة قيود Attendance أو Enrollments أو RoomAccess وإظهار أثر كل عملية تحقق.

### 3.14 القيود والتحسينات المستقبلية

يمثل هذا النموذج نسخة أولية (Prototype) تركز على إثبات الفكرة. من التحسينات المقترحة مستقبلاً: إضافة كشف الحيوية (Liveness Detection) لمنع محاولات الخداع بالصور، استخدام قاعدة بيانات أقوى مثل PostgreSQL، تحسين إدارة الجلسات والتكامل مع جدول المحاضرات الرسمي، تشفير قوالب الوجه أو تخزينها بشكل آمن (مثل تشفير على مستوى الحقل)، وإضافة أدوات مراقبة (Monitoring) وتقارير إحصائية متقدمة.

### 3.15 الخلاصة

قدم هذا الفصل شرحاً تفصيلياً للبنية البرمجية لنظام الحضور، بدءاً من المعمارية العامة، مروراً بتقسيم المكونات وتصميم قاعدة البيانات، وصولاً إلى آليات تسجيل الطالب والتحقق من الحضور والتحكم بالوصول وسجلات التدقيق. تشير النتائج العملية من لوحة التحكم وسجلات القاعدة إلى نجاح دمج التعرف على الوجه مع سياسات التفويض، مما يوفر نظام حضور أكثر انضباطاً وقابلية للتتبع مقارنة بالحلول التقليدية.

## الفصل الثاني

---

---

## الفصل الثالث

## الفصل الثالث

---

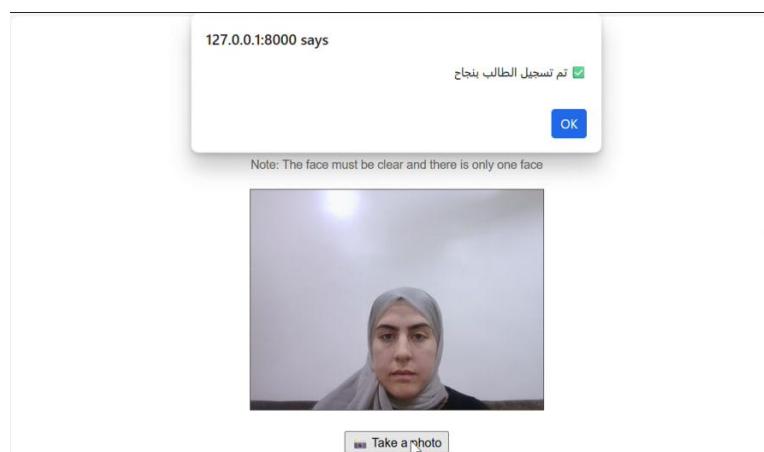
---

## الفصل الرابع

يهدف هذا الفصل إلى عرض وتحليل النتائج المتحققة من تنفيذ نظام تفهيم الحضور الإلكتروني المعتمد على التعرف على الوجه، والمدعوم ببنية برمجية وشبكية آمنة. ويركز الفصل على تقييم مدى نجاح التصميم المقترن في تحقيق أهداف المشروع، وذلك من خلال تحليل نتائج التشغيل العملي، والاختبارات الوظيفية، والاختبارات الأمنية التي أجريت على النظام ضمن بيئه محاكاة تمثل مؤسسة تعليمية جامعية.

