الجامعة السورية الخاصة

كلية الهندسة المعلوماتية

قسم أمن النظم والشبكات الحاسوبية

نظام إدارة كلمات المرور

Password

Management System

اعداد الطلاب:

بسام المعاليقي

رياض الطحان

اشراف:

د. كريستين زينية

م. محمد أمجد الصفدي

2026

الملخص

يهدف هذا المشروع إلى تصميم وتطوير نظام متكامل لإدارة كلمات المرور يعتمد على أحدث معايير الأمن السيبراني، من خلال دمج التوثيق متعدد العوامل (Multi-Factor Authentication – MFA) بالاعتماد على العوامل البيومترية، وبشكل خاص التعرّف على الوجه، إضافةً إلى اعتماد بنية أمنية قائمة على مبدأ انعدام المعرفة (Zero-Knowledge Architecture) ، بما يضمن عدم كشف أي بيانات حساسة أثناء عمليات المصادقة.

يعتمد النظام على بروتوكول التحقق الآمن SRP (Secure Remote Password Protocol) للتحقق من هوية المستخدم دون الحاجة إلى إرسال كلمة المرور أو أي مشتقات مباشرة لها إلى الخادم، مما يحدّ من الهجمات الشائعة مثل هجوم الرجل في المنتصف (Man-in-the-Middle) . كما يستخدم النظام خوارزمية Argon2id لاشتقاق مفتاح تغليف رئيسي(Key Encryption Key – KEK) ، يُستخدم لتغليف مفتاح تشفير البيانات (Data Encryption Key – DEK) العشوائي الخاص بكل مستخدم. ويتم لاحقًا استخدام خوارزمية AES-GCM لتشفير البيانات الحساسة، بما في ذلك البصمات البيومترية وكلمات المرور المُدارة داخل النظام، لضمان السرية والسلامة ومنع التلاعب بالبيانات.

تم تنفيذ الواجهة الخلفية للنظام باستخدام إطار العمل FastAPI وربطها بقاعدة بيانات MySQL لتخزين البيانات المشفّرة، مع تطبيق آليات متقدمة للتحكم بالوصول تشمل التحكم المستند إلى الدور (RBAC) والتحكم المستند إلى الصفات(ABAC) ، بما يضمن إدارة دقيقة لصلاحيات المستخدمين. كما يوفر النظام مولّدًا لكلمات مرور عشوائية يتيح إنشاء كلمات مرور قوية وفق معايير أمان عالي.

أظهرت نتائج التطبيق العملي أن النظام المقترح يحقق مستوىً عالياً من الأمان مع الحفاظ على سهولة الاستخدام، ويعالج نقاط الضعف التقليدية المرتبطة بتخزين كلمات المرور وإدارتها، مما يجعله نموذجًا عمليًا وقابلًا للتطوير في البيئات الرقمية الحديثة.

Abstract

This project aims to design and develop an integrated Password Management System that complies with modern cybersecurity standards by incorporating Multi-Factor Authentication (MFA) using biometric factors, specifically facial recognition. The system is built upon a Zero-Knowledge security architecture, ensuring that no sensitive information is disclosed during the authentication process.

The proposed system employs the Secure Remote Password (SRP) protocol to authenticate users without transmitting passwords or their direct derivatives to the server, thereby mitigating common attacks such as Man-in-the-Middle (MITM). Furthermore, the Argon2id algorithm is utilized to derive a Key Encryption Key (KEK), which securely wraps a user-specific Data Encryption Key (DEK). The DEK is subsequently used with the AES-GCM encryption scheme to protect sensitive data, including biometric templates and stored credentials, ensuring confidentiality, integrity, and resistance to tampering.

The backend is implemented using FastAPI and connected to a MySQL database for encrypted data storage. Advanced access control mechanisms, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), are applied to ensure precise authorization management. In addition, the system provides a secure password generator that enables users to create strong and randomized passwords based on customizable security parameters.

The practical implementation results demonstrate that the proposed system achieves a high level of security while maintaining usability, effectively addressing traditional weaknesses in password storage and

management. Consequently, the system represents a practical and scalable solution suitable for modern digital environments facing increasing cybersecurity threats.

.

المحتويات

فهرس الجداول

فهرس الاشكال

فهرس الصور

المقدمة

في ظل التحول الرقمي المتسارع والاعتماد المتزايد على الخدمات الإلكترونية، أصبحت كلمات المرور الوسيلة الأساسية لحماية الحسابات الرقمية والوصول إلى البيانات الحساسة. إلا أن هذا الاعتماد الواسع ترافق مع ازدياد ملحوظ في الهجمات السيبرانية التي تستهدف بيانات الاعتماد، مستفيدةً من السلوك البشري في اختيار كلمات مرور ضعيفة أو إعادة استخدامها عبر عدة منصات، مما يشكّل نقطة ضعف جوهرية في أمن المعلومات.

بالإضافة الى ان الأساليب التقليدية في إدارة كلمات المرور تعاني من مشكلات متعددة، أبرزها تخزين كلمات المرور أو مشتقاتها على الخوادم، الأمر الذي يجعلها عرضة للاختراق في حال حدوث تسريب لقاعدة البيانات. كما أن الاكتفاء بكلمة المرور كوسيلة وحيدة للتحقق من هوية المستخدم لم يعد كافيًا في مواجهة التهديدات الحديثة مثل هجمات القوة الغاشمة (Brute Force Attacks) ، وهجمات التصيّد(Phishing) ، وهجمات الرجل في المنتصف (Man-in-the-Middle). وقد دفع ذلك إلى البحث عن حلول أكثر تقدمًا تجمع بين الأمان العالي، وحماية الخصوصية، وسهولة الوصول.

1. مشكلة البحث

تتمثل مشكلة البحث في القصور الأمني الذي تعاني منه أنظمة إدارة كلمات المرور التقليدية، والتي تعتمد غالبًا على آليات تحقق لا تمنع بشكل كافٍ تسريب بيانات الاعتماد أو استغلالها في حال اختراق النظام. كما أن العديد من هذه الأنظمة يربط حساب المستخدم بجهاز محدد، أو يتطلب نقل بيانات حساسة عبر الشبكة، مما يحدّ من إمكانية الوصول الآمن من أجهزة مختلفة.

إضافةً إلى ذلك، فإن بعض الحلول التي تضيف عوامل تحقق متعددة قد تؤثر سلبًا على الخصوصية، لا سيما عند التعامل مع البيانات البيومترية، في حين تفتقر حلول أخرى إلى بنية مفاتيح تشفير تضمن حماية البيانات المخزنة حتى في حال الوصول غير المصرح به إلى قاعدة البيانات. وبناءً على ذلك، تبرز الحاجة إلى نظام موحّد يدمج بين إدارة آمنة لكلمات المرور، ومصادقة قوية، وإمكانية الوصول من أي جهاز دون فقدان مستوى الأمان.

2. هدف المشروع

يهدف هذا المشروع إلى تصميم وتطوير نظام متكامل لإدارة كلمات المرور يوفّر مستوىً عالياً من الأمان، ويعالج نقاط الضعف الشائعة في الأنظمة التقليدية، من خلال اعتماد بنية أمنية حديثة تقوم على مبدأ انعدام المعرفة(Zero-Knowledge Architecture) ، بما يضمن عدم نقل كلمة المرور أو تخزينها بصيغة قابلة للاستغلال.

يركّز المشروع على استخدام بروتوكول التحقق الآمن SRP (Secure Remote Password Protocol)بوصفه آلية مصادقة قائمة على كلمة المرور دون الحاجة إلى إرسالها إلى الخادم، مع تحقيق مصادقة متبادلة بين المستخدم والنظام. كما يهدف إلى اعتماد بنية متقدمة لإدارة المفاتيح تعتمد على الفصل بين المفاتيح، من خلال استخدام مفتاح تشفير البيانات (Data Encryption Key – DEK)لتشفير البيانات الحساسة، ومفتاح مشتق (Key Encryption Key – KEK) لتغليف هذا المفتاح قبل تخزينه، بما يضمن حماية البيانات حتى في حال اختراق قاعدة البيانات.

كما يسعى المشروع إلى تمكين المستخدم من الوصول إلى بياناته المشفّرة من أي جهاز وفي أي وقت، دون ربط الحساب بجهاز محدد، وذلك اعتمادًا على آلية اشتقاق المفاتيح من كلمة المرور نفسها. إضافةً إلى ذلك، يعتمد النظام على التوثيق متعدد العوامل باستخدام التعرّف على الوجه كعامل بيومتري، يتم تنفيذه محليًا على جهاز المستخدم، دون إرسال الصور أو البيانات البيومترية إلى الخادم.

3. أهمية المشروع

تكمن أهمية هذا المشروع في معالجته إحدى القضايا الأساسية في مجال أمن المعلومات، وهي إدارة كلمات المرور بشكل آمن ومرن في آن واحد. إذ يقدّم المشروع نموذجًا يقلل من الاعتماد على الحلول التقليدية، وحل بعض مشاكل الأنظمة الحديثة عن طريق اعتماد على بروتوكولات تحقق آمنة وبنية تشفير تمنع استغلال البيانات حتى في حال تسريبها.

