الجمهورية اليمنية
وزارة التربية والتعليم والبحث العلمي
الجامعة الإماراتية الدولية
كلية الهندسة وتكنولوجيا المعلومات

نظام تأمين وحماية أتمتة الأنظمة

عمل الطلاب كل من:

م	اسم الطالب	الرقم الأكاديمي
1	مصطفى عامر عمر خالد	2021030094
2	محمد احمد يحي القاضي	2021030310
3	احمد مجاهد احمد عبدالله	2021030240
4	عبدالعزيز عبدالله الصماط	2021030300
5	احمد محمد احمد السباعي	2021030301
6	عاصم عبدالله محمد السعيدي	2021030450

تحت إشراف

الدكتور/ جميل راشد

تقرير مشروع التخرج المقدم لقسم أمن المعلومات استكمالاً لمتطلبات الحصول على درجة البكالوريوس في أمن المعلومات

لسنة 1446هـ – 2025م

ABSTRACT

In light of the accelerating pace of digital transformation and organizations' increasing reliance on automation systems to manage their critical operations and sensitive data, there is an urgent need to enhance the protection and security mechanisms for these systems. This project primarily aims to design and develop an integrated system for securing and protecting automation systems, ensuring operational continuity, safeguarding data from unauthorized access or manipulation, and fostering trust in organizations' digital environments.

The project addresses current security challenges, such as weak data transfer protection, difficulty in precisely managing permissions, the absence of comprehensive audit logs, and low employee security awareness. To tackle these issues, the project proposes a multi-layered security framework that combines the latest technologies and practices. This includes implementing a precise role-based access control (RBAC) system, encrypting sensitive data during storage and transfer using strong algorithms, and integrating advanced authentication mechanisms such as multi-factor authentication (MFA) that includes biometrics and one-time passwords (OTP), along with linking each user to a specific device.

The project also focuses on providing a comprehensive audit log that documents all activities and operations within the system, facilitating the tracking of any security breaches and enhancing accountability. The project adopts the flexible Agile methodology in its development, ensuring continuous adaptation to requirements and testing of deliverable components. The system was implemented using Dart and SQL languages, relying on platforms like Supabase and PostgreSQL databases, which provides a robust and scalable architecture.

Comprehensive testing results demonstrate that the system possesses high resistance to common attacks, with efficient performance and fast response times. This project contributes to providing a practical and reliable solution for organizations seeking to enhance the security of their automated infrastructure, and offers valuable recommendations for future work, including integrating emerging technologies and improving user experience, thus affirming its capability to confront evolving security challenges in digital work environments.

الملخص

في ظل التطور المتسارع للتحول الرقمي واعتماد المؤسسات المتزايد على أنظمة الأتمتة لإدارة عملياتها الحيوية وبياناتها الحساسة، تبرز الحاجة الملحّة لتعزيز آليات الحماية والتأمين لهذه الأنظمة. يهدف هذا المشروع بشكل أساسي إلى تصميم وتطوير نظام متكامل لتأمين وحماية أتمتة الأنظمة، لضمان استمرارية العمليات، وحماية البيانات من الوصول غير المصرح به أو التلاعب، وتعزيز الثقة في البيئة الرقمية للمؤسسات.

يتناول المشروع التحديات الأمنية الراهنة، مثل ضعف حماية نقل البيانات، وصعوبة إدارة الصلاحيات بدقة، وغياب سجلات التدقيق الشاملة، وانخفاض الوعي الأمني لدى الموظفين. لمعالجة هذه المشكلات، يقترح المشروع إطاراً أمنياً متعدد الطبقات يجمع بين أحدث التقنيات والممارسات. يشمل ذلك تطبيق نظام صلاحيات دقيق يعتمد على الأدوار (RBAC)، وتشفير البيانات الحساسة أثناء التخزين والنقل باستخدام خوارزميات قوية، بالإضافة إلى دمج آليات مصادقة متقدمة مثل المصادقة متعددة العوامل (MFA) التي تشمل البصمة ورموز التحقق لمرة واحدة (OTP)، وربط المستخدم بجهاز محدد.

كما يركز المشروع على توفير سجل تدقيق شامل يوثق جميع الأنشطة والعمليات داخل النظام، مما يسهل تتبع أي خروقات أمنية ويعزز المساءلة. ويتبنى المشروع منهجية Agile المرنة في تطويره، مما يضمن التكيف المستمر مع المتطلبات واختبار الأجزاء القابلة للتسليم. تم تنفيذ النظام باستخدام لغات Dart وSQL، مع الاعتماد على منصات مثل Supabase وقواعد بيانات PostgreSQL، مما يوفر بنية قوية وقابلة للتوسع.

تُظهر نتائج الاختبارات الشاملة أن النظام يتمتع بمقاومة عالية للهجمات الشائعة، مع أداء فعال ووقت استجابة سريع. يساهم هذا المشروع في توفير حل عملي وموثوق للمؤسسات تسعى لتعزيز أمن بنيتها التحتية المؤتمتة، ويقدم توصيات قيمة للأعمال المستقبلية، بما في ذلك دمج التقنيات الناشئة وتحسين تجربة المستخدم، مما يؤكد على قدرته على مواجهة التحديات الأمنية المتطورة في بيئات العمل الرقمية..

التفويض

نُخوّل الجامعة الإماراتية كلية الهندسة بتزويد المكتبات أو الهيئات أو الأفراد بنسخ من تقرير مشروع تخرجنا عند الطلب، كما يُخوّل للكلية استخدامها في المسابقات المحلية والدولية.

م	اسم الطالب	التوقيع	تاريخ
1	مصطفى عامر عمر خالد		
2	محمد احمد يحيى القاضي		
3	احمد مجاهد احمد عبدالله		
4	عبدالعزيز عبدالله الصماط		
5	احمد محمد احمد السباعي		
6	عاصم عبدالله محمد السعيدي		

إقـــــــــرار

نُقرّ نحن الطلاب المذكورة أسماؤنا أدناه أن هذا المشروع قد تم إنجازه بجهودنا الفردية والجماعية، تحت إشراف الدكتور/ جميل راشد، وبمساهمة فاعلة من جميع أعضاء الفريق. كما نؤكد أن المشروع لم يتم نسخه أو اقتباسه من أي جهة خارجية إلا ما تم توثيقه صراحةً ضمن التقرير، وأن جميع البيانات والنتائج المدرجة تم الحصول عليها وتنفيذها في إطار المشروع البحثي الخاص بنا.

1. مصطفى عامر عمر خالد
2. محمد احمد يحي القاضي
3. احمد مجاهد احمد عبدالله
4. عبدالعزيز عبدالله الصماط
5. احمد محمد احمد السباعي
6. عاصم عبدالله محمد السعيدي

شهادة المشرف

أشهد بأن إعداد هذا المشروع بعنوان نظام تأمين وحماية أتمتة الأنظمة

أُعدت بواسطة.....

.....

.....

.....

.....

.....

.....

.....

.....

كانوا تحت إشرافي في قسم أمن المعلومات استكمالاً جزئياً لمتطلبات الحصول على درجة البكالوريوس في أمن المعلومات

أ.م.د/جميل راشد

لجنة المنافسة

عنوان المشروع: نظام تأمين وحماية أتمتة الأنظمة

المشرف

م	الاسم	الصفة	التوقيع
1	أ.م.د/جميـل راشـد	رئيس القسم	

لجنة الفاحصين

م	الاسم	الصفة	التوقيع
1			
2			
3			

رئيس القسم

الإهـــداء

"بكـــل فخـــر واعـــتزاز، نهـــدي هـــذا العمـــل المتواضـــع إلـــى مـــن كـــان لهـــم الفضـــل الأكـــبر في صـــناعته، إلـــى آبائنـــا اللـــذين كـــانوا لنـــا مـــلاذاً آمنـــاً ومصـــدر قـــوة وقـــدوة، شـــكراً لكـــم علـــى دعمكـــم اللامحـــدود وتضـــحياتكم الـــتي لا تُقـــدرَّ بـــثمن، إلـــى إخوتنـــا الأعـــزاء، أصـــدقائنا في الحيـــاة، شـــكراً لكـــم علـــى وجـــودكم الـــدائم بجانبنـــا وعلـــى تشـــجيعكم المســـتمر، وإلـــى أســـاتذتنا الأفاضـــل، الـــذين أفنـــوا أعمـــارهم في نشـــر العلـــم والمعرفـــة، شـــكراً لكـــم علـــى كـــل مـــا قـــدمتموه لنـــا مـــن علـــمٍ وخـــبرة، لا يســـعنا إلا أن نتوجـــه بخـــالص الشـــكر والعرفـــان لكـــل مـــن ســـاهم في إنجـــاز هـــذا المشـــروع، فـــأنتم جميعـــاً جـــزء لا يتجزأ من نجاحنا"

جدول المحتويات

قائمة الأشكال

فهرس الجداول

الفصل الأول

1.1. المقدمة:

في عصر يشهد تسارعاً غير مسبوق في تبنّي التحول الرقمي، أصبحت المؤسسات تعتمد بشكل جوهري على الأنظمة الإلكترونية لإدارة بياناتها وعملياتها الحيوية. هذا الاعتماد المتزايد، رغم فوائده الكبيرة، أفرز تحديات أمنية معقدة تتطلب أنظمة ذكية ومؤمنة لضمان حماية المعلومات وحسن إدارتها. من هذا المنطلق، جاءت هذه الدراسة لتسلّط الضوء على أهم الركائز التي تقوم عليها بيئة العمل الرقمية الآمنة، والتي يمكن تناولها من خلال المحاور التالية:

1.1.1. أولاً: تأمين البيانات:

في ظل التحول الرقمي المتسارع، أصبحت البيانات الأصول الأكثر حساسية في المنظمات الحديثة، مما يستدعي تأمينها ضد التهديدات الرقمية المتنوعة. تشمل عمليات التأمين استخدام بروتوكولات اتصال مشفّرة، ومصادقة متعددة العوامل، ونُظم مراقبة صارمة لضمان سرّية البيانات وسلامتها وتوفرها.

1.1.2. ثانياً: حماية البيانات:

لا يكفي تأمين قنوات الوصول إلى البيانات، بل من الضروري ضمان حماية البيانات نفسها أثناء التخزين والمعالجة والنقل. ويتم ذلك عبر آليات مثل التشفير القوي، وتحديد صلاحيات دقيقة للوصول، وتوثيق كامل للعمليات المرتبطة بالبيانات الحساسة. فالحماية الناجحة تقلل من احتمالات التسريب أو التلاعب أو الاستخدام غير المشروع.

1.1.3. ثالثاً: الأنظمة المؤتمتة:

باتت الأنظمة المؤتمتة العمود الفقري لإدارة العمليات المؤسسية، لما توفره من كفاءة في الأداء ودقة في المعالجة. إلا أن هذه الأنظمة تحمل تحديات أمنية متزايدة، منها ضعف الصلاحيات، غياب التوثيق اللحظي للعمليات، أو القابلية للاختراق عند غياب تدابير الحماية، ما يتطلب دمج عناصر الأمن في بنية النظام منذ التصميم.

1.1.4. رابعاً: أهمية الدراسة:

تُعد هذه الدراسة استجابة عملية لحاجة المؤسسات إلى حلول آمنة لإدارة عملياتها المؤتمتة. إذ يهدف المشروع إلى تطوير نظام ذكي يدمج بين تقنيات التوثيق البيومتري، وإدارة الصلاحيات، والتشفير، ومراقبة الأنشطة في الوقت الفعلي، مما يُسهم في رفع مستوى الأمان وتعزيز الكفاءة الإدارية. وبذلك تمثل هذه الدراسة خطوة نحو بناء بنية تحتية رقمية آمنة ومستدامة داخل بيئة العمل المؤسسي.

1.2. بيان المشكلة:

تواجه جميع الأنظمة الحديثة تحديات أمنية متزايدة، خاصة تلك الأنظمة المؤتمتة التي تعتمد على تداول المستندات والمعلومات الحساسة. من أبرز هذه التحديات عدم وجود حماية كافية لتبادل البيانات بين الموظفين، بالإضافة إلى غياب سجل دقيق يوثق حركة العمليات داخل النظام. لتسليط الضوء على هذه الثغرات الأمنية الجوهرية التي يسعى هذا المشروع لمعالجتها، يمكن تلخيص المشكلات الفرعية التالية في هيئة أسئلة بحثية:

1.2.1. عدم حماية نقل البيانات وحمايتها:

ما هي الآليات الأمنية الفعالة التي يمكن تطبيقها لضمان سرية وسلامة البيانات أثناء نقلها بين الموظفين والأنظمة في بيئة الأتمتة؟

1.2.2. وصول البيانات للمخولين أو عدم وصولها:

كيف يمكن تصميم نظام صلاحيات دقيق يضمن وصول المستخدمين المخولين فقط إلى المعلومات التي يحتاجونها لأداء مهامهم، ويمنع الوصول غير المصرح به للبيانات الحساسة؟

1.2.3. حماية البيانات في بيئة الدورة المستندية:

ما هي الإجراءات والتقنيات التي يمكن اتخاذها لتعزيز حماية المستندات والمعلومات الحساسة ضمن نظام الدورة المستندية، والحد من انتهاك خصوصيتها أو التلاعب بها، وتوفير رقابة دقيقة على حركة التعديل والعرض؟

1.2.4. إدارة البيانات:

كيف يمكن تنظيم وتخزين البيانات في النظام المؤتمت لضمان دقة السجلات وتحديثها، وتسهيل استخراج التقارير المطلوبة عن الحضور والأداء والإجازات؟

1.2.5. توعية الموظفين لحماية بياناتهم:

ما هي الاستراتيجيات الفعالة لرفع مستوى الوعي الأمني لدى الموظفين لتقليل السلوكيات غير الآمنة (مثل مشاركة كلمات المرور أو فتح الروابط المشبوهة)، وبالتالي حماية بيانات المؤسسة والموظفين من الاختراقات والوصول غير المصرح به؟

1.3. الهدف من الدراسة:

يهدف هذا المشروع بشكل أساسي إلى تصميم وبناء نظام صلاحيات متكامل يضمن إدارة الوصول الآمن والفعال إلى بيانات ومعلومات المؤسسة الحساسة، وذلك بتقييد الاطلاع والتعامل مع هذه البيانات بحيث يكون مقتصراً على المستخدمين المخولين فقط ووفقاً للصلاحيات المحددة لهم بدقة.

1.3.1. أهداف المشروع:

بالاستناد إلى الهدف العام للدراسة، يمكن تفصيل الأهداف الأمنية الرئيسية التي يسعى هذا المشروع لتحقيقها في النقاط التالية:

1.3.2. حماية تناقل البيانات:

تطبيق آلية أمان متقدمة تضمن سرية وسلامة البيانات المتبادلة بين الأنظمة والمستخدمين، وذلك من خلال استخدام تقنيات تشفير قوية للبيانات أثناء عملية التبادل.

1.3.3. تحقيق مبدأ الوصول بأقل صلاحية:

ضمان أن يتمكن كل مستخدم من الوصول إلى المعلومات والموارد الضرورية فقط لأداء مهامه، ومنع الوصول إلى أي بيانات لا تندرج ضمن صلاحياته المحددة.

1.3.4. توفير سجل تدقيق شامل:

إنشاء نظام تسجيل دقيق يوثق جميع الأنشطة والعمليات التي تتم داخل النظام، بما في ذلك محاولات الوصول، وتعديلات البيانات، وحركة المستندات، لضمان المساءلة وسهولة تتبع أي خروقات أمنية.

1.3.5. تعزيز أمان البيانات المخزنة:

تأمين البيانات الحساسة المخزنة ضمن النظام من خلال آليات حماية فعالة تمنع الوصول غير المصرح به والتلاعب بالمعلومات، مع التركيز على حماية المستندات في بيئة الدورة المستندية.

1.3.6. رفع الوعي الأمني للمستخدمين:

تضمين آليات أو توصيات لزيادة وعي المستخدمين بأفضل ممارسات الأمن السيبراني، لتقليل المخاطر الناجمة عن الأخطاء البشرية أو التصرفات غير الآمنة التي قد تؤدي إلى اختراق النظام أو تسريب البيانات.

1.4. الدوافع والمساهمة:

تأتي أهمية هذا المشروع ودوافعه من الحاجة الملحة لمعالجة جملة من التحديات الأمنية والتشغيلية التي تواجه أنظمة أتمتة المستندات والمعلومات في المؤسسات الحديثة. لقد لوحظت المشكلات الجوهرية التالية، والتي تشكل الدافع الرئيسي لتطوير نظام يوفر حماية معززة وفعالية أكبر:

ضعف في آليات تشفير البيانات أثناء التخزين والنقل: حيث أن غياب التشفير الكافي يعرض المعلومات الحساسة لخطر الوصول غير المصرح به أو التعديل أثناء انتقالها أو حتى أثناء تخزينها.

عدم وضوح في إدارة الصلاحيات للمستخدمين: مما يؤدي إلى صعوبة التحكم في وصول المستخدمين إلى البيانات، وينجم عنه إما منع الوصول عن المخولين أو السماح بالوصول لغير المخولين.

غياب سجل دقيق لتتبع حركة البيانات داخل النظام: والذي يعيق قدرة المؤسسة على متابعة الأنشطة، وتحديد المسؤوليات، واكتشاف أي خروقات أمنية أو عمليات تلاعب بالبيانات.

انخفاض مستوى الوعي الأمني لدى الموظفين: الذي يشكل نقطة ضعف رئيسية يمكن استغلالها من قبل المهاجمين، حيث قد تؤدي الأخطاء البشرية إلى تسريب البيانات أو تعريض النظام للخطر.

سوء تنظيم البيانات داخل النظام المؤتمت: مما يؤثر سلباً على كفاءة العمليات، ويجعل من الصعب إدارة واسترجاع المعلومات بدقة، ويزيد من مخاطر فقدان البيانات أو تلفها.

يهدف هذا المشروع، من خلال معالجة هذه المشكلات، إلى المساهمة في توفير بيئة عمل رقمية أكثر أماناً وكفاءة، تمكن المؤسسات من حماية أصولها المعلوماتية وتعزيز ثقة مستخدميها في الأنظمة المؤتمتة.

1.5. تعريف النظام أو المشروع

يُعرف المشروع بأنه نظام معلومات مؤتمت يهدف إلى إدارة الدورة المستندية داخل المؤسسات بطريقة آمنة وفعّالة. يعتمد النظام على تطبيق Android يوفر للمستخدمين واجهة سهلة الاستخدام لتنفيذ المهام الإدارية، مع دمج تقنيات أمنية متقدمة لضمان حماية البيانات ومنع الوصول غير المصرّح به، يتضمن النظام المكونات الأساسية التالية:

- نظام صلاحيات دقيق (RBAC) لإدارة وصول المستخدمين.
- تشغيل المصادقة الثنائية باستخدام البصمة وOTP.
- تشفير المستندات والبيانات الحساسة داخل قاعدة البيانات.
- تسجيل شامل للعمليات (Logs) لمراقبة التفاعلات داخل النظام.
- إدارة الحضور باستخدام GPS والتوثيق البيومتري.