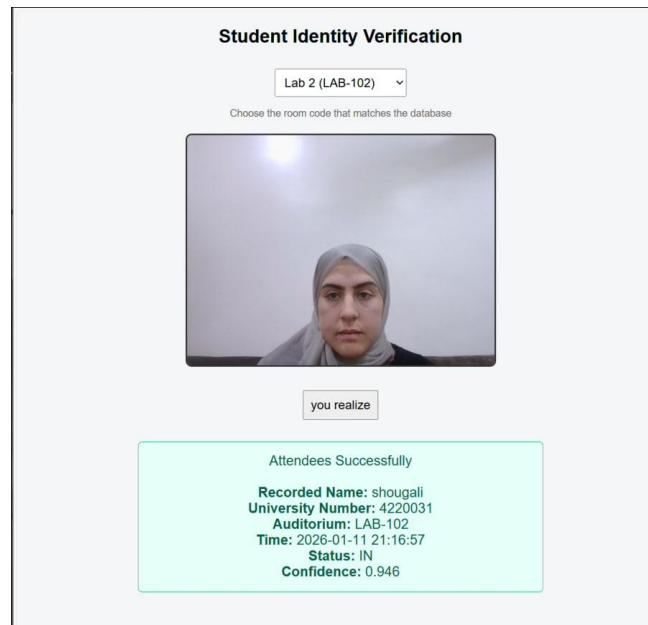
### 4.1 نتائج البنية البرمجية للنظام

أظهرت نتائج التنفيذ أن البنية البرمجية للنظام نجحت في تحقيق الوظائف الأساسية المطلوبة بكفاءة واستقرار. فقد تمكّن النظام من تنفيذ عمليات تسجيل الطلبة (Face Enrollment) واستخراج بصمة الوجه الرقمية (Face Embedding) باستخدام نموذج ArcFace، وربطها بهوية الطالب داخل قاعدة البيانات بشكل صحيح. كما أثبتت آلية التحقق (Verification) قدرتها على التعرف على الطلبة المسجلين بدقة مناسبة، وتسجيل الحضور تلقائياً دون تدخل بشري.

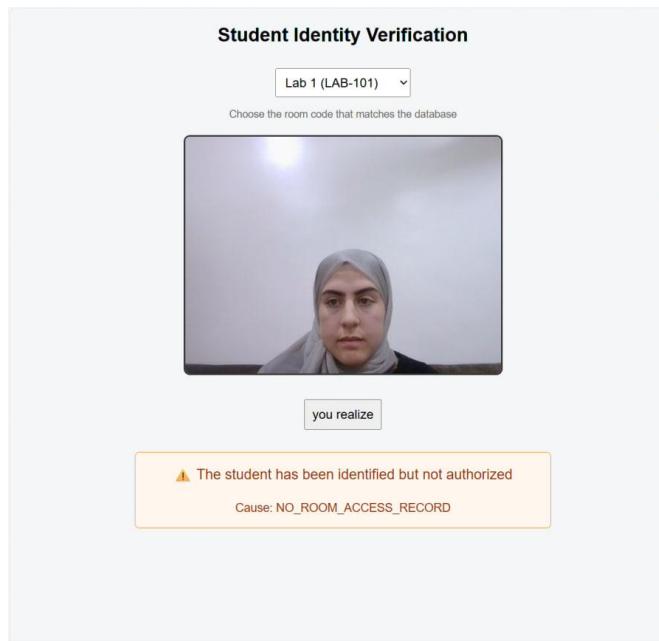


الشكل (4.1): نتائج التعرف على الوجه وتسجيل الحضور بنجاح

## الفصل الرابع



الشكل (4.2): نتائج عملية التحقق (Verification) وتسجيل الحضور مع قيمة الثقة



الشكل (4.3): نتائج عملية التتحقق (Verification) مع فشل التفویض (Authorization Failure)

| Attendance Record |           |          |                   |            |                      |  |
|-------------------|-----------|----------|-------------------|------------|----------------------|--|
| Trust             | Status    | The Hall | University Number | Student    | Time                 |  |
| 0.95              | FORBIDDEN | Lab 1    | 4220031           | shougali   | 12/01/2026, 00:17:10 |  |
| 0.95              | IN        | Lab 2    | 4220031           | shougali   | 12/01/2026, 00:16:57 |  |
| 0.85              | FORBIDDEN | Lab 2    | 4223311           | husain ali | 11/01/2026, 21:08:44 |  |
| 0.87              | IN        | Lab 1    | 4223311           | husain ali | 11/01/2026, 21:04:11 |  |

( الشكل (4.4): مثال على مخرجات نظام الحضور الإلكتروني (IN / FORBIDDEN)

كما بينت نتائج التشغيل أن الفصل بين منطق التعرف على الوجه ومنطق التفويض (Authorization) أسهم في تحسين موثوقية القرار النهائي، حيث لم يقتصر النظام على التعرف على هوية الطالب فقط، بل تحقق أيضًا من مدى أحقيته بالدخول إلى القاعة المحددة. وقد انعكس ذلك في تسجيل حالات متعددة مثل (OUT, FORBIDDEN, IN) بشكل واضح داخل لوحة التحكم.