وتبرز أهمية المشروع في اعتماده على بروتوكولSRP ، الذي يمنع نقل كلمة المرور أو أي مشتقات مباشرة لها عبر الشبكة، ويحدّ من مخاطر الهجمات الشائعة المرتبطة بالمصادقة. كما تسهم بنية إدارة المفاتيح المعتمدة على KEK و DEKفي تقليل أثر أي اختراق محتمل لقاعدة البيانات، ومنع الوصول المباشر إلى البيانات الحساسة.

كما يولي المشروع أهمية خاصة لحماية الخصوصية، من خلال تنفيذ التحقق البيومتري باستخدام التعرّف على الوجه محليًا على جهاز المستخدم، دون تخزين أو نقل بيانات بيومترية خام، مما يقلل من احتمال الهجوم ويعزّز ثقة المستخدم بالنظام. وإضافةً إلى ذلك، يوفّر المشروع مرونة عالية في الاستخدام من خلال دعم الوصول من أجهزة متعددة، وهو ما يجعله مناسبًا للتطبيق في البيئات الحديثة التي تتطلب حلولًا آمنة وقابلة للتوسع.

1 الفصل الأول

الإطار النظري

1.1 التمهيد

يهدف هذا الفصل إلى عرض وشرح المفاهيم والنظريات الأساسية التي يستند إليها المشروع، والتي تشكّل الأساس العلمي والتقني لتصميم وتنفيذ نظام إدارة كلمات المرور المقترح. ويأتي هذا العرض بهدف توضيح الخلفية النظرية للتقنيات والخوارزميات والبروتوكولات المستخدمة، مع التركيز على دور كل منها في تعزيز أمن النظام وتحقيق متطلبات الحماية العالية للبيانات الحساسة.

2.1 نظام إدارة كلمات المرور

يُقصد بنظام إدارة كلمات المرور (Password Management System) منظومة برمجية تُستخدم لتوليد كلمات مرور قوية، وتخزينها وإدارتها بطريقة آمنة، بما يتيح للمستخدم الوصول إلى بيانات تسجيل الدخول الخاصة به دون الحاجة إلى حفظها. ويهدف هذا النوع من الأنظمة إلى تقليل المخاطر الأمنية الناتجة عن استخدام كلمات مرور ضعيفة أو مكررة عبر عدة منصات. [8][9][10]

تعتمد أنظمة إدارة كلمات المرور الحديثة على تقنيات تشفير متقدمة لحماية البيانات المخزنة، بحيث لا يتم الاحتفاظ بكلمات المرور بصيغتها الصريحة، وإنما تُخزن بعد معالجتها باستخدام خوارزميات تشفير أو تهشير مناسبة. ويُعد هذا الأسلوب عنصرًا أساسيًا في منع الوصول غير المصرح به إلى بيانات الاعتماد، حتى في حال حدوث اختراق لقاعدة البيانات. [6][15][16]

تتجاوز وظيفة نظام إدارة كلمات المرور مجرد التخزين الآمن، إذ تشمل عادةً توفير آليات لتوليد كلمات مرور عشوائية قوية وفق سياسات محددة، وإدارة بيانات تسجيل الدخول لمواقع وخدمات متعددة ضمن بيئة موحدة. كما تسعى هذه الأنظمة إلى تحسين تجربة المستخدم من خلال تقليل الاعتماد على الذاكرة البشرية، مع الحفاظ على مستوى عالٍ من الأمان.

ومع تطور التهديدات السيبرانية، أصبح من الضروري أن تتكامل أنظمة إدارة كلمات المرور مع آليات تحقق متقدمة، مثل التوثيق متعدد العوامل وبروتوكولات التحقق الآمن، لضمان أن الوصول إلى كلمات المرور المخزنة لا يتم إلا بعد التحقق الكامل من هوية المستخدم. ويُعد هذا التكامل أحد الركائز الأساسية في النظام المقترح في هذا المشروع، حيث سيتم لاحقًا توضيح كيفية دعم هذه الأنظمة ببنية تحقق وتشفير متقدمة تلبّي متطلبات الأمان الحديثة.

3.1 التوثيق متعدد العوامل(Multi-Factor Authentication –MFA) .

يُعد التوثيق متعدد العوامل (Multi-Factor Authentication – MFA) من أهم الآليات الحديثة المستخدمة لتعزيز أمن الأنظمة الرقمية، حيث يعتمد على التحقق من هوية المستخدم باستخدام أكثر من عامل تحقق مستقل بدلًا من الاعتماد على كلمة المرور وحدها. ويهدف هذا الأسلوب إلى تقليل مخاطر الوصول غير المصرح به، خاصة في الحالات التي يتم فيها تسريب كلمة المرور أو تخمينها بوسائل مختلفة. [4][15][19]

يقوم مفهوم التوثيق متعدد العوامل على مبدأ الجمع بين عوامل تحقق تنتمي إلى فئات مختلفة، بحيث لا يكون اختراق أحد العوامل كافيًا للوصول إلى النظام. ويؤدي هذا النهج إلى رفع مستوى الأمان بشكل ملحوظ مقارنة بالتحقق الأحادي، إذ تصبح عملية المصادقة أكثر مقاومة للهجمات الشائعة التي تستهدف بيانات الاعتماد.

تُصنّف عوامل التحقق المستخدمة في أنظمة MFA عادةً إلى ثلاث فئات رئيسية، يتم عرضها فيما يلي:

1.3.1 شيء يعرفه المستخدم(Something You Know)

يشير هذا العامل إلى المعلومات التي يمتلكها المستخدم معرفيًا، مثل كلمة المرور أو الرقم السري (PIN). ويُعد هذا العامل الأكثر شيوعًا في الأنظمة التقليدية، إلا أنه يُعتبر الأضعف من حيث الأمان، نظرًا لقابليته للتسريب أو التخمين أو إعادة الاستخدام عبر منصات متعددة. لذلك، لا يُعتمد على هذا العامل وحده في الأنظمة الحديثة ذات الحساسية العالية، بل يُستخدم كجزء من منظومة تحقق متعددة العوامل.

2.3.1 شيء يمتلكه المستخدم(Something You Have)

يمثل هذا العامل عنصرًا ماديًا يكون بحوزة المستخدم، مثل الهاتف الذكي، أو البطاقة الذكية، أو رمز تحقق يتم توليده عبر تطبيقات المصادقة أو إرساله من خلال الرسائل النصية. ورغم أن هذا العامل يضيف طبقة أمان إضافية، إلا أنه قد يتأثر بمشكلات عملية مثل فقدان الجهاز أو اعتراض الرموز، مما يجعله غير كافٍ للاعتماد عليه بشكل مستقل في بعض السيناريوهات الأمنية.

3.3.1 شيء يُمثل المستخدم(Something You Are)

يعتمد هذا العامل على الخصائص الفيزيائية أو السلوكية الفريدة للمستخدم، ويُعرف بالعوامل البيومترية(Biometric Factors) ، مثل بصمة الإصبع وبصمة الوجه. وتتميّز هذه العوامل

بصعوبة تقليدها أو مشاركتها، مما يجعلها من أكثر عوامل التحقق موثوقية في أنظمة الأمان الحديثة، خاصة عند دمجها مع عوامل تحقق أخرى. [4][19]

في إطار هذا المشروع، تم اعتماد مزيج من عاملين للتحقق من هوية المستخدم، هما :شيء يعرفه المستخدم (كلمة المرور)، وشيء يُمثله المستخدم (التحقق البيومتري) .ويهدف هذا الدمج إلى تحقيق توازن فعّال بين مستوى الأمان العالي وسهولة الاستخدام، دون الاعتماد على وسائل تحقق خارجية قد تؤثر على تجربة المستخدم أو تحدّ من إمكانية الوصول من أجهزة متعددة.

يسهم التوثيق متعدد العوامل في تعزيز مقاومة النظام للهجمات الشائعة، مثل هجمات القوة الغاشمة (Brute Force Attacks)وهجمات التصيّد(Phishing) ، حيث يصبح امتلاك كلمة المرور وحده غير كافٍ للوصول إلى الحساب. كما يُعد MFA عنصرًا أساسيًا في الأنظمة التي تتعامل مع بيانات حساسة، مثل أنظمة إدارة كلمات المرور، نظرًا لدوره في تقليل احتمالية الاختراق حتى في حال تسريب بيانات الاعتماد الأساسية. [15][19]

وبذلك، يشكّل التوثيق متعدد العوامل جزءًا محوريًا من البنية الأمنية للنظام المقترح في هذا المشروع، حيث يعمل جنبًا إلى جنب مع بروتوكولات التحقق الآمنة وآليات التشفير المتقدمة لضمان حماية شاملة لهوية المستخدم وبياناته.