1.6. منهجية عمل المشروع

تم اعتماد منهجيةAgile لتطوير هذا المشروع، وهي منهجية مرنة تتيح تقسيم العمل إلى دورات تطوير قصـــيرة (Sprint) بما يُمكّن الفريق من اختبار أجزاء قابلة للتنفيذ من النظام وتحديثها بشكل مستمر وفقاً للتغذية الراجعة، وتتمثل مراحل العمل في المنهجية على النحو الآتي:

- **التحليل:** دراسة المتطلبات وتحليل النظام المطلوب.
- التصميم: وضع الهيكل العام للنظام، وتصميم واجهات الاستخدام وقواعد البيانات.
- **البرمجة:** تنفيذ الوظائف البرمجية باستخدام لغات Dart وSQL.
- **الاختبار:** فحص جودة العمل والتأكد من خلو النظام من الأخطاء.
- **المراجعة:** تقييم النتائج وتحسين جودة المنتج.
- **الإطلاق التجريبي:** تقديم نسخة أولية قابلة للاستخدام والتقييم.

1.7. تنظيم المشروع

تم تنفيذ المشروع من قِبل أعضاء فريق، حيث تم توزيع المهام بشكل يُراعي كفاءة وقدرات كل عضو في الفريق، لضمان إنجاز جميع مراحل المشروع بكفاءة.

- **فريق التحليل والتخطيط:** مسؤول عن جمع المتطلبات وتحليل النظام.
- **فريق البرمجة:** تولى تطوير التطبيق وتنفيذ البنية البرمجية.
- **فريق أمن المعلومات:** ركز على تطبيق عناصر الحماية والتشفير.
- **فريق التوثيق:** قام بإعداد الوثائق والتقارير الخاصة بالمشروع.

الفصل الثاني

الدراسة الفنية للمشروع

2.1. مقدمة الفصل / الخلفية النظرية للمشروع:

رغم المزايا الكبيرة التي توفّرها أنظمة الأتمتة، إلا أنها أصـــبحت في الوقت ذاته بيئة خصبة للهجمات الإلكترونية والتجاوزات الأمنية. فمع كل خطوة نحو الرقمنة، يظهر تحدٍ جديد يتطلب حلولاً أمنية متقدمة لحماية البيانات الحساسة من التسريب أو التلاعب أو الفقدان، تشـير التقارير العالمية في أمن المعلومات إلى أن نسـبة الهجمات السـيبرانية على الأنظمة المؤتمتة قد ارتفعت بنســـبة تتجاوز 30% في الســـنوات الأخيرة، وتتركز هذه الهجمات على الثغرات في إدارة الصلاحيات، ضعف التشفير، وعدم وجود توثيق دقيق لحركة البيانات. بل أن بعض الدراســـات تشـير إلى أن أكثر من 60% من الاختراقات تحدث نتيجة خطأ بشـــري أو ضـــعف الوعي الأمني لدى الموظفين، مما يُبرز أهمية دمج ممارسات التوعية داخل بيئة العمل المؤتمتة.

في هذا الســـياق، برزت الحاجة إلى إنشـــاء أنظمة مؤتمتة لا تقتصـــر على توفير الوظائف الإدارية بل تُدمج فيها مكونات أمنية متكاملة تتضمن: التحقق البيومتري، التشفير القوي، المصـــادقة متعددة العوامل، تتبع سجل العمليات (Logs)، وتحديد الموقع الجغرافي. كما ينبغي أن تكون هذه الأنظمة مرنة، قابلة للتكامل مع الأنظمة الأخرى، وســـهلة الاستخدام لضمان قبولها داخل المؤسسات.

يهدف هذا المشـــروع إلى تقديم نموذج متكامل لنظام تأمين وحماية أتمتة أنظمة الخدمات الإدارية، يعالج الثغرات الشـــائعة ويوفر بيئة رقمية أكثر أماناً وموثوقية، ويعتمد على

منهجيات تطوير حديثة (مثل Agile)، ولغات برمجة مرنة (Dart وSQL)، ويُنفذ على منصة Android لسهولة الوصول والتنقل.

2.2. الدراسات السابقة

اعتمد المشروع في تطوير فكرته وتنفيذها على مراجعة مجموعة من الدراسات السابقة والأبحاث العلمية التي تناولت موضوع أمن المعلومات في أنظمة الأتمتة. وقد تم التركيز على الأبحاث التي تتقاطع في ثلاث مجالات رئيسية: أمن الأنظمة المؤتمتة، التحكم في الوصول، والمصادقة متعددة العوامل.

2.2.1. أولاً: أمن الأنظمة المؤتمتة

- (Zhou et al., 2020): قدّموا دراسة حول التهديدات المحتملة في أنظمة [Workflow Management Systems] وأوصوا بضرورة اعتماد أنظمة صلاحيات مرنة مع تشفير قوي لضمان سلامة العمليات.
- (Nguyen et al., 2021): ناقشوا أهمية وجود سجل دقيق لحركة البيانات داخل الأنظمة المؤتمتة، وأوصوا بإنشاء Logs مفصلة يمكن الرجوع إليها في حالات الشك أو التحقيق.

2.2.2. ثانياً: التحكم في الوصول (Access Control)

- بحثت دراسة نشرت في IEEE Transactions on Information Forensics and Security في مدى فعالية أنظمة التحكم في الوصول القائمة على الأدوار (RBAC) مقارنة بأنظمة DAC وMAC، وتوصّلت إلى أن RBAC هو الأنسب لبيئات العمل الديناميكية، كما هو الحال في هذا المشروع.
- دراسات أخرى بيّنت ضرورة مراجعة الصلاحيات بشكل دوري لضمان عدم احتفاظ المستخدمين السابقين أو المنتهية خدماتهم بصلاحيات داخل النظام، وهو ما يُعد من أهم مصادر التسريبات الأمنية.

2.2.3. ثالثاً: المصادقة متعددة العوامل (MFA)

- بحث منشور في Journal of Cybersecurity عام 2022 تناول مزايا دمج المصادقة البيومترية مع المصادقة السحابية (OTP)، وأثبت أن ذلك يرفع مستوى الأمان بنسبة تفوق 85% مقارنة بالأنظمة التقليدية التي تعتمد على اسم المستخدم وكلمة المرور فقط.
- كما أشارت دراسة أخرى إلى أن المستخدمين يفضلون المصادقة البيومترية بسبب سهولتها، مما يُسهم في تعزيز تجربة الاستخدام دون التضحية بالأمان.

2.2.4. رابعاً: الوعي الأمني والتدريب

- بحث بعنوان "The Role of User Awareness in System Security" نُشر في مجلة Computers & Security أظهر أن تعزيز وعي الموظفين بأمن المعلومات يُقلّل من احتمالية الوقوع في هجمات الهندسة الاجتماعية بنسبة تصل إلى 70%.

2.2.5. خلاصة الدراسات:

كل الدراسات السابقة أجمعت على أن تحقيق الأمان في أنظمة الأتمتة يتطلب مزيجاً من:

- بنية تقنية محمية (تشفير – مصادقة – صلاحيات).
- سجل عمليات شفاف.
- توعية مستمرة للمستخدمين.
- مراجعة دورية للثغرات وإجراءات التحديث.

وقد استند هذا المشروع إلى تلك المبادئ في بناء النظام المقترح، مما يجعله منسجماً مع أحدث ما توصل إليه البحث العلمي في هذا المجال.

تبين الجداول التالية الدراسات السابقة:

Recommendations	Results	Methodology	Objectives	Problem	Title
- Broaden implementation of automation systems. - Continuous development and training on system usage. - Regular system updates for security and efficiency.	- Significant improvement in employee satisfaction and task completion speed.	- Needs analysis through surveys and interviews. - Developed an automated system with modern technologies. - Tested the system to ensure user needs are met.	- Improve operational efficiency. - Enhance productivity, reduce errors, and improve employee experience.	Institutions face challenges in efficiently managing employee services, such as delays in request processing, attendance tracking issues, and difficulty accessing critical information.	Employee Services Automation System

الجدول (1.1): تقنيات الحماية التقنية المستخدمة في الأنظمة المؤتمتة

Recommendations	Results	Methodology	Objectives	Problem	Title	Researcher and Date
- Enhance management support and employee training. - Upgrade technological infrastructure. - Leverage advanced MIS features to optimize operations.	- Need for stronger management support. - Importance of modern networks and advanced MIS capabilities.	- Descriptive analytical approach. - Survey of 262 employees at a telecom company. - Data analysis using SPSS software.	- Understand MIS impact on employee performance. - Evaluate the current performance levels. - Explore employee perspectives on MIS needs.	Assess the ability of MIS systems to meet user needs and improve operational efficiency.	Impact of Computerized MIS on Employee Performance	Al-Omari (2009)

الجدول (1.2): أنواع الهندسة الاجتماعية الشائعة وتأثير الوعي عليها

Recommendations	Results	Methodology	Objectives	Problem	Title	Researcher and Date
- Provide trained personnel for automation. - Reduce development costs with effective financing plans	The study highlightsthe importance of office automation systems to enhance the efficiency and effectiveness of human resources administrative	Descriptive methodology. - Data collection from secondary sources.	-Assess the reality of applying office automation in personnel departments. - Clarify the role of automation in planning, recruitment, selection, training needs, and resource evaluation.	Automation enhances administrative effectiveness. - Challenges include lack of skilled staff, high development costs	Automation and its Role in Improving Personnel Management Performance in Government Ministries in Gaza	Zaarb (2008)

الجدول (1.3): دور سجل العمليات في تعزيز الأمان

Recommendations	Results	Methodology	Objectives	Problem	Title	Researcher and Date
Invest in MIS infrastructure and training. - Reduce administrative complexity via automation.	Strong correlation between MIS usage and operational efficiency. - Limited adoption of advanced technologies.	Data collection from literature and a survey of 270 employees in a public finance department. - Statistical analysis using SPSS software	Analyze the application of management information systems (MIS) in public finance departments	Challenges like bureaucracy, complex procedures, and reliance on manual data handling hinder administrative performance.	The Role of Management Information Systems in Public Administration Issues	Nader et al. (2008)

الجدول (1.4): تأثير التدريب المستمر على تقليل المخاطر الأمنية

Recommendations	Results	Methodology	Objectives	Problem	Title	Researcher and Date
Develop policies to maximize technological benefits	Office automation is vital but underutilized beyond basic applications like word processing and photocopying	Data collection from books, journals, and interviews Statistical analysis using Minitab software	Identify actual usage levels of office automation systems. - Explore key investment areas and challenges in adopting such technologies	Challenges include traditional activity burdens, outdated technology	Determining Levels of Office Automation Utilization	Tawfiq (2010)

الجدول (1.5): مراجعة الثغرات وتحديث الأنظمة في الدراسات السابقة

2.3. الدراسة الحالية

في ضوء مراجعة الدراسات السابقة المتعلقة بأمن الأنظمة المؤتمتة، يظهر أن معظم المشاريع ركّزت على جانب واحد من جوانب الحماية، مثل إدارة الصلاحيات أو التوثيق البيومتري، دون تقديم حلول متكاملة تعالج التحديات الأمنية من منظور شامل. على خلاف ذلك، تميّزت الدراسة الحالية بتقديم نموذج أمني متكامل يجمع بين تقنيات التحقق المتعددة (OTP، البصمة، الموقع الجغرافي)، وتشفير البيانات الحساسة، وإدارة الصلاحيات المستندة إلى الأدوار (RBAC)، إلى جانب اعتماد واجهة محمولة سهلة الاستخدام مبنية على Android.

بالإضافة إلى ذلك، اعتمد المشروع على أدوات حديثة مثل PostgreSQL وSupabase التي تتيح تطبيق صلاحيات دقيقة على مستوى الصفوف (RLS)، وربط كل مستخدم بجهاز محدد وتسجيل سجلات الحركة (Logs) بتفصيل دقيق، مما يوفّر بنية أمنية تُعتبر أكثر شمولاً من الأنظمة التقليدية. كما تم دعم النظام بلوحة تحكم إدارية (Admin Panel) تسمح بمتابعة العمليات وتوزيع الصلاحيات والتنبيهات بشكل فعّال.

هذه التركيبة تجعل من المشروع الحالي ليس مجرد تطبيق أمني، بل بنية متكاملة للتأمين والتحكم والمراقبة داخل بيئة العمل المؤتمتة، مع قابلية التوسع والربط بأنظمة أخرى مستقبلاً، ما يُعزز مكانته مقارنة بالأبحاث والتطبيقات السابقة في المجال نفسه.

رغم تعدد المشاريع التي استهدفت بناء أنظمة مؤتمتة، إلا أن هذا المشروع يتميز بعدة جوانب:

- الدمج المتكامل بين تقنيات التحققOTP، البصمة، والموقع الجغرافي) وهو أمر نادر في التطبيقات المؤسسية المحلية.
- تسجيل دقيق لحركة البيانات من خلال إنشاء Logs داخل قاعدة البيانات، ما يتيح إمكانية تتبع الأحداث والمراجعة الأمنية.
- تصميم يعتمد على واجهة محمولة (Android) سهلة الاستخدام ومرتبطة مباشرة ببيئة العمل.

- تشفير البيانات باستخدام خوارزميات قوية مثل Bcrypt لحماية كلمات المرور والبيانات الحساسة.
- استخدام قاعدة بيانات PostgreSQL عبر منصة Supabase مع صلاحيات وصول تفصيلية (RLS).
- واجهة إدارة للمشرفين (Admin Panel) تتيح التحكم الكامل بالصلاحيات والتنبيهات.

كل هذه الخصائص تجعل النظام أكثر شمولية من الأنظمة التقليدية التي غالباً ما تعتمد على طبقة واحدة من الحماية.

2.4. دراسة الجدوى:

تمت دراسة الجدوى للمشروع من جوانب متعددة كما يلي:

2.4.1. الجدوى التقنية:

النظام يعتمد على تقنيات مفتوحة المصدر (Flutter، Supabase)، مما يسهل التطوير والصيانة، ويوفر بيئة مرنة للتوسع المستقبلي دون الاعتماد على حلول تجارية مرتفعة التكلفة..

2.4.2. الجدوى الاقتصادية:

باستخدام أدوات مجانية ومجتمع دعم مفتوح المصدر، يمكن تقليل التكاليف التشغيلية والتطويرية. كذلك، يُمكن للأنظمة القائمة أن تتكامل بسهولة مع المشروع عبر واجهات API.

2.4.3. الجدوى التشغيلية:

النظام مصمم ليتوافق مع بيئات العمل القائمة، من خلال تطبيق محمول يدعم التحقق بالبصمة والوجه وOTP، ما يُسهّل عملية التبني والاعتماد عليه دون الحاجة لتغيير البنية التحتية الحالية.

2.4.4. الجدوى الأمنية:

اعتماد نظام صلاحيات دقيق، وتوثيق كامل للعمليات، وتشفير قوي للبيانات، يجعل النظام قادراً على مواجهة التهديدات السيبرانية المتزايدة.

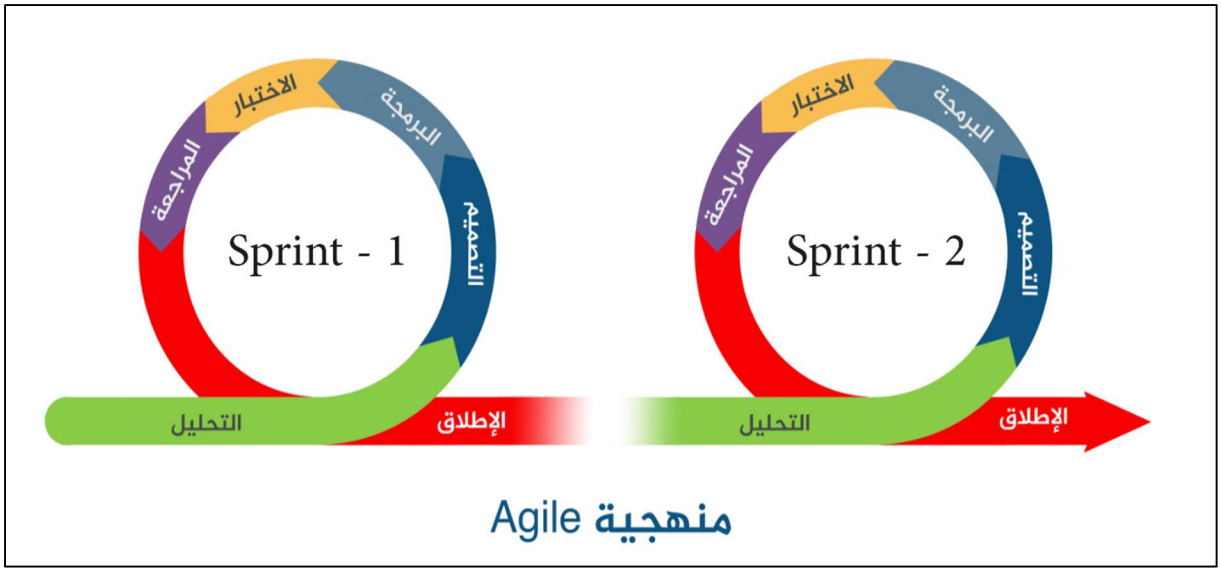
2.5. نطاق المشروع:

يمتد نظام أتمتة خدمات الموظف ليشمل مجموعة من الوظائف الإدارية الأساسية، مع التركيز على تأمين البيانات والعمليات، وضمان وصول آمن ومراقب للمعلومات، يشمل نطاق المشروع تطوير نظام متكامل لأتمتة خدمات الموظفين، مع التركيز على الجوانب التالية:

- إدارة الصلاحيات والوصول عبر نظام RBAC.
- تشغيل المصادقة الثنائية باستخدام OTP والبصمة.
- تشفير البيانات والمستندات الحساسة.
- ربط كل مستخدم بجهاز محدد مع منع الدخول المتعدد.
- تحديد الموقع الجغرافي عند تسجيل الدخول والخروج.
- تسجيل شامل لحركة العمليات داخل النظام باستخدام ملفات Logs.
- توفير لوحة تحكم للمشرفين لإدارة التنبيهات وتوزيع الصلاحيات.

النظام موجه بالأساس للمؤسسات الحكومية أو الخاصة التي تسعى إلى تأمين عملياتها الإدارية والتحكم في الوصول للبيانات.

2.6. منهجية المشروع:



شكل رقم (2.1) مخطط منهجية **Agile**

يعتمد المشروع على منهجية (**Agile Methodology**) لضمان تطوير آمن ومرن، ومن خلال (شكل رقم 2.1) يتبين ان لهذه المنهجية عدداً من المراحل على النحو التالي:

2.6.1. المبدأ الأساسي في (Agile):

a. الاعتماد على التحسين المستمر والتفاعل السريع مع التغيير.

b. تقسيم المشروع إلى دورات قصيرة تسمى Sprint.، في كل دورة، يتم تقديم جزء قابل للتسليم والتجربة من المنتج.

2.6.2. المراحل:

a. **التحليل (اللون الأخضر):**

- يتم في هذه المرحلة دراسة متطلبات العميل وتحليل ما يحتاجه النظام أو التطبيق.

b. **التصميم (الأزرق الغامق):**

- يتم رسم وتخطيط الهيكل العام للنظام بناءً على التحليل، بما في ذلك واجهات الاستخدام وقواعد البيانات.

c. **البرمجة (الأزرق):**

- يتم تنفيذ الكود البرمجي للوظائف المحددة.

d. **الاختبار (البرتقالي):**

- يتم التأكد من أن البرنامج يعمل بشكل صحيح من خلال اختبارات وظيفية وتقنية.

e. **المراجعة (البنفسجي):**

- يُراجع الفريق النتائج لمناقشة التحسينات والتعديلات.

f. **الإطلاق (الأحمر):**

- يتم إطلاق النسخة الأولى أو التجريبية للمستخدم، وغالباً ما تكون نسخة تحتوي فقط على الميزات الأساسية (Minimum Viable Product).