## 4.2 نتائج البنية الشبكية والأمنية

أظهرت نتائج الاختبارات الشبكية أن البنية المعتمدة وفرت مستوى جيداً من العزل بين مكونات النظام المختلفة. فقد نجح استخدام البنية متعددة الطبقات ومنطقة العزل الشبكي (DMZ) في منع الوصول المباشر من شبكات المستخدمين إلى خوادم التطبيق وقواعد البيانات الداخلية، مما قلل من سطح الهجوم المحتمل.

كما أثبت تطبيق سياسات التحكم بالوصول باستخدام قوائم ACL فاعليته في حصر حركة المرور بالمسارات الضرورية فقط، حيث سُمح للمستخدمين بالوصول إلى واجهة النظام عبر الخادم الوسيط (Reverse Proxy) دون تمكين أي اتصال

## الفصل الرابع

مباشر بالخوادم الداخلية. وأظهرت الاختبارات أن أي محاولة وصول غير مصرح بها يتم حجبها وتسجيلها، مما يعزز الجانب الأمني للنظام.

### 4.3 نتائج التسجيل المركزي للأحداث والتدقيق

بيّنت نتائج التطبيق أن آلية التسجيل المركزي للأحداث (Centralized Logging) أسهمت في تعزيز قابلية المراقبة والتتبع. فقد تم تسجيل جميع العمليات الحساسة، مثل تسجيل الطلبة، ومحاولات التحقق الناجحة والفاشلة، ومحاولات الوصول غير المصرح بها، ضمن سجلات تدقيق واضحة تحتوي على معلومات السياق الزمني وعنوان الشبكة والنتيجة النهائية.

وقد أتاح ذلك إمكانية تتبع "من قام بماذا ومتى"، وهو ما يدعم مبدأ المحاسبة (Accountability) ويساعد في تحليل الأخطاء والحوادث الأمنية المحتملة، وبُعد مؤشرًا مهمًا على نضج التصميم الأمني للنظام.

### 4.4 مقارنة النتائج مع أهداف المشروع

عند مقارنة النتائج المتحققة مع الأهداف المحددة في الفصل الأول، يتضح أن النظام نجح في تحقيق معظم أهداف المشروع. فقد تحقق هدف أتمته عملية تفقد الحضور باستخدام التعرف على الوجه، والحد من التلاعب والانتحال، إضافة إلى بناء بنية برمجية مرنّة وقابلة للتتوسيع. كما تحققت الأهداف الأمنية المتمثلة في عزل المكونات الحساسة، وتطبيق مبدأ أقل صلاحية، ودعم المراقبة والتدقيق.

### 4.5 التحديات التي ظهرت أثناء التنفيذ

على الرغم من نجاح النظام في تحقيق أهدافه الأساسية، أظهرت النتائج بعض التحديات العملية، مثل تأثير دقة التعرف على الوجه في حالات الإضاءة غير المناسبة، وال الحاجة إلى ضبط عتبة الثقة (Threshold) بعناية لقليل حالات الرفض أو القبول الخاطئ. كما تطلب إعداد سياسات ACL وضبط الشبكة مراحل اختبار تدريجية لتفادي أخطاء الضبط التي قد تؤثر على استمرارية الخدمة.

### الخاتمة

في ظل التطور المتتسارع في التقنيات الرقمية والاعتماد المتزايد على الأنظمة الإلكترونية في المؤسسات التعليمية، برزت الحاجة إلى تطوير حلول تقنية موثوقة تسهم في تحسين الكفاءة الإدارية وضمان دقة العمليات الأكademية. وقد تناول هذا العمل تصميم دراسة نظام تفقد حضور إلكتروني يعتمد على تقنية التعرف على الوجه، بوصفها إحدى تقنيات القياسات الحيوية القادرة على معالجة أوجه القصور المرتبطة بالأساليب التقليدية المعتمدة في تسجيل الحضور.