4.1 العوامل البيومترية (Biometric Authentication)

يُعد التحقق البيومتري (Biometric Authentication) من أكثر أساليب التحقق تطورًا في أنظمة أمن المعلومات الحديثة، إذ يعتمد على خصائص فيزيائية أو سلوكية فريدة لكل مستخدم، مما يقلّل من احتمالية انتحال الهوية مقارنة بالعوامل المعرفية أو المادية. وتُستخدم هذه الآلية على نطاق واسع في الأنظمة التي تتطلب مستوى أمان مرتفعًا، نظرًا لصعوبة تقليد الخصائص البيومترية أو مشاركتها بين المستخدمين. [12][13]

في سياق هذا المشروع، تم اعتماد التعرّف على الوجه (Facial Recognition) بوصفه العامل البيومتري المستخدم ضمن منظومة التوثيق متعدد العوامل. ويأتي هذا الاختيار لما يوفّره من توازن بين مستوى الأمان، وسهولة الاستخدام، وإمكانية الوصول من أجهزة مختلفة، مع الحفاظ على متطلبات الخصوصية وعدم فرض قيود تشغيلية إضافية على المستخدم.

1.4.1 التعرّف على الوجه(Facial Recognition)

يعتمد التعرّف على الوجه على تحليل السمات المميّزة لوجه الإنسان، مثل توزيع الملامح والمسافات النسبية بين الأجزاء المختلفة للوجه، وتحويلها إلى تمثيل رقمي يُستخدم لاحقًا في عملية المطابقة. وقد شهدت هذه التقنية تطورًا ملحوظًا مع التقدم في تقنيات الرؤية الحاسوبية والتعلّم العميق، مما أسهم في رفع دقتها واعتمادها في التطبيقات الأمنية الحديثة.

في هذا المشروع، لا يتم التعامل مع صور الوجه بصيغتها الخام(Raw Images) ، بل تُعالج الصورة لاستخراج تمثيل رقمي (Face Encoding أوFace Descriptor) يُستخدم حصريًا لأغراض التحقق من هوية المستخدم. ويسهم هذا النهج في تقليل المخاطر المرتبطة بتخزين الصور البيومترية الخام، ويعزّز من حماية الخصوصية والامتثال للممارسات الأمنية الحديثة.

تم تنفيذ عملية التعرّف على الوجه محليًا على جهاز المستخدم(Client-side) ، دون إرسال الصور أو التمثيلات الرقمية إلى الخادم. ويأتي هذا القرار انسجامًا مع مبادئ التصميم الآمن وحماية الخصوصية، حيث لا يمتلك الخادم أي دور في معالجة البيانات البيومترية أو التحقق منها، ويقتصر دوره على إدارة الجلسات والتعامل مع البيانات المشفّرة فقط.

تعتمد آلية العمل على معالجة بيانات الوجه داخل المتصفح، حيث يتم استخراج التمثيل الرقمي ومقارنته محليًا بالتمثيل المعتمد للمستخدم. وفي حال نجاح عملية التحقق، يُسمح بالانتقال إلى الخطوات اللاحقة داخل النظام، مثل تنفيذ العمليات الحساسة أو الوصول إلى البيانات المشفّرة. أما في حال الفشل، فلا يتم إرسال أي بيانات إضافية إلى الخادم.

يسهم هذا الأسلوب في تقليل سطح الهجوم(Attack Surface Reduction) ، إذ يمنع نقل البيانات البيومترية عبر الشبكة، ويحدّ من مخاطر اعتراضها أو إساءة استخدامها. كما يتوافق مع مبدأ انعدام المعرفة(Zero-Knowledge) ، حيث لا يمتلك الخادم أي معلومات تمكّنه من إعادة بناء البيانات البيومترية أو استخدامها للتحقق بشكل مستقل. [12][14]

2.4.1 معالجة وتشفير البيانات البيومترية في النظام المقترح

يتم التعامل مع البيانات البيومترية في هذا المشروع بحساسية عالية، حيث لا يتم تخزين أي بيانات بيومترية بصيغتها الخام(Raw Data) . إذ تُعالج بيانات الوجه لاستخراج تمثيل رقمي

(Encoding)يُستخدم لأغراض التحقق فقط، ثم يُشفّر باستخدام خوارزمية AES-GCMبالاعتماد على مفتاح تشفير البيانات(Data Encryption Key – DEK) . [6][12][14]

ويُغلف مفتاح تشفير البيانات (DEK) باستخدام مفتاح مشتق (Key Encryption Key – KEK) قبل تخزينه، مما يضمن حماية البيانات البيومترية المخزنة حتى في حال اختراق قاعدة البيانات. ويمنع هذا الأسلوب الوصول إلى البيانات المشفّرة أو فك تشفيرها دون المرور بآليات التحقق والمصادقة المعتمدة في النظام، ويعزّز من طبقات الحماية ضمن البنية الأمنية المقترحة.

3.4.1 دور التحقق البيومتري في النظام.

يشكّل التحقق البيومتري باستخدام التعرّف على الوجه عنصرًا مكمّلًا لكلمة المرور ضمن منظومة التوثيق متعدد العوامل في النظام المقترح. فحتى في حال تسريب كلمة المرور، لا يمكن للمهاجم الوصول إلى الحساب دون اجتياز عامل التحقق البيومتري، مما يرفع مستوى الأمان ويقلّل من احتمالية الاختراق.

كما يتيح هذا النهج للمستخدم الاستفادة من عامل تحقق قوي دون الحاجة إلى أجهزة إضافية أو وسائل تحقق خارجية، مع الحفاظ على إمكانية الوصول إلى الحساب من أي جهاز. وبذلك، يسهم التحقق البيومتري في تحقيق هدف المشروع المتمثل في الجمع بين الأمان العالي، وحماية الخصوصية، وسهولة الاستخدام ضمن نظام موحّد لإدارة كلمات المرور.

5.1 بروتوكول التحقق الآمن SRP وبروتوكول Diffie–Hellman

يُعد اختيار بروتوكول المصادقة وتبادل المفاتيح من القرارات الجوهرية في تصميم أنظمة إدارة كلمات المرور، نظرًا لحساسية البيانات المتداولة أثناء عملية التحقق من هوية المستخدم. وفي هذا السياق، تم اعتماد بروتوكول التحقق الآمن SRP (Secure Remote Password Protocol) بدلًا من آليات تبادل المفاتيح التقليدية مثل(DH (Diffie–Hellman ، وذلك استنادًا إلى فروقات بنيوية وأمنية جوهرية بين النهجين. [2][3]

1.5.1 بروتوكول(DH (Diffie–Hellman

يُعد بروتوكول Diffie–Hellman من أقدم واشهر بروتوكولات تبادل المفاتيح، ويهدف إلى تمكين طرفين من الاتفاق على مفتاح سري مشترك عبر قناة غير آمنة. يعتمد DH على مبادئ

رياضية قائمة على صعوبة حل مسألة اللوغاريتم المنفصل، ويُستخدم على نطاق واسع كجزء من بروتوكولات أمان مثل TLS. [21]

إلا أن Diffie–Hellman ليس بروتوكول مصادقة بحد ذاته، بل يقتصر دوره على تبادل المفاتيح فقط. وهذا يعني أن البروتوكول لا يوفّر آلية مدمجة للتحقق من هوية الأطراف المتواصلة، مما يجعله عرضة لهجوم الرجل في المنتصف (Man-in-the-Middle – MITM) في حال عدم دمجه مع آليات مصادقة إضافية أو شهادات رقمية. كما أن DH لا يرتبط بمفهوم كلمة المرور، ولا يوفّر نموذج تحقق مناسبًا للأنظمة المعتمدة على كلمات المرور مثل أنظمة إدارة كلمات المرور.

2.5.1 بروتوكول التحقق الآمنSRP

بروتوكول SRP (Secure Remote Password Protocol) هو بروتوكول مصادقة وتبادل مفاتيح قائم على كلمة المرور، صُمّم خصيصًا لمعالجة نقاط الضعف الموجودة في الأنظمة التقليدية التي تعتمد على إرسال أو تخزين كلمات المرور. يعتمد SRP على مبدأ انعدام المعرفة (Zero-Knowledge Proof)، حيث يتم التحقق من صحة كلمة المرور دون إرسالها أو إرسال أي مشتقات مباشرة قابلة للاستغلال إلى الخادم.