2.7. وظائف النظام (System Goals):

ينفذ نظام تأمين أنظمة الاتمته الالكتروني الوظائف التالية:

2.7.1. مراقبة العمليات:

مراقبة كافة العمليات التي تحدث على النظام حسب سياسة معتمدة لحفظ البيانات بشكل محدد، وتتم هذه العملية على النحو الآتي:

- يتم انشاء جداول لحفظ عمليات النظام داخل قاعدة البيانات بحيث يتم تسجيل بعض العمليات الخاصة بحركة البيانات التي تحدث على النظام لمراقبتها بشكل دوري ومبسط.
- اعتماد احداث (Logs) على قاعدة البيانات بحيث يتم الرجوع اليها في حال الحاجة الوصول الى حركة البيانات بشكل مفصل.

2.7.2. الصلاحيات:

عمل نظام صلاحيات آمن لتحديد صلاحيات المستخدمين المخول لهم من خلال:

- تطبيق أنظمة إدارة صلاحيات (RBAC - Role-Based Access Control) .
- مراجعة دورية لصلاحيات المستخدمين.
- تسجيل محاولات الوصول غير المصرح بها وتنبيه المسؤولين.

2.7.3. ربط الصلاحيات:

تأكيد ربط العمليات لكل مستخدم (User) على حدة، بتوقيع الكتروني فريد:

a- طلب فحص بصمة اليد أو الوجه قبل الدخول الى واجهة النظام.

b- ارسال رسائل تأكيد باستخدام تقنية (OTP) قبل اعتماد عمليات الطلبات الهامة عبر.

c- ربط جهاز واحد لكل مستخدم (User)، وحظر عمليات الدخول المتعدد.

2.7.4. حماية البيانات:

يجب حماية البيانات من خلال القيام بالتالي:

a- تشفير البيانات قبل انتقالها بين الموظفين.

b- حفظ كلمات المرور(Passwords) الخاصة بالمستخدمين مشفرة داخل قاعدة البيانات باستخدام خوارزمية (Bcrypt)، مع مراعاة ضرورة تغييرها بشكل دوري .

c- حماية قاعدة البيانات من خلال تأمينها وعمل نُسخ احتياطية (Back Up) متعددة تحفظ في امكان مختلفة ومؤمنه.

d- ربط نظام الحماية مع الأنظمة الأخرى عن طريقة تقنية API (Application Programming Interface).

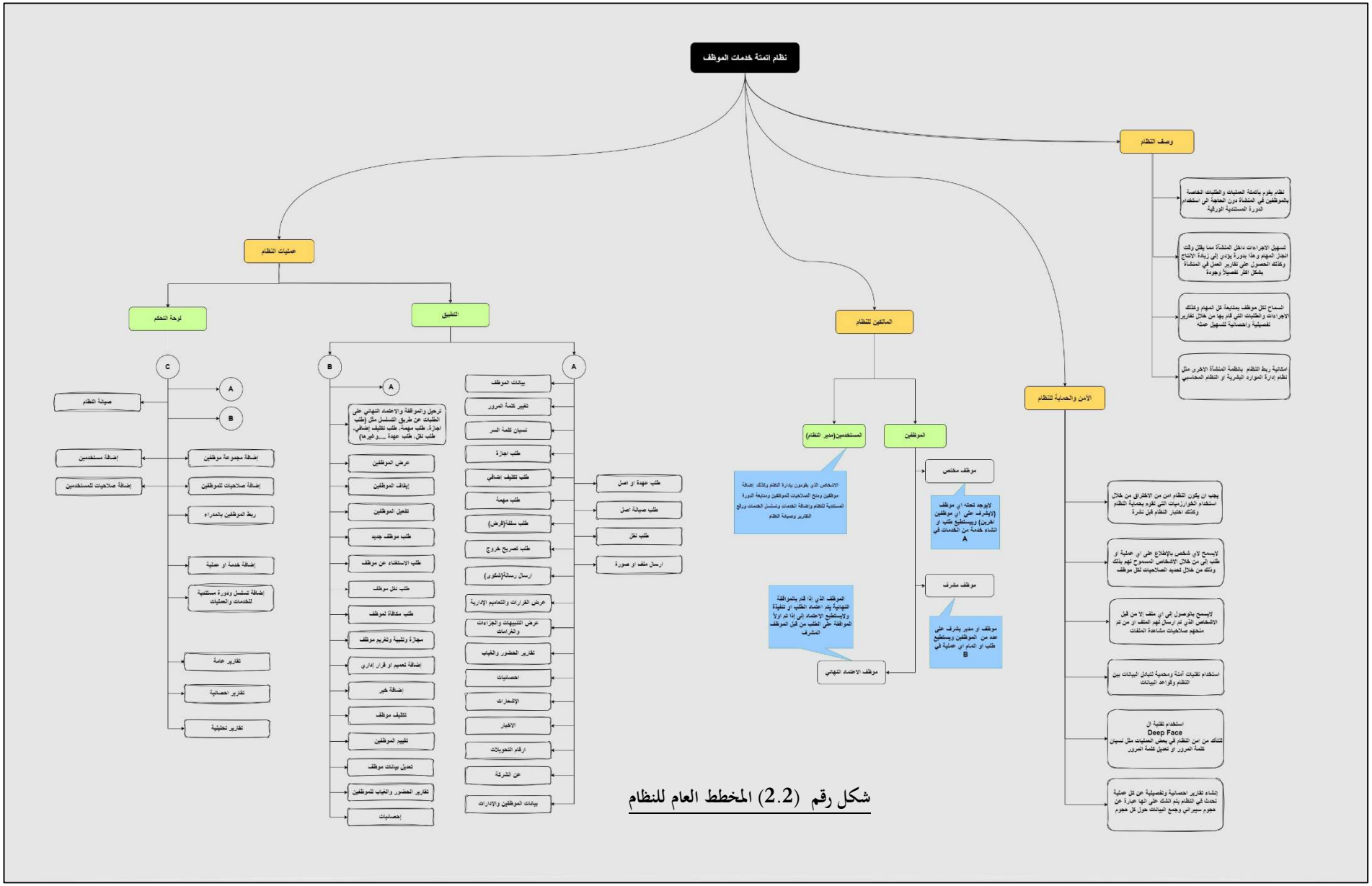
2.8. هيكل المشروع (Project Structure):

. من خلال تحليل نظام اتمتة يلبي احتياجات أي مؤسسة يجب ان يتم هيكلة المشروع على النحو الآتي:

1- تحليل عمل النظام من خلال تحديد أهدافه وكذلك تصميم مخطط للنظام وجميع المهام التي سوف يقوم النظام بإنجازها ويبين الشكل رقم (2.2) المخطط العام للنظام

2- قاعدة البيانات حيث تم استخدام قواعد البيانات (PostgreSQL) لحفظ البيانات ويمكن استخدام أي نوع من قواعد البيانات حسب المتاح في المؤسسة.

3- واجهة المستخدم حيث تم عمل تطبيق اندرويد (Android) يلبي الاحتياجات المطلوبة.



شكل رقم (2.2) المخطط العام للنظام

الفصل الثالث

التحليل

3.1. السيناريو العام للنظام:

يتضمن هذا النظام سيناريو عملي لتأمين وتحسين الخدمات الإدارية داخل بيئة العمل المؤسسية، من خلال تطبيق إلكتروني يسمح للموظف بتنفيذ عدد من الإجراءات (مثل تسجيل الحضور، تقديم الإجازات، استعراض المستحقات) بطريقة مؤتمتة وآمنة. يعتمد السيناريو على استخدام الهاتف المحمول لتسجيل الدخول، حيث يخضع المستخدم لعملية تحقق ثنائية تشمل البصمة وكود تحقق (OTP)، مع تسجيل الموقع الجغرافي.

عند تنفيذ أي عملية (مثل تقديم طلب إجازة)، يتم توجيه الطلب آلياً إلى المسؤول المختص وفقاً للبنية التنظيمية للمؤسسة، مع حفظ كل تفاعل داخل سجل حركة مفصل يمكن الرجوع إليه. يعزز هذا السيناريو الأمان والشفافية ويقلل الاعتماد على الإجراءات الورقية التقليدية.

3.2. دراسة الجدوى:

تمت دراسة الجدوى للمشروع من جوانب متعددة كما يلي:

- **الجدوى الفنية:** استخدام أدوات مفتوحة المصدر مثل Flutter وSupabase يوفّر بيئة تطوير فعالة من حيث الأداء والتكلفة. النظام يعمل على نظام Android لتسهيل اعتماده.
- **الجدوى التشغيلية**: سهولة الاستخدام والاعتماد على التحقق البيومتري يضمن تجربة مستخدم مريحة دون تعقيد.
- **الجدوى الاقتصادية**: تقليل التكاليف التشغيلية من خلال تقليل الورقيات والاعتماد على معالجة رقمية آمنة.
- **الجدوى الأمنية**: تقديم نظام متعدد الطبقات من الحماية يشمل التشفير، المصادقة الثنائية، والمراقبة المستمرة.

3.3. جمع المتطلبات:

تم جمع المتطلبات باستخدام عدة أدوات:

- مقابلات مع موظفين وإداريين داخل المؤسسة.
- استبيانات لتحديد الصعوبات في الأنظمة الحالية.
- تحليل النظام القائم ودراسة نقاط الضعف فيه.
- مراجعة أنظمة مماثلة للحصول على أفضل الممارسات.

هذه الخطوات مكّنت الفريق من بناء نموذج شامل لاحتياجات النظام المقترح.

3.4. متطلبات المستخدم

تشمل متطلبات المستخدم النهائية ما يلي:

- تسجيل الدخول عبر OTP والبصمة.
- تقديم طلبات (إجازة، شكوى، تحديث بيانات) بسهولة عبر التطبيق.
- استلام إشعارات بحالة الطلبات.
- إمكانية متابعة الحضور والمستحقات من خلال لوحة تحكم شخصية.
- الثقة في سرية البيانات وصحة المعالجة.

3.5. المتطلبات الوظيفية (Functional Requirements)

تم تحديد المتطلبات الوظيفية الأساسية كما يلي:

- تسجيل دخول المستخدم باستخدام OTP والمصادقة البيومترية.
- عرض معلومات الحساب الشخصية.
- تقديم طلبات إدارية (إجازات، شكاوى، مستحقات).
- إدارة الحضور والانصراف من خلال GPS والبصمة.
- حفظ كل عملية في قاعدة بيانات مع تفاصيل المستخدم.

- إمكانية رفض أو قبول الطلبات من قِبل المسؤول مع إشعار فوري.

3.6. المتطلبات غير الوظيفية (Non-Functional Requirements)

- **الأمان:** تشفير البيانات، وإجراءات تحقق صارمة.
- **الاعتمادية:** النظام يعمل بكفاءة دون انقطاع.
- **الاستجابة:** سرعة في تحميل الصفحات والعمليات.
- **قابلية الاستخدام:** تصميم سهل وبسيط يناسب جميع المستخدمين.
- **التوافق:** يعمل على كافة أجهزة Android الحديثة.

3.7. مخططات النظام

تتضمن مخططات النظام ما يلي:

- **مخطط تدفق البيانات** (DFD) : يوضّح تدفق الطلبات داخل النظام من المستخدم حتى المشرف.
- **مخطط هيكل النظام** (Architecture Diagram): يعرض البنية العامة للنظام من طبقة الواجهة، إلى طبقة الخوادم، إلى قاعدة البيانات.
- **مخطط قواعد البيانات:** يوضّح الجداول الأساسية، العلاقات، ومفاتيح الربط.

3.8. الخطة الأمنية لقواعد البيانات

- تشفير الحقول الحساسة داخل قاعدة PostgreSQL.
- تفعيل صلاحيات "Row-Level Security" لكل مستخدم.
- منع الوصول المباشر إلى قاعدة البيانات من أي طرف خارجي غير مصرّح.
- استخدام نسخ احتياطية تلقائية تحفظ في أماكن مؤمنة على فترات منتظمة.

3.9. الخطة الأمنية للأكواد البرمجية

- مراجعة الكود دورياً (Code Review) لاكتشاف الثغرات.
- استخدام مكتبات تحقق (Input Validation) لمنع إدخال أوامر خبيثة.
- حماية المفاتيح السرية (API Keys) باستخدام ملفات بيئية .env.
- منع الوصول إلى واجهات برمجية حساسة إلا من أجهزة مصرح لها.

3.10. الخطة الأمنية لنقل البيانات عبر الشبكة

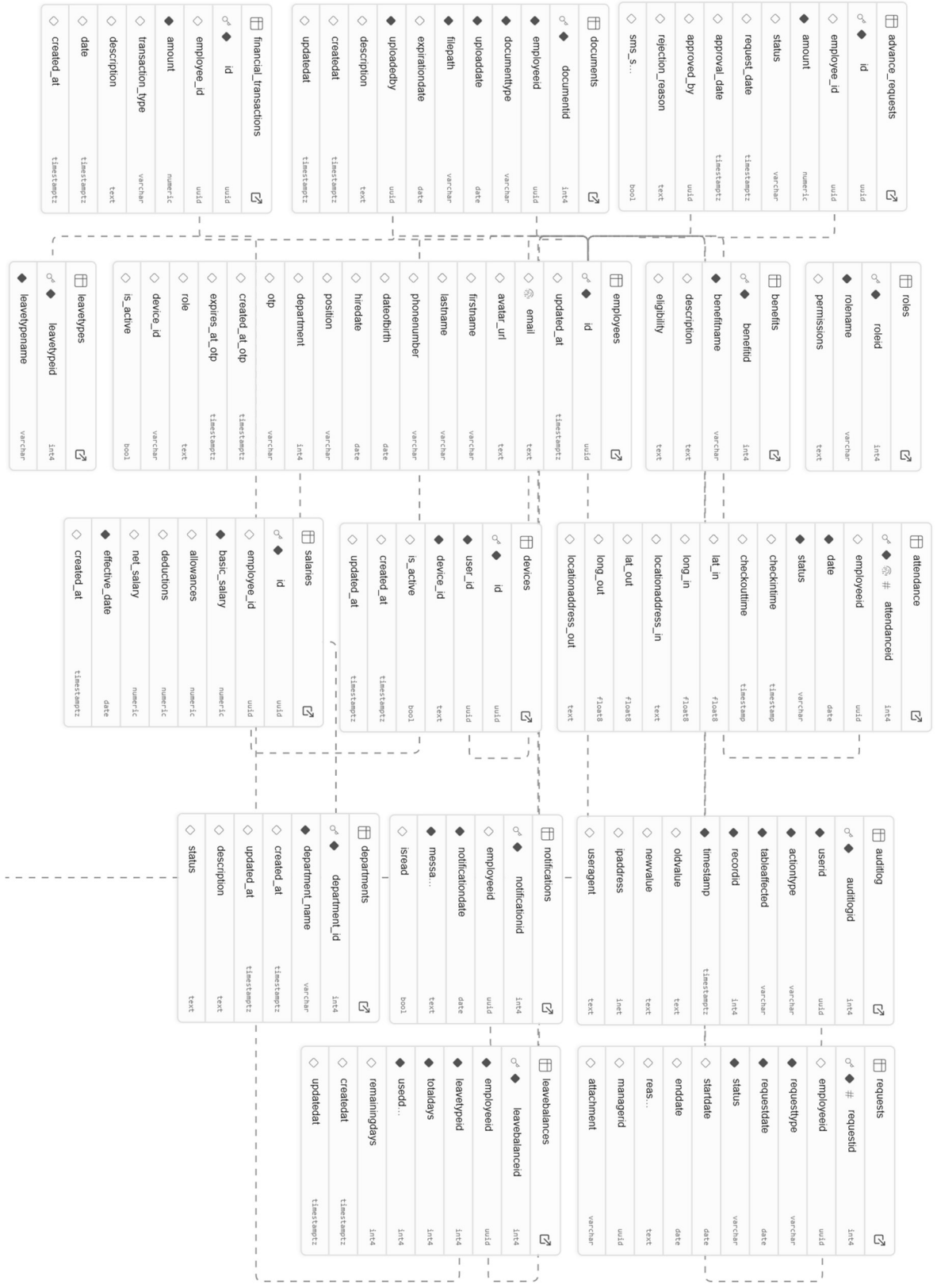
- استخدام بروتوكول HTTPS لتأمين الاتصال بين التطبيق والخادم.
- تشفير البيانات قبل الإرسال باستخدام AES.
- منع عمليات Man-in-the-middle عبر المصادقة الثنائية.
- مراقبة حركة البيانات وتحليلها بشكل دوري.

3.11. الخطة الأمنية للنظام بشكل عام

- استخدام نموذج الحماية متعدد الطبقات (Defense in Depth).
- تفعيل التحقق بخطوتين لجميع المستخدمين.
- تحديد الصلاحيات الدقيقة لكل فئة مستخدم باستخدام RBAC.
- تسجيل كل عملية في سجل أحداث Log لتدقيق الأمان.
- إرسال تنبيهات فورية للمشرفين عند محاولات الدخول الفاشلة المتكررة.

3.12. هيكل البيانات (Data Structure)

تعتبر البيانات اهم جزء في النظام ولا يمكن لأي نظام أن يعمل بالشكل المطلوب إن لم يحتوي على بيانات يتم حفظها واسترجاعها عند الاحتياج، ولكي يتم حفظ البيانات بشكل أفضل يتم انشاء جداول رئيسية وفرعية ويتم الربط بينها برمز او رقم بحيث لا يتم تضخم قاعدة البيانات والشكل رقم (3.1) يوضح الهيكل العام للبيانات.



شكل رقم (3.1) الهيكل العام للبيانات

3.12.1. أولاً: اللغات (Languages)

تعتمد عملية تطوير النظام على لغتين أساسيتين:

- لغة Dart: تُعد اللغة الأساسية المستخدمة في بناء التطبيقات باستخدام إطار عمل Flutter، وتُستخدم في تصميم الواجهات وتنفيذ المنطق البرمجي للتطبيق.
- لغة (SQL) ضمن: تُستخدم لإدارة قواعد البيانات، تنفيذ الاستعلامات، وإجراء العمليات على البيانات داخل قاعدة.

3.12.2. ثانيا: قواعد البيانات (Databases)

النظام يعتمد على قواعد بيانات قوية ومرنة تدعم الأمان والتخزين في الوقت الفعلي:

- Supabase (PostgreSQL): تُستخدم كقاعدة بيانات رئيسية مفتوحة المصدر، وتدعم المصادقة، التخزين، تنفيذ استعلامات SQL، وتحديث البيانات في الوقت الحقيقي، بالإضافة إلى دعم صلاحيات الوصول (RLS).
- Get Storage: تُستخدم لحفظ بيانات مؤقتة محلياً دون الحاجة للاتصال بالإنترنت.

وبإمكاننا استخدام أي نوع من أنواع البيانات حسب قاعدة البيانات المطلوبة من الشركة والمؤسسة

3.12.3. ثالثا: الأدوات (Tools)

تُستخدم الأدوات في تطوير تطبيقات أتمتة خدمات الموظفين لتسهيل عمليات معينة أو تنفيذ وظائف جاهزة، ومن أهمها:

- Get/GetWidget: تُستخدم لإدارة الحالة داخل التطبيق، والتنقل بين الصفحات، وتوفير مكونات واجهة استخدام جاهزة.
- HTTP: تُستخدم لتنفيذ طلبات REST API للتواصل مع الخوادم الخارجية وجلب البيانات.