وقد ركّز العمل على دمج الجوانب النظرية والتطبيقية المتعلقة بالبنية البرمجية والبنية الشبكية الآمنة، بما يسهم في بناء نظام يتمتع بدرجة مناسبة من الدقة والاعتمادية. كما أظهرت النتائج أن اعتماد مفاهيم مثل البنية متعددة الطبقات، ومنطقة العزل الشبكي، والتحكم بالوصول، يسهم في تعزيز مستوى الأمان وحماية البيانات الحساسة.

وفي ضوء ما تم التوصل إليه، يمكن اعتبار النظام المقترن خطوة داعمة نحو تطوير أنظمة تفقد حضور إلكترونية أكثر كفاءة وقابلية للتطبيق في المؤسسات التعليمية، مع إمكانية تطويره مستقبلاً لتحسين الأداء وتوسيع نطاق الاستخدام بما يتناشئ مع متطلبات التحول الرقمي في التعليم.

---

## قائمة المصطلحات

- البنية متعددة الطبقات (Three-Tier Architecture)
- التسجيل المركزي للأحداث (Centralized Logging)
- التشفير (Encryption)
- التشفير أثناء التخزين (Encryption at Rest)
- التشفير أثناء النقل (Encryption in Transit)
- التعلم العميق (Deep Learning)
- التعرف على الوجه (Face Recognition)
- الذكاء الاصطناعي (Artificial Intelligence – AI)
- العميل (Client)
- القياسات الحيوية (Biometrics)
- الجدار النارى (Firewall)
- الخادم (Server)
- خادم التطبيق (Application Server)
- خادم قاعدة البيانات (Database Server)
- كشف الوجه (Face Detection)
- قائمة التحكم بالوصول (ACLs – Access Control Lists)
- قاعدة البيانات (Database)
- منطقة العزل الشبكي (DMZ – Demilitarized Zone)
- نظام تفقد الحضور الإلكتروني (Electronic Attendance System)
- نموذج التعرف (Recognition Model)
- واجهة المستخدم (User Interface – UI)
- واجهة برمجة التطبيقات (API – Application Programming Interface)
- بصمة الوجه (Face Embedding)
- فصل الصالحيات والمهام (Separation of Duties)

---

## قائمة الاختصارات (List of Abbreviations)

- ACL — Access Control List
- AI — Artificial Intelligence
- API — Application Programming Interface
- CNN — Convolutional Neural Network
- CPU — Central Processing Unit
- DB — Database
- DMZ — Demilitarized Zone
- DNS — Domain Name System
- GUI — Graphical User Interface
- HTTP — HyperText Transfer Protocol
- HTTPS — HyperText Transfer Protocol Secure
- IAM — Identity and Access Management
- IP — Internet Protocol
- JWT — JSON Web Token
- LAN — Local Area Network
- ML — Machine Learning
- OS — Operating System
- RAM — Random Access Memory
- RBAC — Role-Based Access Control
- REST — Representational State Transfer
- SSL — Secure Sockets Layer
- TLS — Transport Layer Security
- UI — User Interface
- URL — Uniform Resource Locator
- WAN — Wide Area Network

---

## References

1. Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 4690–4699).  
[https://openaccess.thecvf.com/content\\_CVPR\\_2019/html/Deng\\_ArcFace\\_Additive\\_Angular\\_Margin\\_Loss\\_for\\_Deep\\_Face\\_Recognition\\_CVPR\\_2019\\_paper.html](https://openaccess.thecvf.com/content_CVPR_2019/html/Deng_ArcFace_Additive_Angular_Margin_Loss_for_Deep_Face_Recognition_CVPR_2019_paper.html)
2. Grother, P., Ngan, M., & Hanaoka, K. (2020). Face Recognition Vendor Test (FRVT) Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology.  
<https://doi.org/10.6028/NIST.IR.8280>
3. Fielding, R., & Reschke, J. (2014). Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing (RFC 7230). RFC Editor. <https://doi.org/10.17487/RFC7230>
4. Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). RFC Editor. <https://doi.org/10.17487/RFC8446>
5. Jones, M., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT) (RFC 7519). RFC Editor. <https://doi.org/10.17487/RFC7519>
6. Krawczyk, H., Bellare, M., & Canetti, R. (1997). HMAC: Keyed-Hashing for Message Authentication (RFC 2104). RFC Editor. <https://doi.org/10.17487/RFC2104>