يُحقق SRP مصادقة متبادلة (Mutual Authentication) بين العميل والخادم، بحيث يتأكد كل طرف من هوية الطرف الآخر قبل إنشاء المفتاح السري المشترك. كما يُعد البروتوكول مقاومًا لهجمات الرجل في المنتصف، لأن أي طرف غير شرعي لا يمتلك كلمة المرور الصحيحة لا يمكنه توليد القيم المطلوبة لإتمام عملية المصادقة.[3][2]

3.5.1 المقارنة بين SRP وDiffie–Hellman

يوضح الجدول (1-1) مقارنة بين بروتوكولي SRP و Diffie–Hellmanمن حيث الخصائص الأمنية والملاءمة لأنظمة إدارة كلمات المرور:

جدول 1-1 مقارنة بين بروتوكولي SRP وDiffie–Hellman

	DH	SRP
طبيعة البروتوكول	تبادل مفاتيح فقط	مصادقة + تبادل مفاتيح
الاعتماد على كلمة المرور	لا	نعم
إرسال كلمة المرور عبر الشبكة	غير مدعوم	لا
المصادقة المتبادلة	غير مدعوم	مدعومة
مقاومة هجومMITM	غير مضمونة	عالية
نموذج انعدام المعرفة Zero-Knowledge	غير مدعوم	مدعومة
الملاءمة لأنظمة إدارة كلمات المرور	منخفضة	عالية جدًا

4.5.1 مبررات اختيار SRP في هذا المشروع

تم اختيار بروتوكول SRP في هذا المشروع لكونه يلبّي متطلبات الأمان الخاصة بأنظمة إدارة كلمات المرور، حيث يوفّر آلية تحقق آمنة دون تعريض كلمة المرور أو أي مشتقات حساسة لخطر التسريب. كما يتيح دمج عملية المصادقة مع بنية إدارة المفاتيح المعتمدة في المشروع، ويضمن أن الوصول إلى البيانات المشفرة لا يتم إلا بعد التحقق الكامل من هوية المستخدم.

على عكس Diffie–Hellman، الذي يتطلب طبقات إضافية لتحقيق المصادقة، يوفّر SRP حلاً متكاملًا يجمع بين المصادقة وتبادل المفاتيح ضمن بروتوكول واحد، مما يقلل من التعقيد ويحد

من نقاط الضعف المحتملة. لذلك، يُعد SRP خيارًا مناسبًا وفعّالًا لبناء نظام إدارة كلمات مرور آمن يعتمد على أعلى معايير حماية عالية.

6.1 إدارة المفاتيح والتشفير

تُعد إدارة المفاتيح والتشفير من الركائز الأساسية في تصميم الأنظمة الآمنة، ولا سيما أنظمة إدارة كلمات المرور التي تتعامل مع بيانات شديدة الحساسية. فحتى مع اعتماد آليات مصادقة قوية، يبقى أمن البيانات المخزنة مرتبطًا بشكل مباشر بكيفية توليد المفاتيح، واستخدامها، وحمايتها من الوصول غير المصرّح به. ومن هذا المنطلق، يجب تحقيق أعلى مستوى من الحماية مع الحفاظ على مرونة الوصول من أجهزة متعددة.

1.6.1 المفهوم العام لإدارة المفاتيح(Key Management Concept)

تعتمد أنظمة التشفير الحديثة على مبدأ الفصل بين المفاتيح(Key Separation) ، حيث لا يُستخدم مفتاح واحد لجميع الأغراض، بل يتم توزيع الأدوار على مفاتيح مختلفة لكل وظيفة أمنية. ويسهم هذا المبدأ في تقليل أثر أي اختراق محتمل، إذ لا يؤدي كشف أحد المفاتيح بالضرورة إلى كشف جميع البيانات. [5][6]

في هذا المشروع، تم اعتماد بنية هرمية لإدارة المفاتيح (Key Hierarchy) تتكون من:

- مفتاح تشفير البيانات(Data Encryption Key – DEK) :

  يُستخدم لتشفير البيانات الحساسة الخاصة بالمستخدم، مثل كلمات المرور المُدارة والتمثيلات الرقمية للبيانات البيومترية.

- مفتاح تشفير المفاتيح(Key Encryption Key – KEK) :

  يُستخدم لتغليف (Wrapping) مفتاح DEK وحمايته قبل تخزينه.

ويتم تخزين مفتاح DEK بشكل مشفّر فقط، ولا يُخزَّن أي مفتاح تشفير بصيغة مكشوفة داخل قاعدة البيانات. ويضمن هذا الأسلوب أن الوصول إلى البيانات المشفّرة لا يتم إلا بعد المرور بآليات التحقق والمصادقة المعتمدة في النظام.

تُسهم هذه البنية أيضًا في تحقيق إحدى الميزات الجوهرية للمشروع، وهي إمكانية الوصول إلى الحساب من أي جهاز وفي أي وقت، إذ يتم اشتقاق KEK في كل مرة اعتمادًا على بيانات المستخدم نفسها، دون الحاجة إلى ربط الحساب بجهاز محدد.

2.6.1 اشتقاق مفتاح KEK باستخدامArgon2id

يتم اشتقاق مفتاح تشفير المفاتيح (KEK) من كلمة مرور المستخدم باستخدام خوارزمية Argon2id، وهي خوارزمية حديثة مصمّمة خصيصًا لمقاومة هجمات التخمين والهجمات المعتمدة على العتاد(GPU/ASIC Attacks) . وتعتمد عملية الاشتقاق على دمج كلمة المرور مع قيمة عشوائية(Salt) ، مما يمنع هجمات الجداول الجاهزة (Rainbow Tables) ويزيد من كلفة الهجوم الحسابية [5].

يضمن هذا الأسلوب أن:

- KEKلا يتم تخزينه داخل النظام.
- يتم توليد KEK ديناميكيًا عند كل عملية تحقق ناجحة.
- لا يمكن استنتاج KEK دون امتلاك كلمة المرور الصحيحة.

وبذلك، تبقى مفاتيح التشفير محمية حتى في حال الوصول غير المصرّح به إلى قاعدة البيانات، حيث لا تكون كلمة المرور أو المفتاح المشتق متاحة للمهاجم.

3.6.1 تشفير البيانات

توجد عدة طرق لتحقيق سرية البيانات وسلامتها في الأنظمة الآمنة، ومن أكثر الأساليب شيوعًا استخدام خوارزمية AES للتشفير مع خوارزمية HMAC لتحقيق السلامة، أو استخدام أنماط التشفير الموثّق (Authenticated Encryption) مثلAES-GCM . ويُعد فهم الفروقات بين هذين النهجين أمرًا ضروريًا لتبرير اختيار آلية التشفير المناسبة في أنظمة إدارة كلمات المرور.

يعتمد أسلوب AES + HMACعلى تنفيذ عمليتين منفصلتين، حيث تُستخدم خوارزمية AES لتشفير البيانات، ثم تُستخدم خوارزمية HMAC للتحقق من سلامة البيانات وصحتها. ورغم أن هذا الأسلوب يوفّر مستوىً جيدًا من الأمان عند تطبيقه بشكل صحيح، إلا أنه يزيد من تعقيد التنفيذ، ويتطلب إدارة مفاتيح متعددة، كما قد يؤدي إلى أخطاء أمنية في حال تنفيذ الترتيب بشكل غير صحيح.

في المقابل، يوفّر نمط AES-GCM آلية تشفير موثّق مدمجة، حيث يحقق السرية وسلامة البيانات والتحقق من صحتها ضمن عملية واحدة وباستخدام مفتاح واحد. ويتميّز هذا النمط بكفاءته العالية وأدائه الأفضل، إضافةً إلى تقليل احتمالية الأخطاء البرمجية الناتجة عن الدمج غير الصحيح بين التشفير والتحقق [6].

يوضح الجدول (2-1) مقارنة بين AES-GCM وAES + HMAC .

جدول 2-1 مقارنة بين AES-GCM و AES + HMAC

	AES-GCM	AES + HMAC
نوع التشفير	تشفير موثّق (Authenticated Encryption)	تشفير + تحقق منفصل
السرية	مدعومة	مدعومة
السلامة	مدعومة	مدعومة
التحقق من صحة البيانات	مدمج	منفصل
عدد المفاتيح	مفتاح واحد	مفتاحان غالبًا
الأداء	عالي	أقل نسبيًا
الملاءمة لأنظمة إدارة كلمات المرور	عالية جدًا	متوسطة

وبناءً على هذه المقارنة، تم اختيار AES-GCM في هذا المشروع لكونه يوفّر حلاً متكاملًا وبسيطًا من الناحية الأمنية والتنفيذية، ويقلّل من مخاطر الأخطاء البرمجية، مع الحفاظ على

مستوى عالٍ من الأمان، وهو ما يجعله مناسبًا لتشفير البيانات الحساسة في أنظمة إدارة كلمات المرور.