- Connectivity Plus/Internet Connection Checker: تُستخدم للتحقق من وجود اتصال فعّال بالإنترنت لدى المستخدم.
- URL Launcher: تُتيح إمكانية فتح الروابط والمواقع الخارجية من داخل التطبيق.
- Get Storage: تُستخدم لتخزين البيانات مؤقتاً على جهاز المستخدم.
- File Picker / Image Picker: تُستخدم للسماح للمستخدم باختيار ملفات أو صور من جهازه.
- Logger: أداة تُستخدم لطباعة وتتبع العمليات والأحداث أثناء تطوير التطبيق.
- Flutter Test: أداة لتطبيق اختبارات وحدات النظام ووظائفه لضمان عملها بشكل سليم.
- Flutter Lints: تُستخدم لتحسين جودة الكود واكتشاف المشكلات البرمجية.
- Pinput: مكتبة متخصصة في تصميم واجهة إدخال رموز التحقق (OTP) بطريقة أنيقة وفعالة.

3.12.4. رابعا: المكتبات (Libraries)

المكتبات تُستخدم لإضافة خصائص جمالية وتفاعلية متقدمة داخل واجهة المستخدم، ومن أبرزها:

مكتبات المصادقة البيومترية

- local_auth: تُستخدم لتنفيذ المصادقة باستخدام البصمة أو التعرف على الوجه (Face ID/Touch ID).
- تدعم التحقق من توفر المستشعرات البيومترية على الجهاز.

مكتبات (Firebase) للتخزين السحابي والمصادقة

- firebase_auth: تتيح تسجيل الدخول باستخدام البريد الإلكتروني او رقم الهاتف
- تدعم إدارة المستخدمين وجلساتهم.
- cloud_firestore: قاعدة بيانات NoSQL سحابية تعمل في الوقت الفعلي.
- مناسبة لتخزين بيانات المستخدمين والتطبيقات.
- firebase_storage: تُستخدم لرفع وتخزين الملفات (مثل الصور والفيديوهات) على سيرفرات Firebase.

مكتبات التخزين المحلي

- get_storage: تخزن البيانات محلياً على الجهاز بسرعة عالية (بدون حاجة لقواعد بيانات معقدة).
- مناسبة لحفظ الإعدادات أو البيانات المؤقتة.

مكتبات معلومات الجهاز

- device_info_plus: تستخرج معلومات عن الجهاز (النموذج، نظام التشغيل، الإصدار، إلخ).
- unique_identifier: تحصل على رقم تعريف فريد مثل (IMEI أو UUID) للجهاز.

الاستخدام المشترك للمكتبات

- local_auth + firebase_auth: لتأمين الدخول بالمصادقة البيومترية والسحابية.
- get_storage + cloud_firestore: للتخزين المحلي والسحابي معاً.
- device_info_plus + unique_identifier: لتتبع الأجهزة وتحليل الاستخدام.

هذه المكتبات تُشكّل نظاماً متكاملاً لإدارة المستخدمين، التخزين الآمن، وجمع البيانات.

3.13. عمليات النظام

تعتمد عمليات النظام في مشروع "أتمتة خدمات الموظف" على تسلسل دقيق ومرن من الإجراءات التي تتم بين المستخدم والنظام بطريقة مؤمنة ومراقبة. وقد تم تصميم هذه العمليات لتغطي مختلف الجوانب الإدارية الوظيفية التي يحتاجها الموظف والإدارة، مع الأخذ بعين الاعتبار تحقيق أعلى مستويات الأمان والكفاءة.

3.13.1. عملية تسجيل الدخول

- يبدأ المستخدم بفتح التطبيق على جهازه المحمول.
- يقوم بإدخال اسم المستخدم ورمز OTP المُرسل إلى رقم هاتفه أو بريده الإلكتروني.
- يتم التحقق من بصمة الإصبع أو الوجه باستخدام المستشعر البيومتري في الجهاز.
- في حال المطابقة، يتم الدخول للنظام ويتم تسجيل بيانات الدخول (الوقت، الجهاز، الموقع) في قاعدة البيانات.

❖ **جوانب الأمان في صفحة تسجيل الدخول:**

1- حماية البيانات عبر الاتصال الآمن(HTTPS) :

- يتم تشفير الاتصال بين المستخدم والخادم باستخدام بروتوكول HTTPS ، مما يمنع اعتراض البيانات أثناء إرسالها، خصوصاً البريد الإلكتروني وكلمة المرور.

2- تشفير كلمة المرور:

- عند إدخال كلمة المرور، يتم إرسالها مشفرة إلى الخادم باستخدام خوارزميات مثل bcrypt أو SHA-256.
- لا يتم تخزين كلمات المرور بصيغتها الأصلية (Plain Text)، بل بصيغة مشفّرة يصعب اختراقها.

3- التحقق من صحة البيانات(Validation):

- يتم التحقق من صحة البريد الإلكتروني وصيغة كلمة المرور قبل الإرسال لتقليل فرص الهجمات من نوع SQL Injection أو XSS.

4- آلية منع الدخول غير المصرح به:

- يمكن أن يكون هناك قيود مثل: عدد محدد من المحاولات الفاشلة، ثم حظر مؤقت لحماية الحساب من محاولات الاختراق (Brute Force Attack).

5- التحقق بخطوتين (2FA):

- بعد إدخال البيانات الصحيحة، قد يُطلب من المستخدم إدخال رمز تحقق يُرسل إلى بريده الإلكتروني أو هاتفه كطبقة أمان إضافية.

6- عدم كشف الأخطاء الحساسة:

- تظهر رسائل خطأ عامة دون تحديد إذا كان البريد الإلكتروني أو كلمة المرور خاطئة لتقليل فرص التخمين من المخترقين.

3.13.2. عملية تسجيل الحضور والانصراف

- عند الدخول إلى مقر العمل، يفتح الموظف التطبيق ويقوم بتسجيل الحضور عبر البصمة.
- يتم التحقق من الموقع الجغرافي (GPS) للتأكد من وجوده داخل نطاق العمل.
- تسجّل العملية مع تفاصيل الوقت والموقع في النظام بشكل آلي.

3.13.3. تقديم الطلبات الإدارية

- يمكن للمستخدم تقديم طلبات مثل (إجازة، مستحقات، تحديث بيانات) من خلال واجهة المستخدم.
- يتم إرسال الطلب إلى المشرف المعني بناءً على هيكلية الصلاحيات (RBAC).

- يُشعَر المستخدم بأي تحديثات تخص حالته، سواء بالقبول أو الرفض، مع توثيق ذلك في سجل الأحداث.

3.13.4. مراجعة وإدارة الطلبات

- يمتلك المشرف لوحة تحكم تعرض الطلبات المُرسلة له مع كافة التفاصيل.
- يمكن للمشرف قبول أو رفض الطلب، وإضافة ملاحظات إن لزم.
- يتم إشعار الموظف بالقرار، وتُسجّل كل خطوة في سجل العمليات.

3.13.5. التحقق من النشاطات والتقارير

- يمكن للمستخدم استعراض تقرير مفصّل عن الحضور، الطلبات، والأداء الشهري.
- تُتاح للمشرفين إمكانيات توليد تقارير شاملة وتحليلية حول التفاعل داخل النظام.

3.13.6. معالجة الأخطاء الأمنية

- في حال حدوث محاولات دخول مشبوهة أو متكررة، يتم:
  - إرسال إشعار فوري للمسؤول.
  - قفل الحساب مؤقتاً.
  - تسجيل تفاصيل المحاولة (الموقع، الجهاز، الوقت) في قاعدة البيانات.

3.13.7. خلاصة العمليات:

يُدار النظام بطريقة تضمن سلامة العمليات من خلال تسجيل شامل (Logs)، والتحقق المتعدد (Biometric + OTP)، وربط كل عملية بتوقيع إلكتروني خاص بالمستخدم. كما تعتمد بنية النظام على تطبيق تسلسلي آلي للأحداث، ما يتيح سهولة في المتابعة، التحقيق، والتحسين المستمر.

الفصل الرابع

أتمتة الأنظمة

4.1. مقدمة حول تصميم النظام

تُعد مرحلة تصميم النظام من أهم المراحل في دورة حياة تطوير البرمجيات، حيث تُترجم خلالها المتطلبات التي تم جمعها وتحليلها إلى بنية فنية وهيكلية واضحة يمكن استخدامها في البرمجة والتنفيذ. ويُبنى عليها نجاح النظام من حيث الكفاءة والموثوقية وسهولة الاستخدام والأمان، في هذا المشروع، تم تصميم نظام تأمين وحماية أتمتة أنظمة الموظفين باستخدام منهجية تصميم موجه نحو المستخدم (User-Centered Design)، لضمان توافق الوظائف مع احتياجات المستخدمين من جهة، ومعايير الأمان المؤسسي من جهة أخرى. كما تم التركيز على تبسيط الواجهات وتقليل التعقيد، لضمان تجربة استخدام سلسة وآمنة.

يتضمن التصميم عدة مكونات رئيسية:

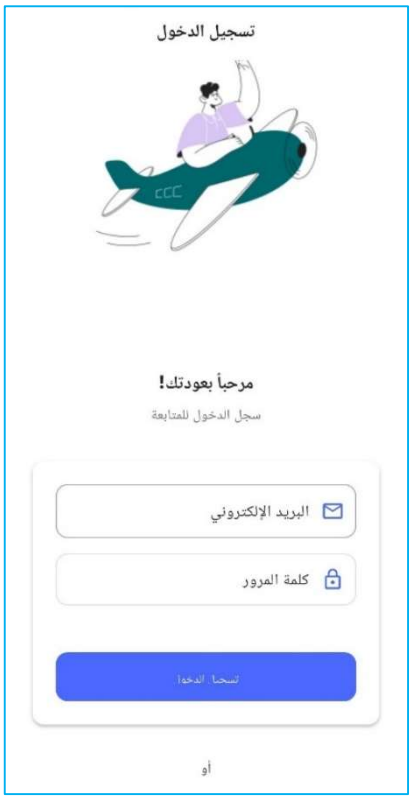
- تصميم قاعدة البيانات (Database Design): بما يشمل الجداول، العلاقات، المفاتيح الأساسية والربط المنطقي بين الكيانات.
- تصميم الواجهات الرسومية (UI Design): باستخدام أدوات مثل Flutter، مع مراعاة التناسق، وضوح المحتوى، وسهولة التنقل.
- تصميم البنية الأمنية (Security Architecture): من خلال إعداد نماذج صلاحيات، وطرق التحقق، وتشفير البيانات.
- تصميم منطق العمليات (Process Logic): يشمل تسلسل تنفيذ الوظائف وآلية التدفق بين شاشات النظام.

وقد تم تمثيل هذه التصاميم بمخططات متعددة مثل: مخطط تدفق البيانات (DFD)، مخطط الكيانات والعلاقات (ERD)، ومخططات واجهات الاستخدام (Wireframes)، لضمان توثيق شامل ومتكامل للنظام قبل البدء في عملية البرمجة والتنفيذ.

4.2. أهم واجهات النظام وفقاً للصلاحيات

شكل رقم (4.1) شاشة الترحيب

في الشكل رقم (4.1) الصورة تعرض شاشة الترحيب لتطبيق باللغة العربية. في منتصف الشاشة يظهر شعار التطبيق مع كلمة "مرحباً" وتحته عبارة "جرّب المستقبل اليوم". يوجد زران في الأسفل: الأول باللون الوردي مكتوب عليه "تسجيل الدخول"، والثاني باللون البنفسجي مكتوب عليه "إنشاء حساب". التصميم عصري بألوان جذابة وخلفية متدرجة من الوردي إلى البنفسجي مع تأثيرات بصرية خفيفة. الشاشة مخصصة للانتقال إلى صفحة تسجيل الدخول أو إنشاء حساب جديد



شكل رقم (4.2) شاشة "تسجيل الدخول"

الشكل رقم (4.2) تُظهر شاشة "تسجيل الدخول" للتطبيق، مكتوبة باللغة العربية. وتحتوي على:

1. عنوان "تسجيل الدخول" في الأعلى.
2. رسم تعبيري لشخص يطير بطائرة.
3. نص ترحيبي: "مرحباً بعودتك! سجل الدخول للمتابعة".
4. حقلي إدخال: واحد للبريد الإلكتروني، وآخر لكلمة المرور.
5. زر أزرق لتسجيل الدخول مكتوب عليه "تسجيل الدخول!"

6. في الأسفل يوجد خيار "أو" لتسجيل بديل (مثل عبر حساب آخر أو طريقة مختلفة).

من الجانب الأمني (الربط بجهاز واحد فقط):

لضمان أن الحساب لا يمكن استخدامه إلا من جهاز واحد، يمكن تنفيذ الآتي:

- جمع معرّف الجهاز (Device ID) أثناء تسجيل الدخول الأول (مثل Android ID أو UUID).
- تخزين معرف الجهاز المرتبط بالحساب في قاعدة البيانات الخلفية (Backend).
- التحقق عند كل محاولة تسجيل دخول ما إذا كان معرف الجهاز المستخدم مطابقاً لما هو مسجل.
- رفض تسجيل الدخول إذا تم استخدام حساب على جهاز غير معرّف.
- توفير آلية لتحديث الجهاز المرتبط فقط بإجراءات تحقق إضافية (مثل رمز OTP أو مراجعة من الدعم)

في الشكل رقم (4.3) تُظهر شاشة "إنشاء حساب جديد" في تطبيق ما، والمحتوى باللغة العربية. وتفاصيل الشاشة كالتالي:

1. العنوان: "إنشاء حساب جديد".
2. توجيه: "املأ التفاصيل الخاصة بك للبدء".
3. حقول الإدخال تشمل: الاسم الأول، رقم الهاتف، البريد الإلكتروني، كلمة المرور، وتأكيد كلمة المرور.

4. خيار للموافقة على "الشروط والأحكام".

5. زر أساسي بلون أزرق بعنوان "إنشاء حساب".

شكل رقم (4.3) شاشة "إنشاء حساب

4.3. الجانب الأمني وتخزين الـ Device ID:

في هذه المرحلة (أثناء إنشاء الحساب)، يتم تنفيذ الخطوة الأمنية التالية:

- جمع معرف الجهاز (Device ID)، مثل:
  - DeviceInfoPluginفي Flutter لجمع Android ID أو UUID.

- تخزين معرف الجهاز مع بيانات الحساب في قاعدة البيانات الخلفية(backend) ، مثل Firebase أو أي API مخصصة.

4.4. كيف يتم الربط فعلياً:

1. عند ضغط المستخدم على "إنشاء حساب":
   - تُرسل البيانات التالية إلى الخادم :(backend) الاسم، الهاتف، البريد، كلمة المرور ومعرف الجهاز (**Device ID**).
   - إذا اختلف، يتم رفض الطلب أو يُطلب تحقق إضافي.
2. يُخزّن الـ Device ID مع الحساب في قاعدة البيانات.

* عند تسجيل الدخول لاحقاً، يتم التحقق أن معرف الجهاز المرسل يطابق الجهاز الأصلي

شكل رقم (4.4) عملية تحقق

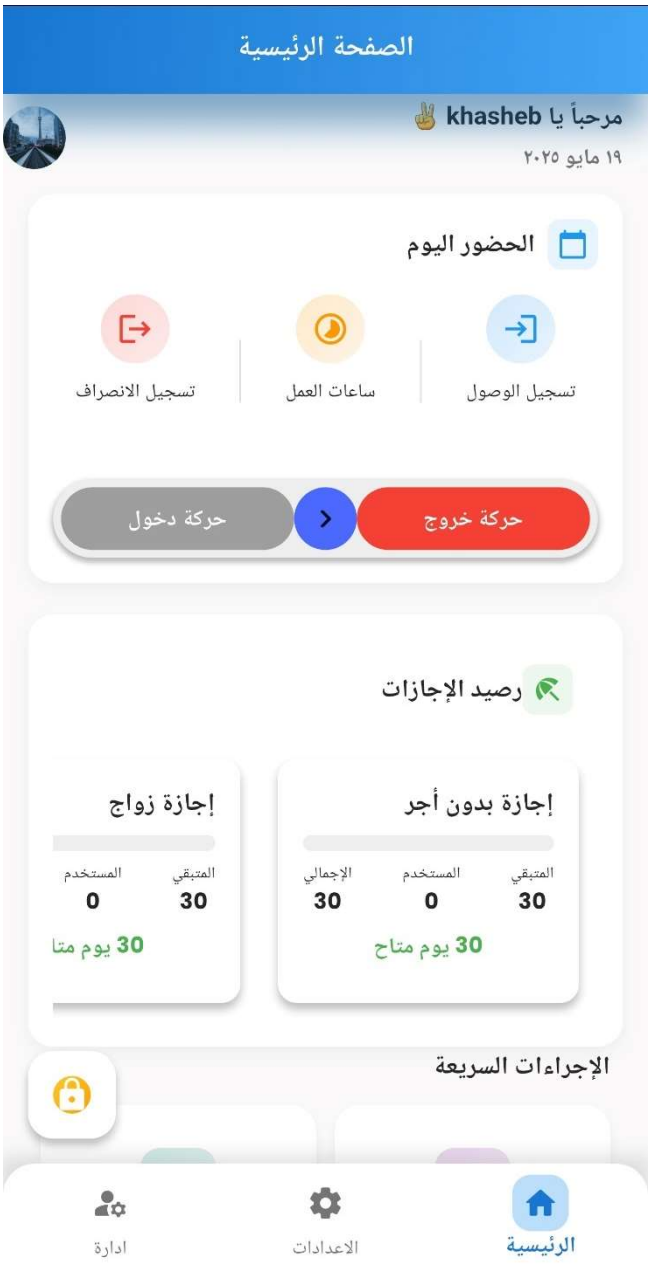
شكل رقم (4.5) إرسال رمز التحقق (**OTP**)

في الشكلين رقم (4.4 - 4.5) الآلية تتضمن عملية تحقق الهوية للمستخدم عند محاولة تسجيل الدخول من جهاز جديد. عند محاولة المستخدم تسجيل الدخول من جهاز غير معروف، يتم توجيهه لشاشة تأكيد الهوية حيث يتم طلب إدخال رمز التحقق المرسل إلى رقم هاتف المستخدم المسجل. بعد تأكيد الرقم، يتم إرسال رمز التحقق (OTP) عبر رسالة نصية إلى الهاتف المسجل. بعد ذلك، يتم طلب من المستخدم إدخال رمز التحقق في الخانات الفارغة المعروضة على الشاشة. بعد إدخال الرمز، يمكن للمستخدم التحقق من صحة الرمز عن طريق النقر على زر "تحقق من OTP". إذا كان الرمز المدخل يتطابق مع الرمز المرسل، يتم اعتبار الجهاز موثقاً ويتمكن المستخدم من الوصول إلى حسابه على الجهاز الجديد. إذا لم يتطابق الرمز، يتم عرض رسالة خطأ وقد يتم طلب من المستخدم إعادة إدخال الرمز أو طلب رمز جديد.