- 
7. Eby, P. J. (2010). PEP 3333 – Python Web Server Gateway Interface (WSGI) v1.0.1. Python Enhancement Proposals. <https://peps.python.org/pep-3333/>
8. Django Software Foundation. (n.d.). Django documentation: Settings (Security settings, ALLOWED\_HOSTS, CSRF, Sessions, HSTS). Retrieved January 29, 2026, from <https://docs.djangoproject.com/en/5.0/ref/settings/>
9. Django REST framework. (n.d.). Authentication: TokenAuthentication. Retrieved January 29, 2026, from <https://www.django-rest-framework.org/api-guide/authentication/#tokenauthentication>
10. djangorestframework-simplejwt contributors. (n.d.). Simple JWT documentation (JWTAuthentication). Retrieved January 29, 2026, from <https://django-rest-framework-simplejwt.readthedocs.io/en/latest/>
11. Gunicorn Project. (n.d.). Gunicorn documentation: Settings (bind, workers, deployment). Retrieved January 29, 2026, from <https://docs.gunicorn.org/en/stable/settings.html>
12. World Wide Web Consortium (W3C). (n.d.). Media Capture and Streams (getUserMedia). Retrieved January 29, 2026, from <https://www.w3.org/TR/mediacapture-streams/>
13. OpenCV. (n.d.). OpenCV documentation: Color space conversions (cvtColor). Retrieved January 29, 2026, from <https://docs.opencv.org/>
14. ONNX Runtime. (n.d.). ONNX Runtime documentation (Python API / InferenceSession). Retrieved January 29, 2026, from <https://onnxruntime.ai/docs/>
15. Python Cryptographic Authority. (n.d.). cryptography documentation: Fernet (symmetric encryption). Retrieved January 29, 2026, from <https://cryptography.io/en/latest/fernet/>

- 
16. OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. <https://owasp.org/Top10/>
- 17 . Anti-Phishing Working Group. (2025, March 10). Phishing activity trends reports. APWG. Retrieved from <https://apwg.org/trendsreports/>
- 18 . Del Pozo, I., Iturralde, M., & Restrepo, F. (2018, August). Social engineering: Application of psychology to information security. In 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 108–114). IEEE. <https://doi.org/10.1109/FiCloudW.2018.00027>
- 19 . IBM. (2024, May). What is phishing? IBM. Retrieved from <https://www.ibm.com/think/topics/phishing>
- 20 .Mishra, S., & Soni, D. (2023). DSmishSMS—A system to detect smishing SMS. Neural Computing and Applications, 35(7), 4975–4992.  
<https://doi.org/10.1007/s00521-022-07724-4>
- 21 . Figueiredo, J., Carvalho, A., Castro, D., Gonçalves, D., & Santos, N. (2024). On the feasibility of fully AI-automated vishing attacks. arXiv preprint arXiv:2409.13793. <https://arxiv.org/abs/2409.13793>
- 22 . ISACA. (2024). State of cybersecurity 2024. ISACA. Retrieved from <https://www.isaca.org/resources/reports/state-of-cybersecurity-2024>
- 23 . Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social

---

network sites: A personality information processing model. *Computers & Security*, 94, 101862. <https://doi.org/10.1016/j.cose.2020.101862>

24. Yang, L., Zhang, J., Wang, X., Li, Z., Li, Z., & He, Y. (2021). An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features. *Expert Systems with Applications*, 165, 113863.

<https://doi.org/10.1016/j.eswa.2020.113863>

25. Basnet, R. B., Sung, A. H., & Liu, Q. (2011, July). Rule-based phishing attack detection. In *Proceedings of the International Conference on Security and Management (SAM)* (Vol. 1, No. 1, pp. 624–630). CSREA Press.