4.6.1 تكامل إدارة المفاتيح مع بروتوكولSRP

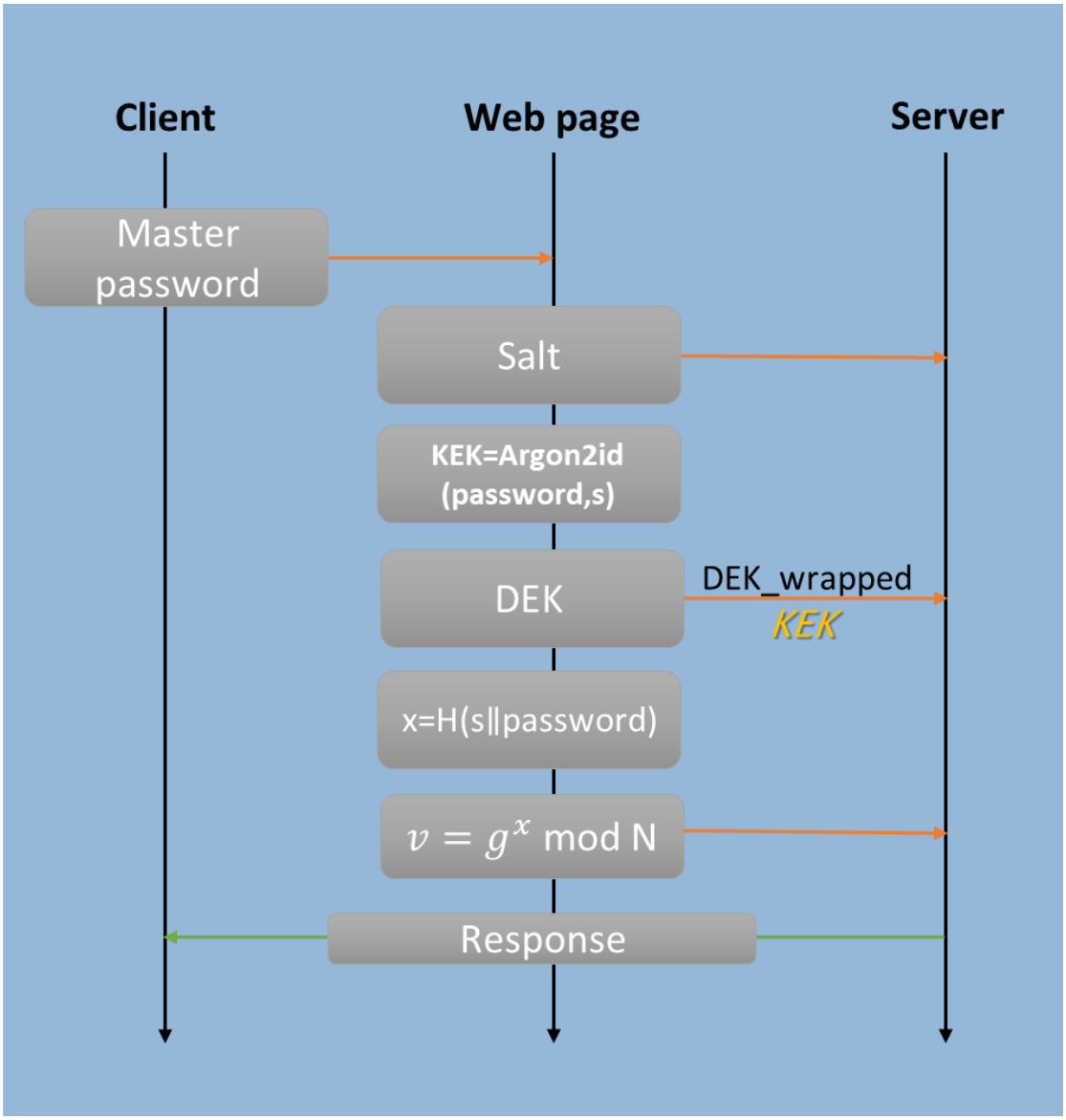
يتكامل نظام إدارة المفاتيح في هذا المشروع تكاملًا مباشرًا مع بروتوكول التحقق الآمنSRP ، بحيث تُعد عملية المصادقة الناجحة باستخدام SRP المرحلة الأساسية التي يُبنى عليها الوصول إلى المفاتيح المشفّرة والبيانات الحساسة. إذ لا يتم اشتقاق مفتاح تشفير المفاتيح (Key Encryption Key – KEK)إلا بعد التأكد الكامل من صحة هوية المستخدم، مما يمنع أي محاولة للوصول إلى مفاتيح التشفير دون اجتياز آلية المصادقة المعتمدة.

عند نجاح المصادقة، يتم اشتقاق KEK اعتمادًا على بيانات المستخدم نفسها، دون الحاجة إلى نقل كلمة المرور أو أي مفاتيح تشفير عبر الشبكة. ويُستخدم هذا المفتاح لفك تغليف مفتاح تشفير البيانات(Data Encryption Key – DEK) ، والذي يكون محفوظًا داخل قاعدة البيانات بصيغة مشفّرة فقط. وبذلك، لا يصبح الوصول إلى البيانات المشفّرة ممكنًا إلا ضمن سياق جلسة مصادقة صحيحة، وبعد المرور بجميع طبقات التحقق المطلوبة.

يسهم هذا التكامل بين SRP وإدارة المفاتيح في ترسيخ بنية انعدام المعرفة (Zero-Knowledge Architecture)المعتمدة في المشروع، حيث لا يمتلك الخادم أي معلومات تمكّنه من استنتاج كلمة المرور أو إعادة توليد المفاتيح بشكل مستقل. وحتى في حال حصول المهاجم على وصول كامل إلى قاعدة البيانات، تبقى البيانات المشفّرة غير قابلة للفك دون امتلاك كلمة المرور الصحيحة وتنفيذ بروتوكول المصادقة بالكامل.

وبذلك، يشكّل التكامل بين بروتوكول SRP وبنية إدارة المفاتيح طبقة حماية أساسية في النظام المقترح، تضمن الفصل التام بين عملية المصادقة وتخزين البيانات، وتُعزز من مقاومة النظام للهجمات التي تستهدف بيانات الاعتماد أو مفاتيح التشفير.

ويوضّح الشكل (3-1) آلية التكامل بين بروتوكول التحقق الآمن SRP وبنية إدارة المفاتيح في النظام المقترح، حيث يتم اشتقاق مفتاح KEK من كلمة المرور عند انشاء الحساب، ثم استخدامه لتغليف مفتاح DEK المولد عشوائياً دون إرسال أي معلومات حساسة عبر الشبكة.



شكل رقم 1-1 آلية تكامل بروتوكول SRP مع بنية إدارة المفاتيح (KEK / DEK) في النظام المقترح

خاتمة

تناول هذا الفصل المفاهيم الأساسية والنظريات الأمنية التي استند إليها تصميم نظام إدارة كلمات المرور المقترح، وشكّلت الأساس العلمي للقرارات المعتمدة في بنية النظام. وقد بدأ الفصل بعرض مفهوم أنظمة إدارة كلمات المرور وأهميتها في الحد من المخاطر الأمنية المرتبطة باستخدام كلمات المرور التقليدية، ثم انتقل إلى توضيح دور التوثيق متعدد العوامل في تعزيز عملية التحقق من هوية المستخدم.

كما استعرض الفصل مفهوم التحقق البيومتري مع التركيز على التعرّف على الوجه بوصفه العامل البيومتري المطبّق في المشروع، وبيّن آلية تنفيذه محليًا على جهاز المستخدم حفاظًا على الخصوصية وتقليل سطح الهجوم. وتم التطرّق بعد ذلك إلى بروتوكول التحقق الآمنSRP ، مع توضيح مبررات اختياره بدلًا من آليات تبادل المفاتيح التقليدية مثلDiffie–Hellman ، لما يوفّره من مصادقة قائمة على مبدأ انعدام المعرفة ومقاومة للهجمات الشائعة.

واختُتم الفصل بشرح مبادئ إدارة المفاتيح والتشفير في النظام المقترح، من خلال اعتماد بنية هرمية تعتمد على الفصل بين المفاتيح واستخدام خوارزميات تشفير حديثة، بما يضمن حماية البيانات الحساسة حتى في حال اختراق قاعدة البيانات، ويدعم إمكانية الوصول الآمن من أجهزة متعددة دون ربط الحساب بجهاز محدد.

يمهّد هذا الفصل للفصل التالي، الذي يتناول الدراسات السابقة ذات الصلة بموضوع إدارة كلمات المرور والتوثيق الآمن، حيث سيتم تحليل الحلول المقترحة في الأدبيات السابقة ، تمهيدًا لإبراز إسهام هذا المشروع وموقعه ضمن التطورات الحديثة في مجال أمن المعلومات.

2 الفصل الثاني

الدراسات السابقة

1.2 تمهيد

يهدف هذا الفصل إلى استعراض وتحليل الدراسات والأبحاث السابقة ذات الصلة بموضوع إدارة كلمات المرور والتوثيق الآمن، وذلك لتكوين إطار مرجعي يوضح التطورات التي شهدها هذا المجال، ونقاط القوة والقصور في الحلول المقترحة سابقًا. ولا يقتصر هذا العرض على السرد الوصفي للأعمال السابقة، بل يركّز على تحليلها ومقارنتها من منظور أمني ووظيفي، بما يبرز الحاجة إلى تطوير حلول أكثر تكاملًا ومرونة.

يتناول الفصل مجموعة من المحاور الأساسية، تشمل أنظمة إدارة كلمات المرور، وبروتوكولات المصادقة القائمة على كلمة المرور، والتوثيق متعدد العوامل، والعوامل البيومترية، إضافةً إلى آليات إدارة المفاتيح والتشفير. ويُختتم الفصل بمقارنة تحليلية توضّح موقع المشروع المقترح بين هذه الدراسات، والفجوة البحثية التي يسعى إلى معالجتها، تمهيدًا للفصل اللاحق الذي يتناول تصميم النظام وتطويره.