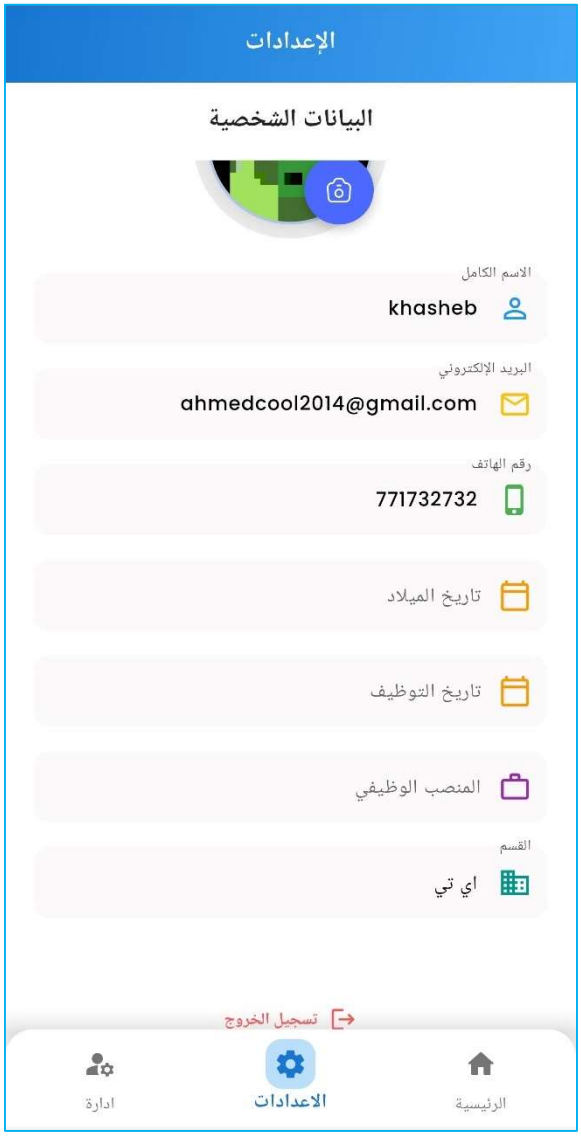
شكل رقم (4.6) تعليق الحساب

في الشكل رقم (4.6) الميزة تقدم للمستخدم إشعاراً بأن حسابه غير نشط حالياً. يمكن أن يكون سبب ذلك متعدداً، مثل تعليق الحساب، إلغاء تنشيطه من قبل المستخدم، أو الحاجة للتحقق. تعرض الشاشة رسالة واضحة تطلب من المستخدم التواصل مع الدعم للحصول على المساعدة، مما يوفر طريقاً واضحاً لحل المشكلة. زر "العودة إلى تسجيل الدخول" يتيح للمستخدم العودة إلى شاشة تسجيل الدخول، ربما لمحاولة تسجيل الدخول مرة أخرى أو استخدام حساب آخر. بشكل عام، تهدف هذه الميزة إلى توفير تواصل واضح للمستخدم حول حالة حسابه وتوجيهه نحو حل أي مشاكل قد تواجهه.

في شكل رقم (4.7) يبين واجهة تطبيق الجوال الذي تم عرضه ومصمماً لإدارة حضور الموظفين ورصيدهم من الإجازات وتسجيل الوصول والانصراف بسهولة، وعرض ساعات العمل ورصيدهم من الإجازات بشكل مفصل. كما يتضمن أيضاً قسماً للإجراءات السريعة، مما يسهل الوصول إلى الوظائف الإدارية والإعدادات بسرعة ويسر، بفضل واجهته البسيطة والواضحة، ويقدم حلاً شاملاً وفعال لإدارة الحضور والإجازات للموظفين، مع تركيز على السهولة في الاستخدام والوصول السريع إلى المعلومات الضرورية.



شكل رقم (4.7) إدارة حضور الموظفين



شكل رقم (4.8) واجهة "الإعدادات"

في شكل رقم (4.8) واجهة "الإعدادات" تعرض معلومات البيانات الشخصية للمستخدم، حيث يمكن للمستخدم تحديث وتعديل معلوماته الشخصية مثل الاسم، البريد الإلكتروني، رقم الهاتف، تاريخ الميلاد، تاريخ التوظيف، المنصب الوظيفي، والقسم التابع له. بالإضافة إلى ذلك، يمكن للمستخدم أن يقوم بتسجيل الخروج من التطبيق من خلال الخيار المخصص لذلك. توفر الواجهة أيضاً رمزاً لصورة الملف الشخصي مع رمز الكاميرا لإضافة أو تغيير الصورة، وتوفر شريط تنقل سفلي يسمح بالوصول السريع إلى أقسام أخرى من التطبيق مثل الإدارة والشاشة الرئيسية.

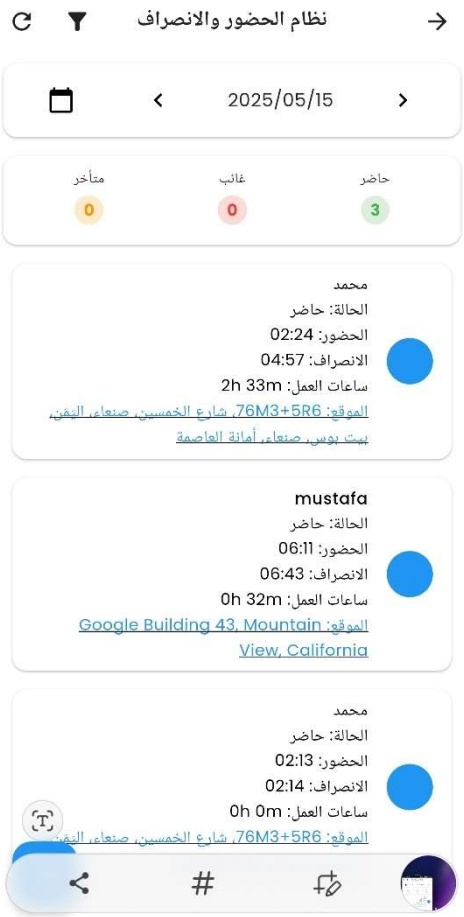
شكل رقم (4.9) "الصفحة الرئيسية"

في شكل رقم (4.9) الشاشة تحتوي على عنوان "الصفحة الرئيسية" وتعرض رمز قفل أحمر ونص "لست مصرح" تحته. أسفل ذلك، هناك زران أزرقي اللون: "اعادة تصريح" و"تخطي". في الجزء السفلي من الشاشة، هناك شريط تنقل يحتوي على رموز للإدارة، الإعدادات، والرئيسية، يبدو أن الزر "اعادة تصريح" هو الذي يطلب المصادقة الحيوية (biometric) والتي تستخدم بيانات الهوية الحيوية مثل بصمة الإصبع أو التعرف على الوجه للمصادقة. بمجرد النقر على هذا الزر، سيتم طلب من المستخدم استخدام بياناته الحيوية للتحقق من هويته وإعادة التصريح بالوصول إلى الصفحة الرئيسية للتطبيق.

شكل رقم (4.10) قسم إدارة الموظفين

في شكل رقم (4.10) الشاشة المعروضة تعرض قسم إدارة الموظفين في التطبيق. يمكن للمسؤول رؤية قائمة بالموظفين، مع إظهار الإدارة التي ينتمون إليها، والصلاحيات التي يحملونها، وربما عنوان البريد الإلكتروني الخاص بهم. يمكن للمشرف أيضاً البحث عن موظفين محددين، تصفية القائمة، وعرض إحصائيات ملخصة لعدد الإجمالي للموظفين، وعدد الموظفين النشطين، وعدد الغير نشطين. من المحتمل أن يسمح التبديل بتفعيل أو تعطيل حالة الموظفين، وأما الرمز الذي يبدو وكأنه قلم تحرير فمن المرجح أن يمكن للمسؤول

تعديل معلومات الموظفين. الرمز بصورة علامة الجمع الزرقاء في الأسفل على الأرجح يسمح للمسؤول بإضافة موظفين جدد إلى النظام ويوفر إمكانية تحويل صلاحية الموظف من مدير إلى موظف والعكس. يمكن للمسؤول استخدام رمز التحرير (القلم) الموجود بجوار كل موظف لتعديل صلاحياتهم. من خلال هذا الرمز، يمكن للمسؤول تغيير صلاحيات الموظف بسهولة بين كونه مديراً أو موظفاً حسب الحاجة والمتطلبات في المنظمة.



شكل رقم (4.11) واجهة نظام الحضور والانصراف

في شكل رقم (4.11) واجهة نظام الحضور والانصراف، حيث تحتوي الشاشة على شريط أدوات في الأعلى يحتوي على أيقونات للرجوع والتصفية، وعلامة تشير إلى الإجراء التالي. تحت الشريط هناك قسم لتحديد التاريخ، ويظهر التاريخ "15/05/2025" مع أزرار للتقديم والتأخير.

أسفل شريط التاريخ، يظهر ملخص لعدد الموظفين الحاضرين والمتأخرين والغائبين. بعد ذلك، يوجد قائمة بسجلات الحضور للموظفين مع تفاصيل محددة لكل واحد منهم بما في ذلك الحالة (حاضر)، ووقت الحضور والانصراف، وساعات العمل، والموقع. ورمز تعديل، ورمز ملف. يمكن للمدير رؤية موقع تسجيل حضور كل موظف عن طريق النقر على رابط الموقع الموجود بجانب كل سجل حضور، مما يتيح له متابعة تواجد الموظفين وتحقق من مواقع تسجيل حضورهم

4.5. الهدف الأمني:

- النظام يتطلب تفعيل خدمة الموقع (GPS) لتحديد الموقع الجغرافي الدقيق الذي تم فيه تسجيل الدخول.
- ذلك يضمن أن الموظف فعلاً متواجد في نقطة العمل أو الموقع المعتمد وليس في مكان خارجي.
- النظام لم يسمح بتسجيل الدخول (أو الخروج) لأن خدمة تحديد الموقع غير مفعلة.
- يتطلب من الموظف تفعيل خدمة الموقع الجغرافي على الجهاز، ثم إعادة المحاولة.

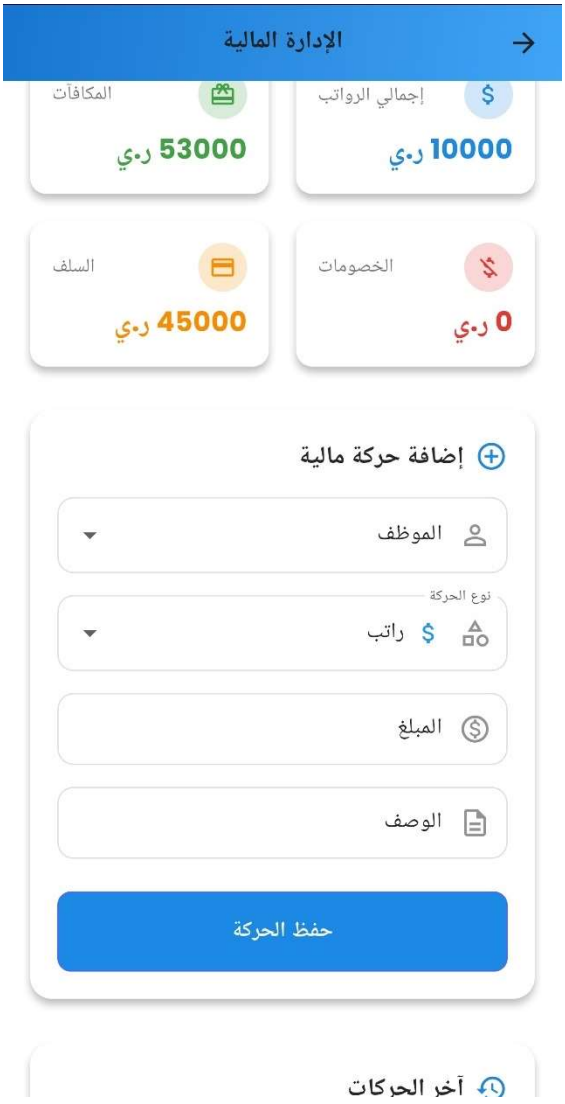
4.6. التوصيات التنظيمية:

- يجب على جميع الموظفين تفعيل خدمة GPS قبل تسجيل الحضور أو المغادرة.
- يمكن للنظام إرسال تنبيه تلقائي لتفعيل الموقع إذا تم الكشف عن أنه غير نشط.
- يُفضّل عرض رسالة توضيحية تقول مثلاً:

⚠ "يرجى تفعيل الموقع الجغرافي لإتمام عملية تسجيل الدخول أو الخروج بنجاح."

4.7. الهدف من تفعيل الموقع الجغرافي:

يُعد تفعيل خاصية الموقع الجغرافي إجراءً تنظيمياً يهدف إلى تعزيز موثوقية نظام الحضور والانصراف وضمان الالتزام بالضوابط المعتمدة. إذ يتيح تحديد موقع تسجيل الدخول التحقق من وجود الموظف ضمن نطاق المنشأة الرسمية، بينما يسهم رصد موقع تسجيل المغادرة في مراقبة مدى تقيده بالحدود الجغرافية المقررة لساعات العمل. كما يحد هذا النظام من إمكانية تسجيل الحضور من مواقع غير مصرح بها، مما يقلل فرص التلاعب أو التحايل. إضافة إلى ذلك، يوفّر للإدارة أدوات تحليل دقيقة تسهم في إعداد تقارير موثوقة تدعم قرارات الموارد البشرية وتُعزز مستوى الانضباط المؤسسي.

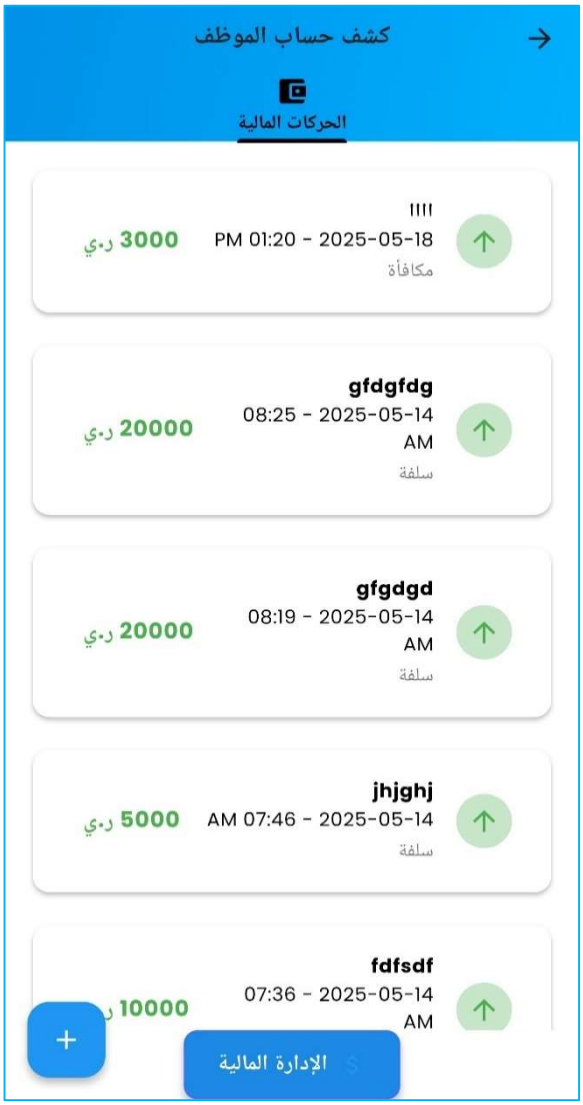


شكل رقم (4.12) شاشة "إدارة المالية"

في شكل رقم (4.12) تُظهر شاشة "إدارة المالية" في تطبيق، حيث يمكن من خلالها إدارة الجوانب المالية للموظفين. في الجزء العلوي، توجد أربع بطاقات تعرض ملخصاً مالياً للرواتب الإجمالية، والمكافآت والسلف والخصومات.

أسفل هذه البطاقات، هناك قسم بعنوان "إضافة حركة مالية"، يتضمن حقولاً لإدخال تفاصيل العملية المالية الجديدة للموظفين، مثل اختيار الموظف، ونوع الحركة المالية مع رمز الدولار، وإدخال المبلغ، وإضافة وصف. هناك زر أزرق يحمل عبارة "حفظ الحركة" يتيح للمستخدم حفظ العملية المالية التي تم إضافتها. في

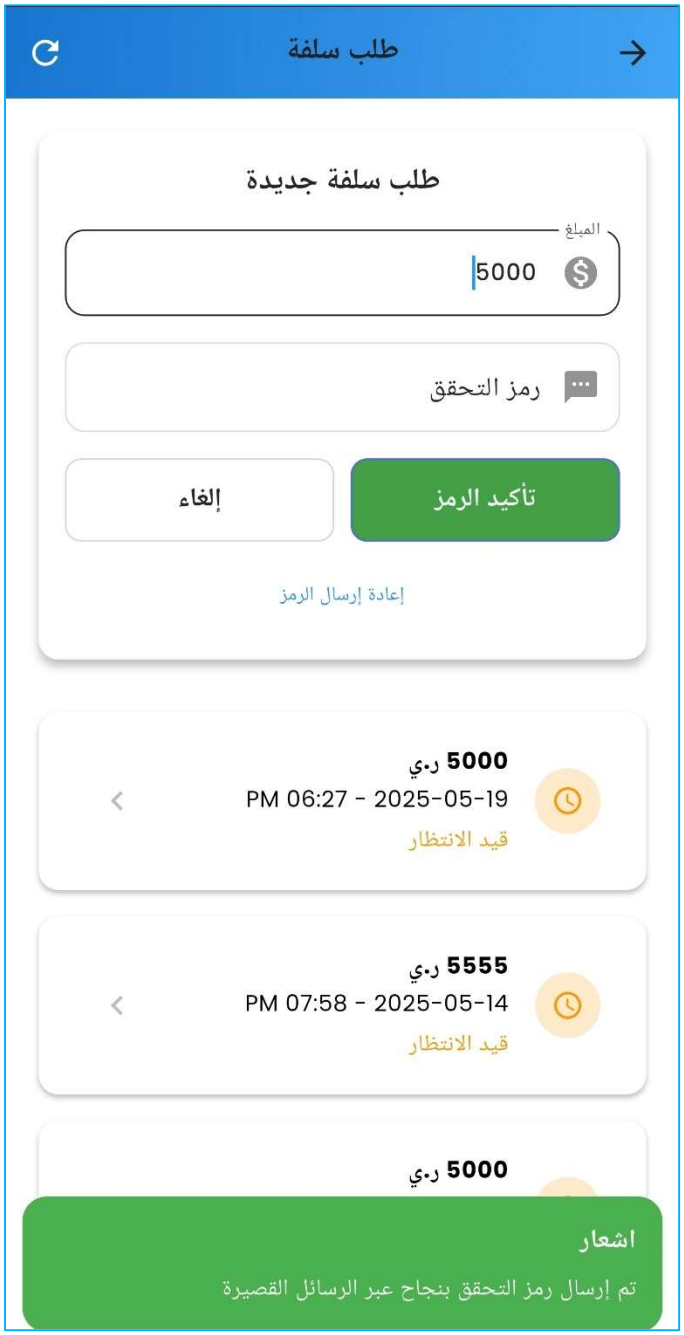
الجزء السفلي، يوجد رابط "آخر الحركات" الذي يبدو أنه يوفر وصولاً سريعاً إلى قائمة بآخر العمليات المالية التي تم تسجيلها مسبقاً.