26. Safi, A., & Singh, S. (2023, February). A systematic literature review on phishing website detection techniques. *Journal of King Saud University – Computer and Information Sciences*, 35(2), 590–611.

<https://doi.org/10.1016/j.jksuci.2020.11.027>

27. Alsariera, Y. A., Alanazi, M. H., Said, Y., & Allan, F. (2024, June). An investigation of AI-based ensemble methods for the detection of phishing attacks. *Engineering, Technology & Applied Science Research*, 14(3), 14266–14274.

<https://doi.org/10.48084/etasr.6895>

7312. Rashid, H., Liaqat, H. B., Sana, M. U., Kiren, T., Karamti, H., & Ashraf, I. (2025, May). Framework for detecting phishing crimes on Twitter using selective features and machine learning. *Computers & Electrical Engineering*, 124, 110363.

<https://doi.org/10.1016/j.compeleceng.2025.110363>

- 
28. Asiri, S., Xiao, Y., Alzahrani, S., Li, S., & Li, T. (2023). A survey of intelligent detection designs of HTML URL phishing attacks. *IEEE Access*, 11, 6421–6443.  
<https://doi.org/10.1109/ACCESS.2023.3236247>
29. Alzaidah, R., Al-Shaikh, A., Al-Mousa, M. R., Khafajah, H., Samara, G., Alzyoud, M., Al-Shanableh, N., & Almatarneh, S. (2023, July). Website phishing detection using machine learning techniques. *Journal of Statistics Applications & Probability*, 13(1), 119–129. <https://doi.org/10.18576/jsap/130113>
30. Mat Rani, L., Mohd Foozy, C., & Mustafa, S. (2023, January). Feature selection to enhance phishing website detection based on URL using machine learning techniques. *Journal of Soft Computing and Data Mining*, 4(1), 30–41.
31. Albishri, A. A., & Dessouky, M. M. (2024, December). A comparative analysis of machine learning techniques for URL phishing detection. *Engineering, Technology & Applied Science Research*, 14(6), 18495–18501.  
<https://doi.org/10.48084/etasr.7267>
32. Sudar, K. M., Rohan, M., & Vignesh, K. (2024, August). Detection of adversarial phishing attack using machine learning techniques. *Sādhanā*, 49(3), 232.  
<https://doi.org/10.1007/s12046-024-02474-3>
33. Tamal, M. A., Islam, M. K., Bhuiyan, T., Sattar, A., & Prince, N. U. (2024, July). Unveiling suspicious phishing attacks: Enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. *Frontiers in*

34. Paithane, P. M. (2025, April). URLGuard: A holistic hybrid machine learning approach for phishing detection. International Journal of Information Engineering and Electronic Business, 17(2), 95–110. <https://doi.org/10.5815/ijieeb.2025.02.07>
35. Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S., & Joga, S. (2023). Phishing detection system through hybrid machine learning based on URL. IEEE Access, 11, 36805–36822. <https://doi.org/10.1109/ACCESS.2023.3272715>
36. Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. A. (2023, April). A deep learning-based innovative technique for phishing detection in modern security with uniform resource locators. Sensors, 23(9), 4403. <https://doi.org/10.3390/s23094403>
37. Asiri, S., Xiao, Y., & Li, T. (2023, December). PhishTransformer: A novel approach to detect phishing attacks using URL collection and transformer. Electronics, 13(1), 30. <https://doi.org/10.3390/electronics13010030>
38. Kavya, S., & Sumathi, D. (2025). Multimodal and temporal graph fusion framework for advanced phishing website detection. IEEE Access, 13, 74128–74146. <https://doi.org/10.1109/ACCESS.2025.3506278>
39. Remya, S., Pillai, M., Aparna, B., Subbareddy, S. R., & Cho, Y. (2025). BGL-PhishNet: Phishing website detection using hybrid model—BERT, GNN, and LightGBM. IEEE Access, 13, 47552–47569.

---

<https://doi.org/10.1109/ACCESS.2025.3378865>

. 40Gaffney, S., et al. (2022).

SQLite: Past, Present, and Future.

Proceedings of the VLDB Endowment, 15(12).

<https://www.vldb.org/pvldb/vol15/p3535-gaffney.pdf>