2.2 الدراسات السابقة في أنظمة إدارة كلمات المرور

تنقسم الدراسات السابقة في أنظمة إدارة كلمات المرور الى:

1.2.2 أنظمة إدارة كلمات المرور التقليدية

شكّلت أنظمة إدارة كلمات المرور التقليدية المرحلة الأولى في تطور حلول حماية بيانات الاعتماد، حيث ركّزت على توفير وسيلة مركزية لتخزين كلمات المرور واسترجاعها عند الحاجة. وقد اعتمدت هذه الأنظمة في الغالب على تخزين كلمات المرور أو مشتقاتها ضمن قواعد بيانات مركزية، مع استخدام خوارزميات تهشير أو تشفير أساسية لحماية البيانات المخزنة. [19][20]

ورغم أن هذه الأنظمة أسهمت في تقليل الاعتماد على حفظ كلمات المرور يدويًا، إلا أنها عانت من نقاط ضعف جوهرية. إذ إن الاعتماد على كلمة المرور كعامل وحيد للتحقق من هوية المستخدم جعلها عرضة للهجمات الشائعة، مثل هجمات القوة الغاشمة وهجمات التصيّد. كما أن النموذج المركزي للثقة، الذي يتيح للخادم الوصول إلى البيانات أو مفاتيح التشفير، جعل هذه الأنظمة حساسة بشكل كبير لأي اختراق أو تسريب لقاعدة البيانات. [15][19]

إضافةً إلى ذلك، افتقرت العديد من الحلول التقليدية إلى آليات تحقق متعددة العوامل أو طبّقتها بشكل محدود، كما أنها غالبًا ما ربطت حساب المستخدم بجهاز أو بيئة تشغيل محددة، مما حدّ من

مرونة الوصول الآمن من أجهزة متعددة. وقد بيّنت الدراسات أن هذه القيود تجعل الأنظمة التقليدية غير قادرة على تلبية متطلبات الأمان الحديثة.

2.2.2 الأنظمة المعتمدة على التشفير من طرف إلى طرف(End-to-End Encryption)

استجابةً للقصور في الأنظمة التقليدية، اتجهت الدراسات الحديثة إلى تطوير أنظمة إدارة كلمات مرور تعتمد على مبدأ التشفير من طرف إلى طرف(End-to-End Encryption – E2EE) ، حيث يتم تشفير البيانات على جهاز المستخدم ولا يمكن فك تشفيرها إلا من قبله. ويهدف هذا النموذج إلى تقليل الثقة بالخادم ومنع وصوله إلى البيانات الحساسة حتى في حال اختراقه.

تعتمد هذه الأنظمة عادةً على اشتقاق مفاتيح التشفير من كلمة مرور المستخدم، مع تخزين البيانات المشفّرة فقط على الخادم. وقد أسهم هذا التوجه في رفع مستوى الأمان وحماية الخصوصية، إلا أن بعض الحلول لا تزال تواجه تحديات تتعلق بإدارة المفاتيح، أو ربط الحساب بجهاز محدد، أو الاعتماد على نماذج تحقق لا تمنع إرسال معلومات حساسة أثناء المصادقة.

كما تشير بعض الدراسات إلى أن تطبيق E2EE دون دمجه مع بروتوكولات مصادقة قائمة على مبدأ انعدام المعرفة قد يترك ثغرات محتملة أثناء عملية تسجيل الدخول أو استعادة الحساب، مما يستدعي استخدام آليات تحقق أكثر تقدمًا لضمان حماية شاملة.

3.2.2 تحليل نماذج الأمان في أنظمة إدارة كلمات المرور التجارية

تناولت العديد من الدراسات الأكاديمية والتقارير التقنية نماذج الأمان المعتمدة في أنظمة إدارة كلمات المرور التجارية واسعة الانتشار، مثل 1Password و Bitwarden وLastPass. وتُعد هذه الأنظمة أمثلة بارزة على تبنّي مفاهيم حديثة مثل التشفير القوي، والتوثيق متعدد العوامل، وإدارة الخزائن الرقمية. [8][9][10] [11]

تعتمد هذه الأنظمة بدرجات متفاوتة على التشفير من طرف إلى طرف، وتوفّر آليات تحقق إضافية لتعزيز الأمان. إلا أن الدراسات أشارت إلى وجود فروقات جوهرية بينها من حيث نموذج الثقة، وآلية المصادقة، وإدارة المفاتيح، إضافة إلى تعاملها مع الخصوصية وإمكانية الوصول من أجهزة متعددة.

ومن خلال تحليل هذه الأنظمة، يمكن استخلاص مجموعة من الملاحظات التي تبرز الحاجة إلى نماذج أكثر تكاملًا تجمع بين المصادقة القائمة على انعدام المعرفة، وإدارة مفاتيح متقدمة، ودعم التحقق البيومتري دون المساس بخصوصية المستخدم.

كما ان الجدول (1-2) يوضح مقارنة تحليلية بين أنظمة إدارة كلمات المرور التجارية

1Password	Dashlane	Bitwarden	
Master Password + MFA	Master Password + MFA	Master Password + MFA	**آلية الدخول**
TOTP / Push	TOTP / SMS	TOTP / Email	**استخدام MFA**
AES-256-GCM	AES-256	AES-256-CBC + HMAC	**التشفير المستخدم**
مفتاح مشتق من كلمة المرور + مفتاح سري إضافي(Secret Key)	مفتاح مشتق من كلمة المرور	مفتاح مشتق من كلمة المرور	آلية إدارة المفاتيح
مدعومة جزئيًا	غير مدعومة	غير مدعومة	**المصادقة المتبادلة**
نعم لكن يحتاج ربط الحساب مع كل جهاز	نعم	نعم	**العمل من أجهزة متعددة**

جدول 1-2مقارنة تحليلية بين أنظمة إدارة كلمات المرور التجارية

تحليل مقارن وخلاصة

يُظهر التحليل المقارن أن أنظمة إدارة كلمات المرور التجارية قدّمت حلولًا متقدمة مقارنة بالأنظمة التقليدية، خاصة فيما يتعلق بالتشفير وحماية الخصوصية. إلا أنها تظل في إطار نماذج تجارية تفتقر في بعض الجوانب إلى الوضوح الأكاديمي في بنية المصادقة وإدارة المفاتيح، كما أن التحقق من العامل الثاني غالباً ما يكون معتمدًا على الجهاز او على جهاز اخر وليس جزءًا من تصميم أمني مستقل.

3.2 الدراسات السابقة في بروتوكولات المصادقة

تمثّل بروتوكولات المصادقة (Authentication Protocols) عنصرًا أساسيًا في أمن الأنظمة الرقمية، إذ تُستخدم للتحقق من هوية المستخدم قبل السماح له بالوصول إلى الموارد المحمية. وقد ركّزت الدراسات السابقة على تطوير آليات مصادقة تعتمد على كلمة المرور بوصفها أكثر وسائل التحقق شيوعًا، مع السعي إلى تقليل المخاطر المرتبطة بتسريبها أو إساءة استخدامها. [2][3][4]

تُظهر الأدبيات أن الاعتماد على كلمة المرور وحدها لم يعد كافيًا لمواجهة التهديدات الحديثة، مما دفع الباحثين إلى اقتراح بروتوكولات مصادقة أكثر تطورًا، تتفاوت في مستوى الأمان، وآلية العمل، ونموذج الثقة المعتمد بين العميل والخادم.

1.3.2 المصادقة التقليدية المعتمدة على كلمة المرور

اعتمدت الأنظمة التقليدية لفترة طويلة على نموذج مصادقة بسيط، يقوم على إرسال كلمة المرور من العميل إلى الخادم، إما بصيغة صريحة أو بعد تطبيق عملية تهشير. ورغم إدخال تحسينات مثل استخدام قنوات اتصال آمنة (TLS) وتخزين كلمات المرور على شكل قيم مُهشَّرة، إلا أن هذا النموذج ظلّ عرضة لعدة تهديدات، أبرزها إمكانية تعرّض كلمات المرور لهجمات التصيّد، أو هجمات الرجل في المنتصف، أو الاستغلال في حال اختراق قاعدة البيانات. كما أن الخادم يمتلك في هذا النموذج معلومات كافية للتحقق من كلمة المرور، مما يجعله نقطة ثقة مركزية وأحد الأهداف الرئيسة للهجمات.

2.3.2 بروتوكولات المصادقة القائمة على تبادل المفاتيح

استجابةً لقيود المصادقة التقليدية، اقترحت بعض الدراسات استخدام بروتوكولات تبادل المفاتيح، مثلDiffie–Hellman ، كجزء من عملية المصادقة. ويهدف هذا النهج إلى إنشاء مفتاح سري مشترك بين الطرفين دون إرسال معلومات حساسة عبر الشبكة. [21]

إلا أن الدراسات أوضحت أن بروتوكولات تبادل المفاتيح، رغم أهميتها، لا تُعد بروتوكولات مصادقة بحد ذاتها، لكونها لا توفّر تحققًا صريحًا من هوية الأطراف. كما أنها لا ترتبط مباشرة بمفهوم كلمة المرور، وتتطلب دمجها مع آليات إضافية لتحقيق مصادقة كاملة، مما يزيد من تعقيد النظام ويترك مجالًا لأخطاء التصميم أو التنفيذ.