شكل رقم (4.13) شاشة "كشف حساب الموظف"

في شكل رقم (4.13) تُظهر شاشة "كشف حساب الموظف" في التطبيق، حيث تعرض قائمة بالعمليات المالية التي تمت على حساب الموظف. كل عملية مالية تتضمن المبلغ بالريال اليمني (ر.ي)، التاريخ والوقت، واسم العملية مثل مكافأة أو سلفة. كما يظهر سهم يشير إلى الأعلى لكل عملية. في الجزء السفلي من الشاشة، يوجد زر "+" الذي يتيح للمستخدم طلب حركة مالية جديدة، بالإضافة إلى زر "الإدارة المالية" الذي قد يقود إلى أدوات إدارية مالية أخرى داخل التطبيق حيث لا يظهر الإدارة المالية للمستخدم بصلاحية غير الادمن.

في شكل رقم (4.14) تُظهر واجهة "طلب سلفة" في تطبيق الهاتف المحمول. يوجد في الأعلى عنوان "طلب سلفة" وفي القسم الرئيسي يوجد قسم "طلب سلفة جديدة" حيث تم إدخال المبلغ، ويبدو أن هذا المبلغ يشير إلى قيمة السلفة المطلوبة. أسفل هذا القسم، يظهر حقل "رمز التحقق" مع رمز فقاعة الحديث. يظهر زرين: "إلغاء" و"تأكيد الرمز" باللون الأخضر. في الجزء السفلي بالأسفل، شريط إشعار أخضر يعرض الرسالة "تم إرسال رمز التحقق بنجاح عبر الرسائل القصيرة". كما يوجد رابط نصي يقرأ "إعادة إرسال الرمز".أسفل قسم طلب السلفة.



شكل رقم (4.14) واجهة "طلب سلفة" الموظف"

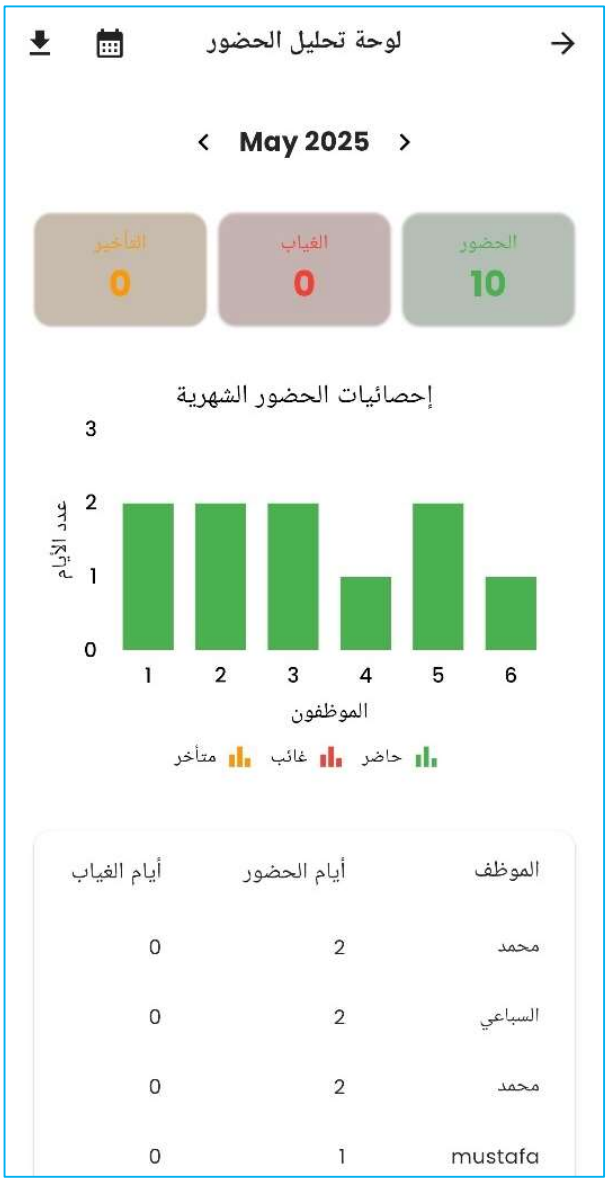
في الشكل رقم (4.15) واجهة تطبيق بعنوان "الموافقة على طلبات السلف"، تعرض قائمة بطلبات السلف المقدمة. كل طلب يتضمن المبلغ المطلوب بالريال، اسم الموظف مقدم الطلب، وحالة الطلب (قيد الانتظار، تم الموافقة، تم الرفض). يوجد أيقونتا الموافقة والرفض ممثلة بعلامة صح خضراء وعلامة X حمراء على التوالي.

توفر للمسؤول أو المدير إمكانية مراجعة طلبات السلف من الموظفين واتخاذ قرار بالموافقة عليها أو رفضها. يمكن للمسؤول استخدام الأيقونات المخصصة للموافقة أو الرفض لكل طلب بناءً على التقييم والسياسات المالية للشركة

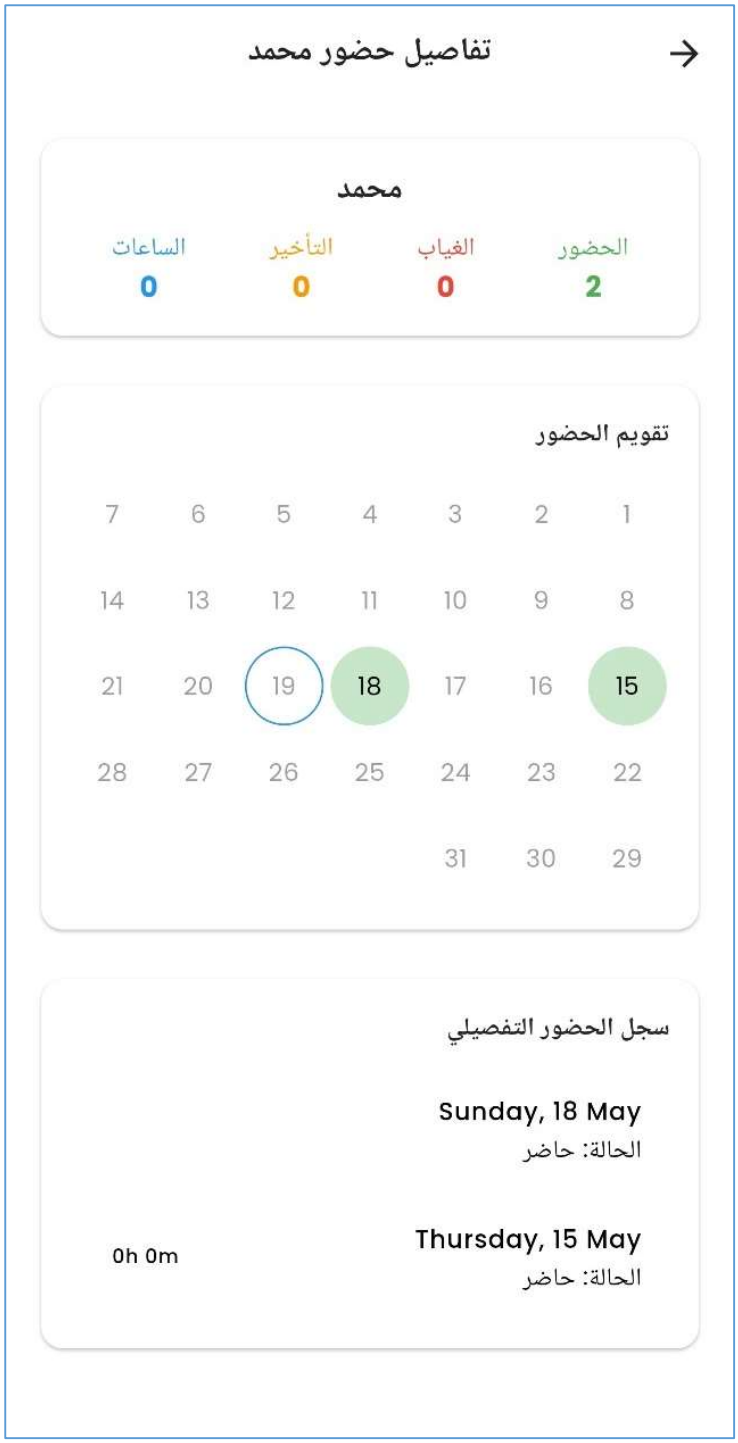
شكل رقم (4.15) "الموافقة على طلبات

يوضح الشكل رقم (4.16) لوحة تحليل الحضور لشهر مايو 2025م في الجزء العلوي من اللوحة، يتم عرض ملخص لحالة الحضور للموظفين، حيث لا يوجد موظفين متأخرين ولا غائبين ويوجد 10 موظفين حاضرين. يظهر في الجزء العلوي أيضاً رسم بياني يوضح إحصائيات الحضور الشهرية، حيث يعرض توزيع أيام الشهر على المحور الأفقي وعدد الأيام على المحور الرأسي.

تحت الرسم البياني، يظهر جدول يعرض عدد أيام الحضور والغياب لكل موظف. يتضمن الجدول أسماء الموظفين وعدد الأيام التي حضروا فيها وعدد الأيام التي كانوا غائبين.



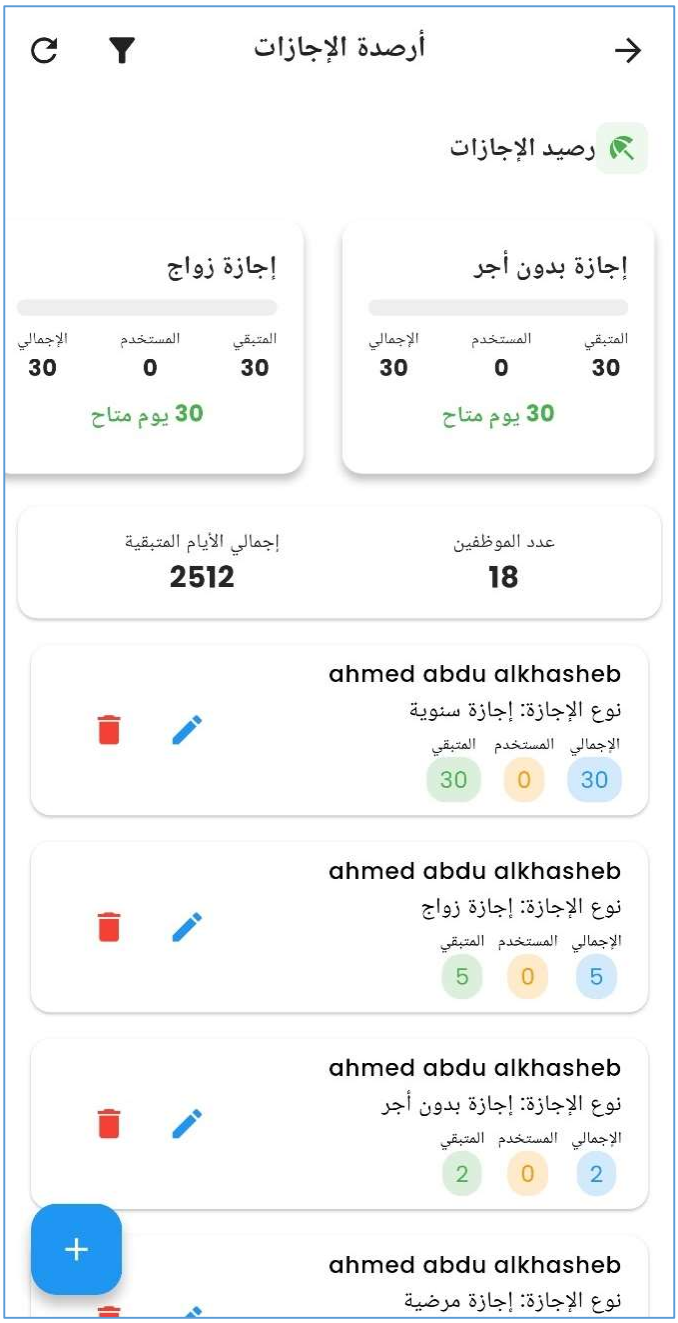
شكل رقم (4.16) لوحة تحليل الحضور



شكل رقم (4.17) واجهة "تفاصيل الحضور "

الشكل رقم (17) تعرض واجهة "تفاصيل الحضور ". في الجزء العلوي من الواجهة، يظهر ملخص لحضور الموظف محمد، حيث يُظهر أنه قد حضر لمدة 2 ساعة، ولم يتأخر ولم يتغيب. يلي ذلك "تقويم الحضور" الذي يعرض أيام الشهر من 1 إلى 31، حيث تم تحديد أيام 15 و 18 باللون الأخضر، وتم تحديد يوم 19 بدائرة.

تحت "تقويم الحضور"، يظهر "سجل الحضور التفصيلي" حيث يُعرض حالة حضور محمد يوم الأحد، 18 مايو كـ "حاضر"، ويوم الخميس، 15 مايو كـ "حاضر



شكل رقم (4.18) "أرصدة الإجازات".

في الشكل رقم (18) تُظهر واجهة تطبيق الهاتف المحمول بعنوان "أرصدة الإجازات". في الجزء العلوي، هناك بطاقتان تعرض ملخصات لـ "إجازة بدون أجر" و "إجازة زواج"، حيث تُظهر كل منها الإجمالي، المستخدم، والأيام المتبقية. أسفل هذه البطاقات، يوجد بطاقة تُظهر "إجمالي الأيام المتبقية" كـ "2512" و "عدد الموظفين" كـ "18".

باقي الشاشة تعرض أرصدة الإجازات الفردية لـ "أحمد عبدو الخاشب" لأنواع الإجازات المختلفة: "إجازة سنوية"، "إجازة زواج"، "إجازة بدون أجر"، و "إجازة مرضية". كل نوع من أنواع الإجازات يعرض الإجمالي، المستخدم، والأيام المتبقية. يوجد رموز للحذف والتعديل بجانب كل إدخال للإجازة. ويوجد رمز زائد في الزاوية السفلية اليسرى.

الفصل الخامس

التنفيذ والاختبار

5.1. المقدمة

في هذا الفصل، سنستعرض عملية تنفيذ النظام واختباره، مع التركيز على الجوانب الأمنية والتقنية التي تم تطبيقها لضمان موثوقية النظام وفعاليته. كما سنقدم نتائج الاختبارات والتوصيات المستقبلية لتحسين النظام.

5.2. التنفيذ

تم القيام بإنشاء النظام لاتمتة عمليات الموظف مثل (طلب، اجازات، سلف، البصمة،،،إلخ) وتم تنفيذيها على النحو التالي:

5.2.1. مراحل التنفيذ

1. التحليل والتصميم:
   - تحليل المتطلبات وتصميم واجهات المستخدم باستخدام Figma.
   - تصميم قاعدة البيانات وإنشاء العلاقات بين الجداول.
2. البرمجة:
   - تطوير الواجهات الأمامية باستخدام Flutter.
   - تنفيذ الوظائف الخلفية مثل المصادقة وإدارة الصلاحيات.
   - ربط النظام مع قاعدة البيانات باستخدام Supabase.
3. التكامل:
   - دمج الواجهات الأمامية مع الخلفية.
   - اختبار التكامل بين المكونات المختلفة.

5.2.2. إنشاء حساب جديد:

تم انشاء واجهة في التطبيق تقوم من خلالها بإنشاء مستخدم جديد حيث يتم من خلالها حفظ بيانات الموظفين على النحو الاتي:

ويلاحظ من خلال الشكل رقم (5.19) عند ادخال البيانات التالية:

1- اسم المستخدم

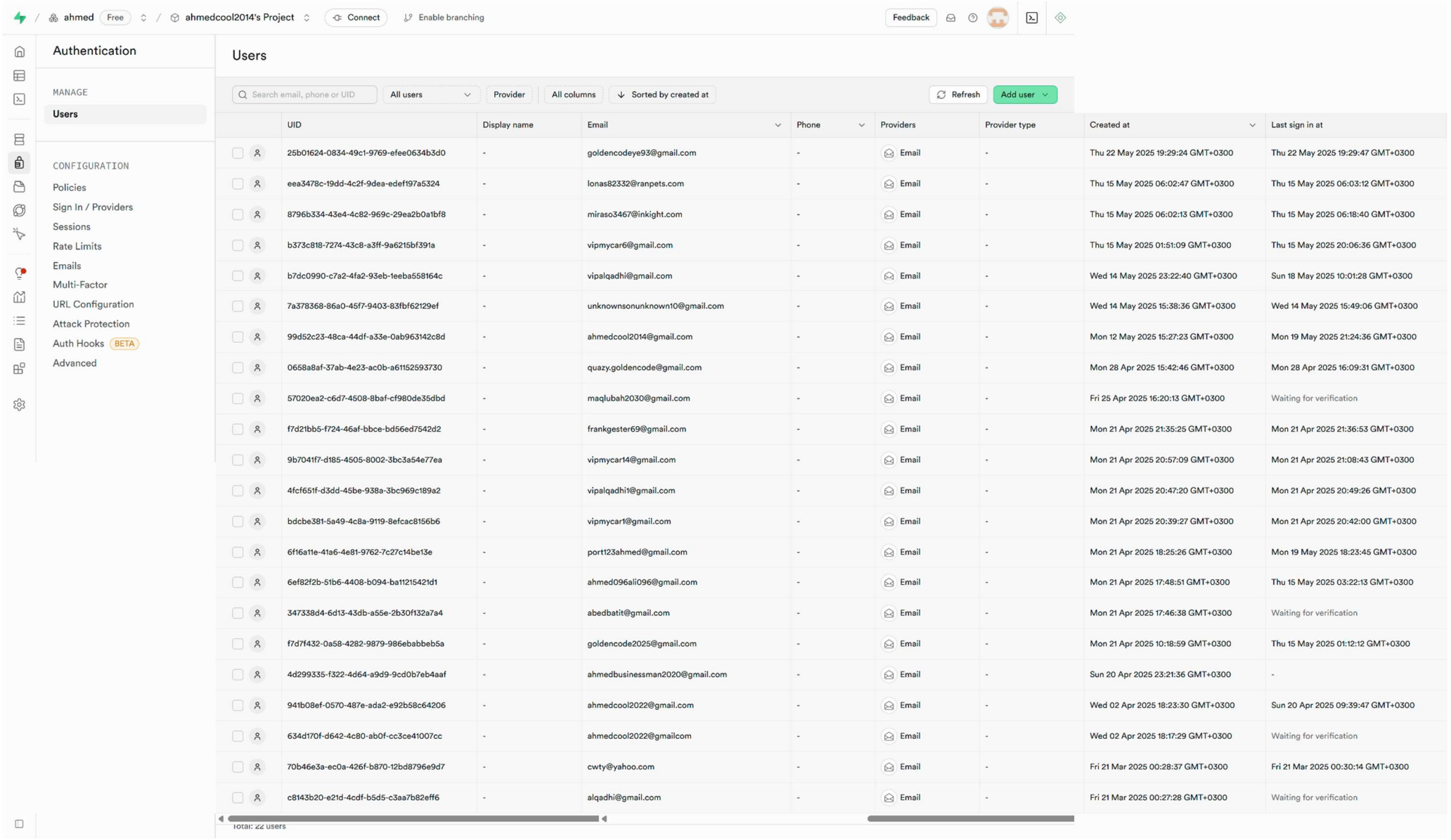
2- كلمة المرور

3- رقم الجوال

4- البريد الالكتروني

وعند الضغط على زر انشاء حساب يتم حفظ البيانات المدخلة في قاعدة البيانات في جدول المستخدمين (Users) كما في الشكل رقم (5.20) الذي يبين جدول المستخدمين في قاعدة البيانات