3.3.2 بروتوكولات المصادقة المعتمدة على كلمة المرور-(PAKE- Password Authenticated Key Exchange)

قدّمت الأدبيات فئة متقدمة من بروتوكولات المصادقة تُعرف باسم بروتوكولات المصادقة وتبادل المفاتيح المعتمدة على كلمة المرور وتهدف هذه البروتوكولات إلى تمكين طرفين من المصادقة وإنشاء مفتاح سري مشترك بالاعتماد على كلمة مرور مشتركة، دون كشفها أو إرسالها عبر الشبكة.

تتميّز بروتوكولات PAKE بقدرتها على تقليل المخاطر المرتبطة بتسريب كلمات المرور، كما أنها تُصمَّم لمقاومة هجمات الرجل في المنتصف وهجمات التخمين غير المتصل. وقد تناولت الدراسات عدة نماذج ضمن هذه الفئة، تختلف في مستوى تعقيدها ودرجة توحيدها القياسي.[22]

4.3.2 بروتوكول SRP

يُعد بروتوكول SRP (Secure Remote Password) من أبرز البروتوكولات التي حظيت باهتمام واسع في الأدبيات الأكاديمية والمعايير التقنية. وقد ركّزت الدراسات على خصائص SRPالأمنية، مثل اعتماده على مبدأ انعدام المعرفة، وتوفيره مصادقة متبادلة بين العميل والخادم، دون الحاجة إلى نقل كلمة المرور أو مشتقاتها. [2] [3]

تشير الدراسات إلى أن SRP يتميّز عن غيره من البروتوكولات بكونه موحّدًا قياسيًا، ومناسبًا للأنظمة المعتمدة على كلمة المرور، خاصة في البيئات التي تتطلب مستوىً عاليًا من الأمان وحماية الخصوصية. كما أوضحت الأبحاث أن استخدام SRP يحدّ بشكل كبير من أثر اختراق

الخادم أو تسريب قاعدة البيانات، لعدم امتلاك الخادم معلومات كافية لإعادة توليد كلمة المرور أو المفاتيح السرية.

5.3.2 خلاصة تحليلية

في البداية يوضح جدول (2-2) مقارنة بين نماذج بروتوكولات المصادقة

	المصادقة التقليدية	Diffie–Hellman	PAKE	SRP
الاعتماد على كلمة المرور	نعم	لا	نعم	نعم
إرسال كلمة المرور عبر الشبكة	نعم / غير مباشر	لا	لا	لا
مصادقة متبادلة	غير مدعومة	غير مدعومة	مدعومة جزئيًا	مدعومة بالكامل
مقاومة هجوم MITM	ضعيفة	غير مضمونة	جيدة	عالية
نموذج Zero-Knowledge	غير مدعومة	غير مدعومة	مدعوم	مدعوم

جدول 2-2 مقارنة بين نماذج بروتوكولات المصادقة

من خلال استعراض الدراسات السابقة في مجال بروتوكولات المصادقة، يتبيّن أن الانتقال من المصادقة التقليدية إلى بروتوكولات قائمة على انعدام المعرفة يمثّل توجّهًا واضحًا في الأنظمة الحديثة. ورغم تعدد الحلول المقترحة، لا تزال بعض الأنظمة تعتمد على نماذج مصادقة لا توفّر حماية كافية ضد الهجمات المتقدمة.

تشير هذه النتائج إلى الحاجة إلى دمج بروتوكولات مصادقة قياسية قائمة على كلمة المرور، مثل SRP، ضمن أنظمة إدارة كلمات المرور بطريقة متكاملة مع آليات التشفير وإدارة المفاتيح، وهو ما يسعى المشروع المقترح إلى تحقيقه في الفصول اللاحقة.

4.2 الدراسات السابقة في التوثيق متعدد العواملMFA

حظي التوثيق متعدد العوامل (MFA) باهتمام واسع في الدراسات الأكاديمية والتقارير التقنية، نظرًا لدوره المحوري في تعزيز أمن الأنظمة الرقمية والحد من المخاطر المرتبطة بالاعتماد على كلمة المرور كعامل تحقق وحيد. وقد أظهرت الدراسات أن دمج أكثر من عامل تحقق مستقل يساهم بشكل كبير في تقليل احتمالية الوصول غير المصرّح به، حتى في حال تسريب بيانات الاعتماد الأساسية. [12][13]

تركّزت الأبحاث في هذا المجال على تحليل فعالية MFA في مواجهة الهجمات الشائعة، ودراسة نماذج تطبيقه في الأنظمة الحساسة، إضافةً إلى التحديات العملية التي تواجه اعتماده على نطاق واسع.

1.4.2 نماذج التوثيق متعدد العوامل في الدراسات السابقة

تشير الدراسات إلى أن نماذج MFA تعتمد على دمج عاملين أو أكثر من فئات تحقق مختلفة، تشمل:

- شيئًا يعرفه المستخدم (كلمة المرور).
- شيئًا يمتلكه (جهاز أو رمز).
- وشيئًا يُمثله (العوامل البيومترية).

وقد أظهرت النتائج أن الجمع بين عوامل من فئات مختلفة أكثر فاعلية من استخدام عدة عوامل من الفئة نفسها. ركزت بعض الدراسات على دمج كلمة المرور مع رموز تحقق مؤقتة (One-Time Passwords – OTP) يتم توليدها عبر تطبيقات مخصّصة أو إرسالها عبر الرسائل النصية. ورغم أن هذا النموذج يضيف طبقة أمان إضافية، إلا أن الأبحاث أشارت إلى محدوديته في مواجهة بعض الهجمات، مثل اعتراض الرسائل أو اختراق الأجهزة المحمولة.

في المقابل، تناولت دراسات أخرى دمج كلمة المرور مع العوامل البيومترية، وبيّنت أن هذا النموذج يوفّر مستوىً أعلى من الموثوقية، نظرًا لصعوبة نسخ أو مشاركة الخصائص البيومترية مقارنةً بكلمات المرور أو الرموز المؤقتة. [4][15][19]

2.4.2 أثر التوثيق متعدد العوامل في تقليل الهجمات

أظهرت الدراسات التحليلية أن اعتماد MFA يقلّل بشكل ملحوظ من نجاح الهجمات المعتمدة على سرقة كلمات المرور، مثل هجمات التصيّد وهجمات القوة الغاشمة. إذ يصبح امتلاك كلمة المرور وحده غير كافٍ للوصول إلى الحساب، ما يفرض على المهاجم تجاوز عامل تحقق إضافي غالبًا ما يكون خارج نطاق سيطرته.

كما بيّنت الأبحاث أن MFA يحدّ من أثر اختراق قواعد البيانات، حيث لا تؤدي سرقة بيانات الاعتماد الأساسية إلى اختراق فوري للحسابات. وتُعد هذه الخاصية ذات أهمية خاصة في الأنظمة التي تتعامل مع بيانات حساسة، مثل أنظمة إدارة كلمات المرور، التي تمثّل هدفًا جذابًا للمهاجمين.

3.4.2 التحديات العملية لتطبيق MFA في الأنظمة الحديثة

على الرغم من الفوائد الأمنية الكبيرة التي يوفّرهاMFA ، تشير الدراسات إلى وجود مجموعة من التحديات التي قد تعيق تطبيقه بشكل فعّال. من أبرز هذه التحديات التأثير المحتمل على تجربة المستخدم، خاصة في حال اعتماد وسائل تحقق معقّدة أو غير مريحة، مما قد يدفع المستخدمين إلى تعطيلها أو تجنب استخدامها.

كما تناولت بعض الدراسات قضايا تتعلق بالخصوصية، خاصة عند استخدام العوامل البيومترية، حيث شدّدت على ضرورة التعامل مع هذه البيانات بحساسية عالية، وتجنب تخزينها بصيغ خام أو نقلها عبر الشبكة. وأكّدت الأبحاث أن نجاح تطبيق MFA لا يعتمد فقط على قوة العوامل المستخدمة، بل أيضًا على طريقة دمجها ضمن بنية أمنية متكاملة تراعي الخصوصية وسهولة الاستخدام.

4.4.2 الخلاصة

يتبيّن من استعراض الدراسات السابقة أن التوثيق متعدد العوامل يُعد عنصرًا أساسيًا في الأنظمة الأمنية الحديثة، وقد أثبت فعاليته في تقليل مخاطر الاختراق والحد من الاعتماد المفرط على كلمة المرور. إلا أن نجاحه يعتمد على اختيار العوامل المناسبة وطريقة تطبيقها ضمن النظام، بما يحقق توازنًا بين الأمان والمرونة. [12][19]

تشير هذه النتائج إلى أهمية دمج MFA ضمن أنظمة إدارة كلمات المرور بطريقة مدروسة، تراعي الخصوصية وتجربة المستخدم، وتتكامل مع بروتوكولات مصادقة آمنة وآليات تشفير متقدمة. ويُعد هذا التوجّه أساسًا لما يعتمده المشروع المقترح، كما سيتم توضيحه في الفصول اللاحقة.