شكل رقم (5.1) إنشاء حساب جديد

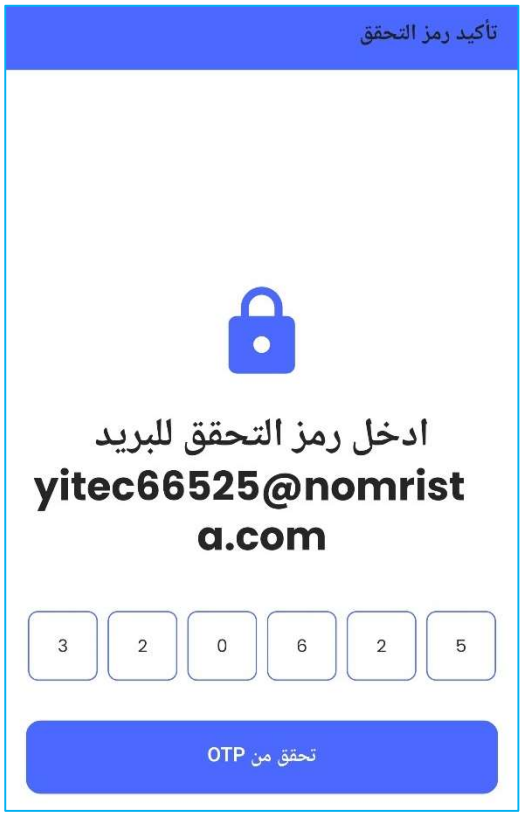


شكل رقم (5.1) جدول المستخدمين في قاعدة البيانات

5.2.3. عملية تأكيد بيانات المستخدم الجديد:

بعد ان تم حفظ بيانات المستخدم الجديد في قاعدة البيانات نقوم بإنشاء رمز تأكيد مكون من 6ارقام يتم حفظة في جدول قاعدة البيانات كما في الشكل رقم (5.2)،ويتم ارسال رمز التأكيد الى البريد الإلكتروني كما في الشكل (5.3)

ويتم ارسال هذا الرمز الى رقم البريد الالكتروني حسب الصورة في الشكل رقم (22) :



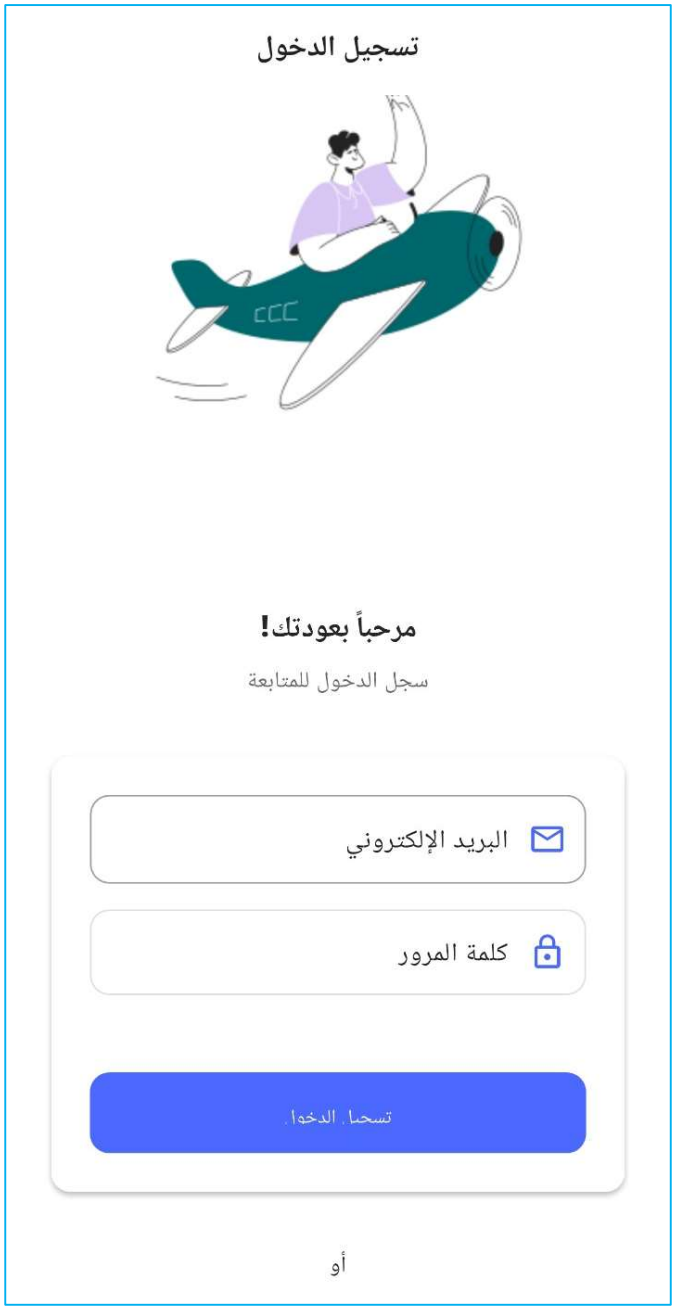
ويتم ارسال الرقم الى البريد الالكتروني حسب الصورة في الشكل رقم (5.3) :

5.2.4. عملية تسجيل الدخول مع التحقق من الجهاز

عندما نقوم بفتح واجهة تسجيل الدخول كما في الشكل رقم (5.3) يتم الاتي:

1. إدخال بيانات تسجيل الدخول:

- وفي هذه الخطوة يقوم المستخدم بإدخال البريد الإلكتروني وكلمة المرور (كما هو موضح في الشكل رقم (5.4)، ثم الضغط على زر تسجيل الدخول، اذا كانت البيانات خاطئة يتم اظهار رسالة للمستخدم بأن البيانات خاطئة، واذا كانت البيانات صحيحة يتم الانتقال للخطوة التالية.



شكل رقم (5.4) إدخال بيانات تسجيل الدخول

التحقق الأساسي:

شكل رقم (5.5) التحقق الأ

- في الشكل رقم (5.5) في هذه العملية قمنا بعمل تأكيد وحماية بحيث لا يستطيع أي موظف ان ينقل حسابة الخاص من جهاز الى اخر الا بعد ارسال كود التحقق OTP الى رقم الهاتف ليتم تسجيل ID هذا الجهاز في قاعدة البيانات وهذا لا يسمح بالدخول المتعدد لحسابات الموظفين ويتم التحقق الأساسي من خلال التالي:

A- الحصـــول على معرف الجهـاز (Device ID):

- يتم توليد معرف فريد للجهاز عند أول تسجيل دخول (أو يمكن استخدام معرّفات مثل: Device ID للهواتف، أو أي معرّف فريد آخر)يتم تخزين هذا المعرف في قاعدة البيانات مرتبطاً بحساب المستخدم

B- التحقق من الجهاز:

- عند محاولة تسجيل الدخول، يرسل التطبيق/الموقع Device ID الحالي مع بيانات الاعتماد
- الخادم يتحقق مما إذا كان هذا Device ID مسجلاً مسبقاً لهذا ال مستخدم

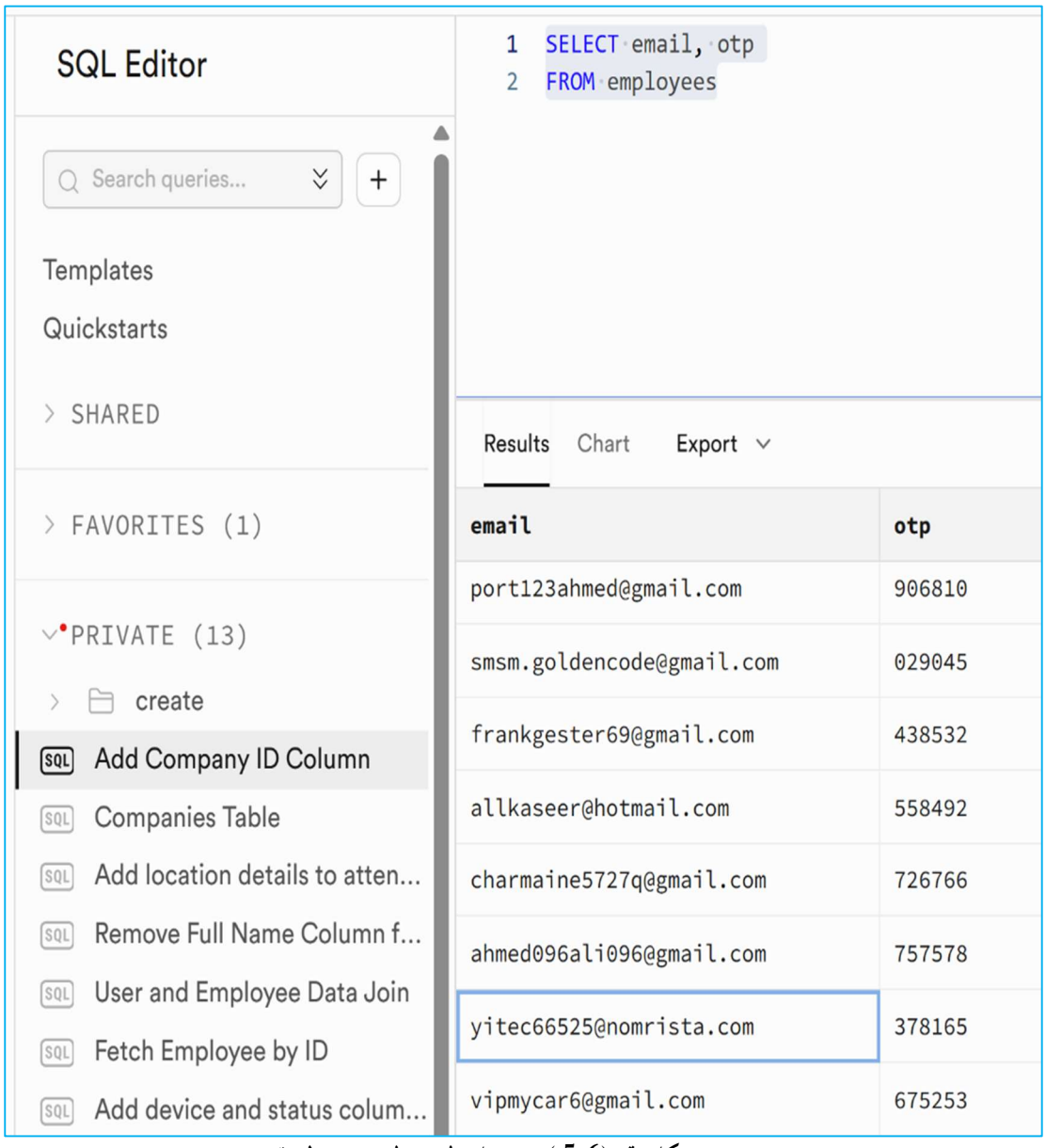
C- سيناريوهات التحقق:

- إذا كان الجهاز معروفاً: يتم منح الوصول مباشرة (أو قد يطلب التحقق الثنائي إذا كان مفعلاً)
- إذا كان الجهاز جديداً يتم:

✓ **طلب التحقق الإضافي كود عبر (SMS).**

✓ **إرسال رساله لرقم المستخدم المخزن في قاعدة البيانات**

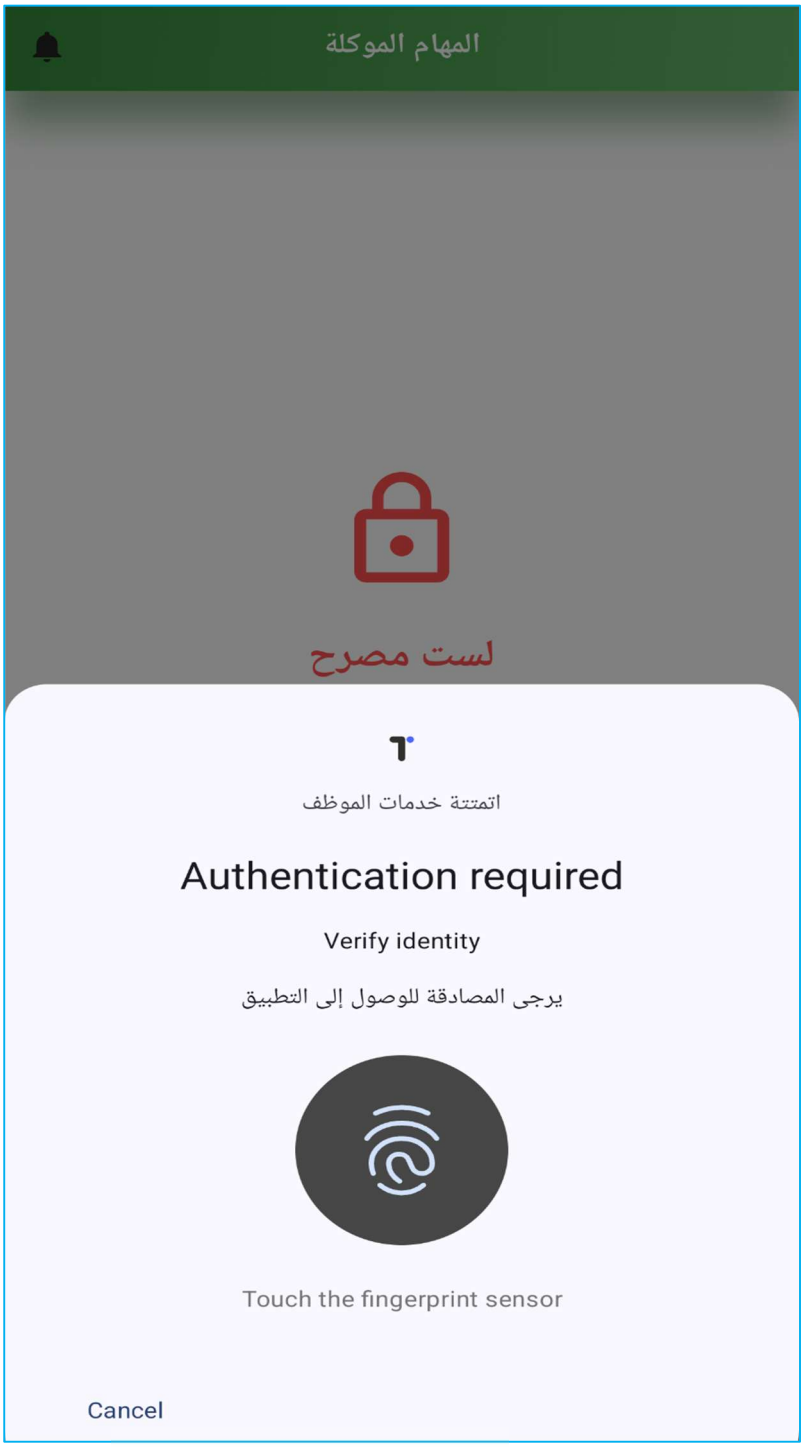
✓ **تسجيل الجهاز الجديد بعد التحقق منه كما في الشكل رقم (5.6)**



شكل رقم (5.6) تسجيل الجهاز الجديد بعد التحقق

5.2.5. عملية الدخول بالصمة الى الواجهة الرئيسية

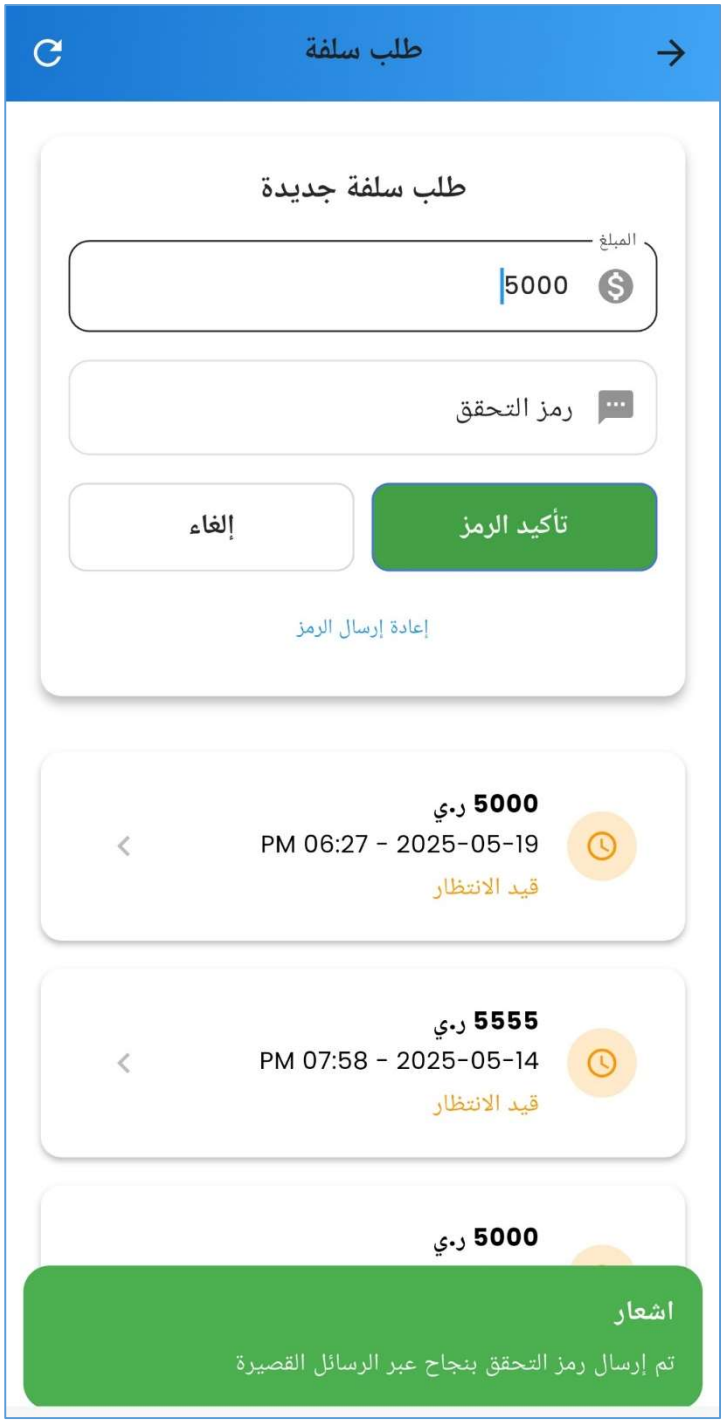
قمنا بإضافة طبقة حماية إضافية للتطبيق بحيث عند الخروج من التطبيق او اغلاقه والرجوع إليه او فتحة مرة أخرى لا يتم عرض شاشة تسجيل الدخول او عرض الواجهة الرئيسية، ولكن يتم اظهار التحقق من البصمة كما في الشكل رقم (5.7) ولا يتم الانتقال الى الواجهة الرئيسية للتطبيق او إمكانية تنفيذ أي عملية إلا إذا كانت البصمة صحيحة.



شكل رقم (5.7) التحقق من البصمة

5.2.6. عمليات النظام

يوجد في النظام الكثير من العمليات منها طلب سلفة طلب إجازة التحضير،،، إلخ، ولا يتم تنفيذ أي عملية او اعتمادها إلا بعد اجتياز جميع طبقات الحماية الخاصة بهذه العمليات وقد تم تحديد طبقات الحماية حسب أهمية العملية في النظام، وسوف نوضح كمثال عملية طلب سلفة كونها تحتوي على معظم طبقات الحماية:



شكل رقم (5.8) عملية طلب سلفة

❖ عملية طلب سلفة:

يُظهر الواجهة المرفقة في الشكل رقم (5.28) نظاماً إلكترونياً لطلب السلفة المالية مع آلية تحقق آمنة تعتمد على كلمة المرور لمرة واحدة (OTP). تم تصميم العملية وفق معايير الأمن المصرفي (مثل PCI DSS) لضمان سلامة المعاملات.

A. خطوات العملية التفصيلية

المرحلة الاولى: بدء طلب السلفة

- **إدخال المبلغ:**
  - يحدد المستخدم مبلغ السلفة (مثال: 5000 ر.ي) كما يظهر في حقل "طب سلفة جديدة".
  - قد يكون النظام يفرض حداً أدنى/أقصى (غير موضح في الصورة).

المرحلة الثانية: توليد وإرسالOTP

- **إرسال الرمز:**
  - يُولّد النظام رمز OTP عشوائي (عادة 4-6 أرقام) ويرسله عبر الرسائل القصيرة (SMS) إلى رقم الهاتف المسجل.
  - تظهر رسالة تأكيد ": تم إرسال رمز التحقق بنجاح عبر الرسائل القصيرة."

- **ضوابط الأمان:**
  - صلاحية الرمز: 3-5 دقائق (افتراضياً).
  - عدد محاولات إدخال خاطئة: 3 محاولات قبل إلغاء الطلب.

المرحلة الثالثة: إدخال وتأكيدOTP

- **واجهة التحقق:**
  - يُطلب من المستخدم إدخال الرمز في حقل "رمز التحقق".
  - خيارات متاحة:
    - "تأكيد الرمز": للمتابعة.

- "إلغاء" :لإنهاء العملية.
- "إعادة إرسال الرمز" :في حالة عدم الوصول إليه.

المرحلة الرابعة: معالجة الطلب

- **إذا نجح التحقق:**
  - يُضاف طلب السلفة إلى قائمة "قيد الانتظار" (كما يظهر للطلبات السابقة: 5000 ر.ي و5555 ر.ي).
  - يُرسل إشعار إلى المدير بتغيير حالة الطلب (قبول/رفض لاحقاً).
- **إذا فشل التحقق:**
  - يُعاد توجيه المستخدم إلى خطوة إعادة الإرسال أو إلغاء الطلب.

B. آلية عمل الواجهة (من وجهة نظر المدير)

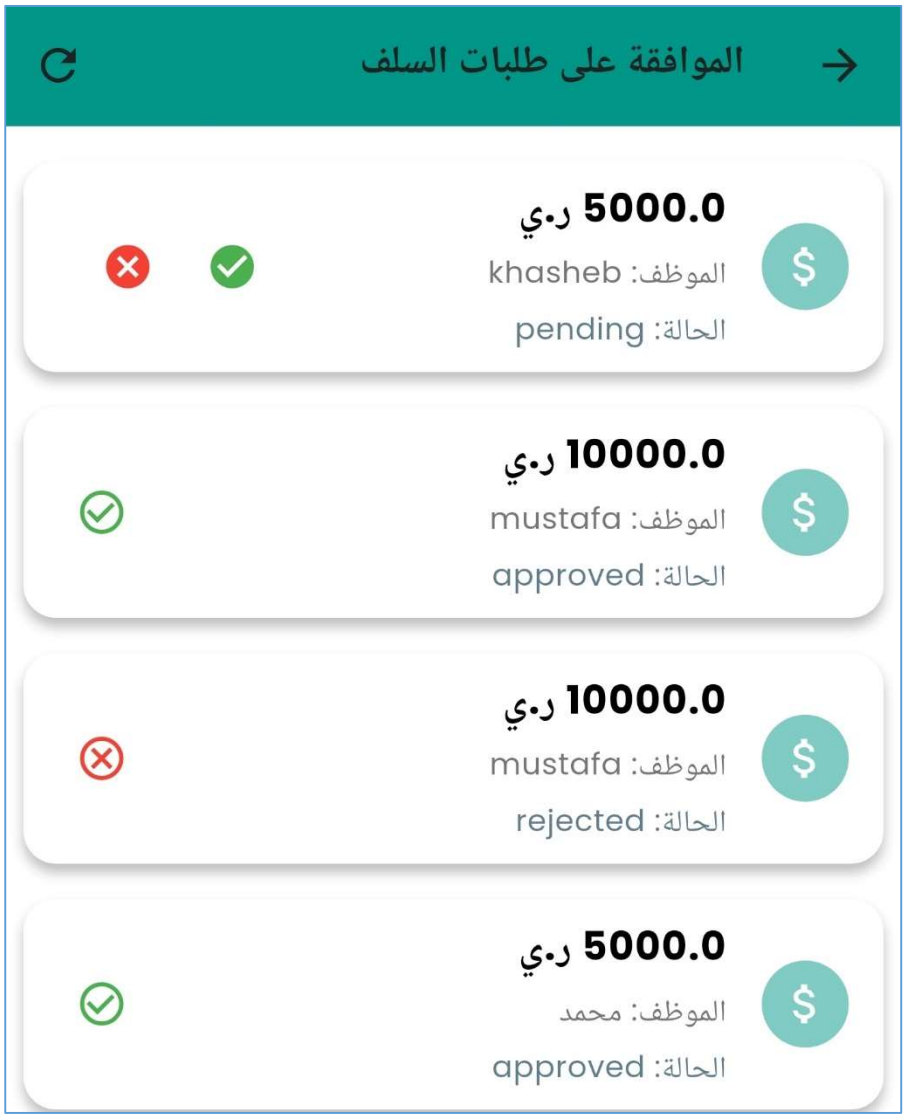
واجهة إدارة العمليات (المدير) حيث يتم في هذه العملية قبول او رفض الطلبات بناء على الصلاحيات الممنوحة للمخولين

المرحلة الأولى: استعراض الطلبات

- يقوم النظام بعرض جميع الطلبات المرسلة من الموظفين في صفحة واحدة.
- يمكن للمدير فرز الطلبات حسب:
  - الحالة (مثل: عرض كل الطلبات "pending" أولاً).
  - المبلغ (من الأصغر إلى الأكبر أو العكس).
  - اسم الموظف (ترتيب أبجدي).

المرحلة الثانية: اتخاذ القرار

- للطلبات الجديدة (pending):
  - يمتلك المدير خيارين رئيسيين (غير ظاهرين في الصورة ولكن مُستنتجين):
    1. **الموافقة** (Approve) : تغيير الحالة إلى "approved".
    2. **الرفض** (**Reject**) : تغيير الحالة إلى "rejected".
  - قد يُطلب من المدير إدخال سبب الرفض أو شروط الموافقة)مثال: خصم المبلغ على أقساط(.



شكل رقم (5.9) شاشة الطلبات

- للطلبات المُقرة أو المرفوضة:
    - تظهر للمدير كسجل مرجعي (مثال: طلب mustafa بقيمة 10,000$ مُوافق عليه، وطلب آخر له مرفوض).

المرحلة الثالثة: إشعار الموظفين

- عند تغيير حالة الطلب،
    - يتم تغيير حالة الطلب في شاشة الموظف..

5.3. الاختبارات

تم إجراء مجموعة من الاختبارات لضمان جودة النظام وأمانه، بما يتوافق مع المعايير الدولية مثل ISO/IEC 27001 لأمن المعلومات.

5.3.1. أنواع الاختبارات

1. اختبارات الوحدة:(Unit Testing)

- اختبار كل وحدة برمجية على حدة (مثل وظائف تسجيل الدخول، إدارة الصلاحيات).
- تم استخدام أداة Flutter Test لتنفيذ هذه الاختبارات.

2. اختبارات التكامل:(Integration Testing)

- اختبار تفاعل الوحدات مع بعضها البعض (مثل تفاعل واجهة المستخدم مع قاعدة البيانات).
- التأكد من أن البيانات تنتقل بشكل آمن بين المكونات.

3. **اختبارات الأمان:(Security Testing)**

- اختبار مقاومة الهجمات مثل SQL Injection وXSS.
- استخدام أدوات مثل OWASP ZAP لفحص الثغرات الأمنية.

4. **اختبارات الأداء:(Performance Testing)**

- قياس وقت استجابة النظام تحت أحمال مختلفة.
- استخدام أدوات مثل JMeter لمحاكاة عدد كبير من المستخدمين.

5. **اختبارات القبول:(User Acceptance Testing - UAT)**

- اختبار النظام من قبل المستخدمين النهائيين للتأكد من أنه يلبي احتياجاتهم.

5.3.2. الحلول المطبقة

1. **المصادقة البيومترية:**

- استخدام مكتبة local_auth في Flutter لدعم البصمة والوجه.

2. **نظام الصلاحيات:**

- تطبيق سياسة "أقل صلاحية" (Least Privilege) مع تحديث دوري للصلاحيات.

3. **أمان البيانات:**

- استخدام بروتوكول HTTPS وتشفير AES للبيانات الحساسة.

5.3.3. نتائج الاختبارات

- اختبارات الوحدة: نجاح جميع الوحدات بنسبة 100%.
- اختبارات التكامل: اكتشاف بعض الأخطاء في نقل البيانات، والتي تم تصحيحها.

- اختبارات الأمان: النظام مقاوم للهجمات الشائعة، مع بعض التوصيات لتحسين التشفير.
- اختبارات الأداء: وقت استجابة أقل من ثانيتين تحت حمل 1000 مستخدم متزامن.
- اختبارات القبول: رضا المستخدمين بنسبة 95%.

الفصل السادس

الخاتمة والأعمال المستقبلية

6.1. الاستنتاجات

من خلا تنفيذ المشروع واختباره لوحظ التالي:

1- تم تصميم وتنفيذ نظام أمني متكامل لأتمتة إدارة الموظفين، مع التركيز على تأمين البيانات وحماية الخصوصية.

2- تحسين أمان البيانات حيث نجح النظام في تطبيق آليات تشفير متقدمة مثل AES-256 لحماية البيانات الحساسة، مما يقلل من مخاطر الاختراق أو التسريب.

3- تم تنفيذ نظام صلاحيات (RBAC) يحدد وصول المستخدمين بدقة، مما يضمن أن كل موظف يصل فقط إلى البيانات المصرح له بها.

4- تعزيز المصادقة والتحقق حيث تم دمج تقنيات المصادقة متعددة العوامل (MFA)، بما في ذلك البصمة وOTP، مما يزيد من صعوبة الوصول غير المصرح به.

5- ربط النظام كل مستخدم بتوقيع إلكتروني فريد، مما يعزز المساءلة ويقلل من فرص التلاعب.

6- مراقبة العمليات وسجلات النشاط حيث تم إنشاء سجلات تفصيلية (Logs) لتسجيل جميع العمليات داخل النظام، مما يوفر شفافية كاملة ويسهل اكتشاف أي أنشطة مشبوهة.

7- تم تطوير لوحة تحكم للمشرفين تتيح مراقبة النشاطات وإدارة التنبيهات الأمنية.

8- التكامل مع التقنيات الحديثة حيث نجح النظام في دعم تقنيات مثل GPS لتحديد الموقع الجغرافي للموظفين، مما يعزز دقة تسجيل الحضور والانصراف.

9- تم استخدام أدوات مثل Firebase وSupabase لضمان تخزين آمن وسريع للبيانات.

باختصار، نجح المشروع في تقديم حل متكامل يوازن بين الأمان وسهولة الاستخدام، مع توفير بيئة آمنة وفعالة لإدارة الموظفين في المؤسسات. هذه النتائج تعكس الجهود الكبيرة التي بذلها الفريق لتحقيق أهداف المشروع وتجاوز التحديات التقنية والأمنية.

6.2. التحديات:

واجه فريق العمل خلال تنفيذ المشروع مجموعة من التحديات الفنية والتنظيمية، بالإضافة إلى بعض جوانب القصور التي تستدعي التطوير في المراحل المستقبلية، والتي يمكن تصنيفها على النحو التالي:

6.2.1. التحديات الفنية

تحديات التكامل مع الأنظمة القائمة:

واجه الفريق صعوبات في تحقيق التكامل السلس مع بعض الأنظمة القديمة المستخدمة في المؤسسات، مما استدعى تطوير واجهات برمجة تطبيقات (APIs) مخصصة.

ظهرت تحديات في توافق النظام مع بعض أنظمة التشغيل القديمة، مما حد من انتشاره في بعض البيئات التقليدية.

تحديات الأداء:

واجه النظام بعض التأخيرات في معالجة البيانات عند التعامل مع أحجام كبيرة من المستخدمين بشكل متزامن.

ظهرت حاجة ملحة لتحسين خوارزميات البحث والاسترجاع في قواعد البيانات لضمان سرعة الاستجابة.

تحديات الأمان:

واجه الفريق صعوبات في تحقيق التوازن بين متطلبات الأمان الصارمة وسهولة الاستخدام من قبل الموظفين غير التقنيين.

ظهرت تحديات في تطبيق آليات المصادقة المتقدمة (مثل البصمة والوجه) على بعض الأجهزة القديمة.

6.2.2. تحديات الموارد

القيود المالية:

حدت الميزانية المخصصة من إمكانية دمج بعض التقنيات المتقدمة مثل أنظمة الذكاء الاصطناعي للكشف عن التهديدات.

أثرت على جودة بعض المكونات الأجهزة المستخدمة في اختبارات النظام.

نقص الخبرات المتخصصة:

واجه الفريق نقصاً في الخبرات المتخصصة في بعض المجالات التقنية المتقدمة مثل أمن السحابة الإلكترونية.

استدعى الأمر الاستعانة بخبراء خارجيين في بعض المراحل، مما أثر على الجدول الزمني للمشروع.

6.3. جوانب القصور

6.3.1. في مجال تجربة المستخدم:

لوحظ أن بعض واجهات النظام تحتاج إلى مزيد من التبسيط لتتناسب مع فئات الموظفين غير التقنيين.

ظهرت حاجة لتطوير أدلة استخدام أكثر تفصيلاً ووضوحاً.

في مجال التوثيق:

لم يتم توثيق بعض الإجراءات الأمنية بالتفصيل الكافي في الوثائق الفنية.

تحتاج خطة الاستجابة للحوادث إلى مزيد من التفصيل والتحديث.

6.3.2. في مجال الاختبارات:

لم تغطِ اختبارات الاختراق جميع السيناريوهات المحتملة للهجمات الأمنية.

اقتصرت اختبارات الأداء على بيئات محدودة ولم تشمل جميع حالات الاستخدام الممكنة.

مقاومة التغيير:

واجه الفريق مقاومة من بعض الإدارات في المؤسسات المستهدفة لتغيير أنظمتها التقليدية.

ظهرت حاجة ماسة لبرامج تدريبية مكثفة لتسهيل عملية الانتقال للنظام الجديد.

الخلاصة

رغم هذه التحديات وجوانب القصور، إلا أنها مثلت فرصاً قيمة للتعلم والتطوير. وسيتم العمل على معالجتها في المراحل القادمة من خلال الخطط التطويرية التي تضمنتها التوصيات. ويبقى الهدف الأساسي هو تطوير نظام متكامل يحقق أعلى معايير الأمان مع الحفاظ على الكفاءة وسهولة الاستخدام.

6.4. التوصيات

بناءً على التحديات وجوانب القصور التي تم تحديدها خلال مراحل تنفيذ المشروع، يوصي الفريق بما يلي لتعزيز كفاءة النظام وأدائه الأمني:

دمج التقنيات الناشئة:

استكشاف تطبيقات Blockchain لإدارة الهويات

دراسة إمكانية تطبيق Homomorphic Encryption

تحسين تجربة المستخدم:

تطوير واجهات مستخدم متكيفة (Adaptive UI)

تطبيق حلول Voice-Activated Controls

تُمثل هذه التوصيات خارطة طريق لتطوير النظام وتعزيز كفاءته الأمنية. يُوصى بتبني هذه التوصيات بشكل تدريجي وفق أولويات المؤسسة ومواردها المتاحة، مع التركيز على تحقيق التوازن بين متطلبات الأمان وسهولة الاستخدام. كما يُشدد على أهمية المراجعة الدورية لهذه التوصيات لتواكب التطورات التقنية والمتطلبات الأمنية المستجدة.

6.5. الاعمال المستقبلية:

من خلال المشروع الذي قمنا بتنفيذه وعند التخطيط للقيام بهذا المشروع اردنا ان يكون المشروع قابل للتطوير والتوسعة والدمج مع أنظمة أخرى مثل:

- **النظام المحاسبي**
- **نظام جرد الأصول**
- **نظام المشتريات**
- **نظام جرد المخازن**
- **نظام إدارة المشاريع**
- **مع مراعاة ان النظام مرن وقابل للتطبيق على أي أنظمة أخرى**

6.6. الخاتمة

تم في هذا الفصل عرض عملية تنفيذ النظام واختباره، مع التركيز على الجوانب الأمنية والتقنية. النظام حقق الأهداف المطلوبة، لكن هناك دائماً مجال للتحسين، خاصة في مجال الأمان والتوسع الوظيفي. التوصيات المقدمة يمكن أن تكون خارطة طريق للتطوير المستقبلي.

المراجع:

الكتب والمراجع الورقية

1. Dwivedi, Himanshu. *Mobile Application Security*. McGraw-Hill, 2021.
2. Elenkov, Nikolay. *Android Security Internals*. No Starch Press, 2014.
3. Thiel, David. *iOS Application Security*. No Starch Press, 2016.
4. Chell, Dominic, et al. *The Mobile Application Hacker's Handbook*. Wiley, 2015.
5. Tamma, Rohit, et al. *Practical Mobile Forensics (4th Edition)*. Packt, 2020.

المقالات العلمية المحكمة

6. Zhang, Y., & Liu, P. "Secure Mobile Applications: A Framework for Threat Modeling." *IEEE Transactions on Mobile Computing*, vol. 19, no. 3, 2020, pp. 512–525. https://doi.org/10.1109/TMC.2019.2902123
7. Johnson, R., et al. "Comparative Analysis of Mobile App Security Testing Methodologies." *Journal of Cybersecurity Research*, vol. 7, no. 2, 2021, pp. 45–62.

الدراسات السابقة

8. Al-Hamdani, M. "Blockchain-Based Authentication for Mobile Applications." *International Journal of Information Security*, vol. 15, no. 4, 2019, pp. 321–335.
9. Smith, K., & Brown, L. "Vulnerability Assessment of Hybrid Mobile Applications." *Proceedings of the 15th International Conference on Security and Privacy*, 2022, pp. 112–128.

المراجع الإلكترونية والمواقع

10. OWASP Mobile Security Testing Guide, 2023. https://owasp.org/mstg
11. NIST Mobile Application Security Guidelines, 2022. https://www.nist.gov/mobile-security
12. Android Developers Security Guide. https://developer.android.com/security
13. Apple iOS Security Documentation. https://support.apple.com/security
14. Mobile App Security Best Practices – MITRE. https://www.mitre.org/mobile-security
15. Microsoft. https://www.microsoft.com
16. YouTube. https://www.youtube.com
17. Flutter Framework. https://flutter.dev
18. Wikipedia. https://www.wikipedia.org
19. IntelliJ IDEA. https://www.jetbrains.com/idea
20. Figma. https://www.figma.com
21. Supabase. https://www.supabase.com