5.2 الدراسات السابقة في التحقق البيومتري

شهد التحقق البيومتري اهتمامًا متزايدًا في الدراسات الأكاديمية بوصفه أحد أكثر أساليب التوثيق موثوقية، نظرًا لاعتماده على الخصائص الفيزيائية أو السلوكية الفريدة للأفراد. وقد ركّزت الأبحاث على دمج العوامل البيومترية ضمن أنظمة التوثيق الحديثة بهدف تعزيز مستوى الأمان وتقليل الاعتماد على كلمات المرور التقليدية.

تشير الدراسات إلى أن استخدام العوامل البيومترية يوفّر مستوىً أعلى من الموثوقية مقارنةً بالعوامل المعرفية أو المادية، نظرًا لصعوبة تقليدها أو مشاركتها. إلا أن هذه الميزات ترافقها تحديات تتعلق بالدقة، والخصوصية، وآلية تخزين ومعالجة البيانات البيومترية. [12][13]

1.5.2 التحقق باستخدام بصمة الإصبع

تُعد بصمة الإصبع من أقدم وأكثر تقنيات التحقق البيومتري انتشارًا، وقد تناولتها العديد من الدراسات نظرًا لسهولة استخدامها ونضج تقنياتها. تعتمد هذه الأنظمة على استخراج خصائص مميّزة من نمط البصمة ومقارنتها بقيم مخزّنة مسبقا.[12]

أظهرت الدراسات أن أنظمة بصمة الإصبع تتمتع بمعدلات دقة مرتفعة، إلا أنها تواجه تحديات عملية، مثل تأثرها بجودة المستشعر، إضافةً إلى المخاوف المرتبطة بتخزين البيانات البيومترية الحساسة. كما أشارت بعض الأبحاث إلى أن ربط أنظمة التحقق ببصمة الإصبع بأجهزة مادية محددة قد يحدّ من مرونة الاستخدام في البيئات متعددة الأجهزة.

2.5.2 التحقق باستخدام التعرّف على الصوت

تناولت دراسات أخرى استخدام التعرّف على الصوت كعامل تحقق بيومتري يعتمد على الخصائص الصوتية الفريدة للمستخدم. ويتميّز هذا النوع من التحقق بإمكانية استخدامه عن بُعد ودون الحاجة إلى أجهزة استشعار متخصصة.[23]

إلا أن الأبحاث بيّنت أن أنظمة التعرّف على الصوت قد تتأثر بعوامل خارجية، مثل الضوضاء، وجودة التسجيل، والتغيّرات الصوتية الناتجة عن المرض أو التقدم في العمر. كما أظهرت بعض الدراسات وجود مخاطر أمنية محتملة، مثل هجمات إعادة التشغيل أو تقليد الصوت، مما يستدعي دمجه مع عوامل تحقق إضافية.

3.5.2 التحقق باستخدام مسح قزحية العين

يُعد التحقق باستخدام قزحية العين من أكثر تقنيات التحقق البيومتري دقةً، نظرًا لتعقيد الأنماط الفريدة التي تحتويها القزحية. وقد أشارت الدراسات إلى انخفاض معدلات الخطأ في هذا النوع من الأنظمة مقارنةً بغيره من العوامل البيومترية.

ومع ذلك، تتطلب أنظمة مسح قزحية العين تجهيزات خاصة ذات تكلفة مرتفعة، كما قد تثير مخاوف تتعلق بقبول المستخدمين وخصوصيتهم. وتشير الأبحاث إلى أن هذه العوامل تحدّ من انتشار هذه التقنية في الأنظمة التجارية واسعة الاستخدام.[24]

4.5.2 التحقق باستخدام التعرّف على الوجه

حظي التعرّف على الوجه باهتمام واسع في الدراسات الحديثة، لكونه يجمع بين سهولة الاستخدام وعدم الحاجة إلى أجهزة مادية إضافية. وتعتمد هذه الأنظمة على استخراج تمثيلات رقمية (Feature Vectors أو Face Embeddings) من صورة الوجه ومقارنتها بقيم مرجعية.

أظهرت الدراسات أن تقنيات التعرّف على الوجه شهدت تطورًا ملحوظًا مع استخدام خوارزميات التعلم العميق، مما أدى إلى تحسين معدلات الدقة وتقليل معدلات الخطأ. إلا أن الأبحاث شدّدت في الوقت نفسه على ضرورة التعامل مع بيانات الوجه بحساسية عالية، نظرًا لكونها من أكثر أنواع البيانات البيومترية ارتباطًا بالخصوصية.[13]

5.5.2 الخصوصية وأمن البيانات البيومترية

ركّزت الدراسات الحديثة بشكل متزايد على قضايا الخصوصية المرتبطة باستخدام البيانات البيومترية، وأكّدت على أهمية تجنّب تخزين البيانات البيومترية بصيغ خام، أو نقلها عبر الشبكة دون حماية كافية. كما أوصت الأبحاث باعتماد نماذج معالجة محلية وتقنيات تشفير قوية للحد من مخاطر تسريب هذه البيانات. [12][14]

تشير هذه التوجهات إلى أن نجاح أنظمة التحقق البيومتري لا يعتمد فقط على دقة الخوارزميات، بل أيضًا على البنية الأمنية المعتمدة في تخزين ومعالجة البيانات، ومدى توافقها مع مبادئ حماية الخصوصية وتقليل سطح الهجوم.

6.5.2 الخلاصة

يتبيّن من استعراض الدراسات السابقة أن العوامل البيومترية تمثّل إضافة فعّالة لأنظمة التوثيق الحديثة، لما توفّره من مستوى عالٍ من الموثوقية. إلا أن اختيار العامل البيومتري المناسب يجب أن يراعي التوازن بين الدقة، وسهولة الاستخدام، وحماية الخصوصية.

وفي هذا الإطار، تُعد تقنيات التعرّف على الوجه من أكثر الحلول ملاءمة للأنظمة متعددة الأجهزة، في حين تُظهر الدراسات أن تقنيات مثل بصمة الإصبع يمكن أن تمثّل خيارًا مناسبًا في بيئات محددة، مما يفتح المجال لإدراجها ضمن الآفاق المستقبلية لتطوير النظام المقترح.

6.2 المقارنة التحليلية بين الدراسات السابقة والمشروع المقترح

يهدف هذا القسم إلى إجراء مقارنة تحليلية شاملة بين ما قدّمته الدراسات السابقة في مجالات إدارة كلمات المرور، وبروتوكولات المصادقة، والتوثيق متعدد العوامل، والتحقق البيومتري، وبين النظام المقترح في هذا المشروع. ولا تقتصر هذه المقارنة على الجوانب الوظيفية، بل تركّز على النماذج الأمنية المعتمدة، وآليات حماية الخصوصية، ومدى تكامل الحلول المقترحة لمعالجة التهديدات الحديثة. [8][9][10][17] ووضح ذلك في جدول(3-2) .

جدول 3-2 مقارنة تحليلية بين الدراسات السابقة والمشروع المقترح

	الدراسات السابقة	المشروع المقترح
نموذج إدارة كلمات المرور	خزائن رقمية مشفّرة مع اعتماد متفاوت على الخادم	نظام متكامل بخزنة مشفّرة وبنية انعدام معرفة
آلية المصادقة	مصادقة تقليدية أو بروتوكولات غير موحّدة	SRPالقياسي (Zero-Knowledge PAKE)
إرسال كلمة المرور عبر الشبكة	غالبًا غير مرسلة، لكن دون مصادقة متبادلة صريحة	لا تُرسل نهائيًا مع مصادقة متبادلة
المصادقة المتبادلة	غير مضمونة في معظم الدراسات	مضمونة بالكامل
إدارة المفاتيح	اشتقاق مباشر من كلمة المرور أو بنى غير موثّقة	فصل مفاتيح (KEK مشتق + DEK عشوائي)
خوارزميات التشفير	AES بأنماط مختلفة / HMAC	AES-GCM (Authenticated Encryption)
التوثيق متعدد العوامل (MFA)	مدعوم في بعض الدراسات (أجهزة/OTP)	مدعوم مع عامل بيومتري
التعامل مع البيانات البيومترية	تخزين تمثيلات أو بيانات خام في بعض الحالات	لا تُخزّن خام؛ تُشفّر بعد Encoding
حماية الخصوصية	متفاوتة وتعتمد على التصميم	مرتفعة (Privacy by Design)
العمل عبر أجهزة متعددة	محدود أو مرتبط بجهاز	مدعوم دون ربط بجهاز

1.6.2 مناقشة تحليلية

تُظهر المقارنة أن الدراسات السابقة قدّمت إسهامات مهمة في تحسين أمن أنظمة إدارة كلمات المرور، خاصة من خلال اعتماد التشفير القوي والتوثيق متعدد العوامل. إلا أن معظم هذه الدراسات لم تعالج بشكل متكامل مسألة المصادقة القائمة على كلمة المرور ضمن إطار انعدام المعرفة مع مصادقة متبادلة صريحة، كما أن نماذج إدارة المفاتيح فيها غالبًا ما تفتقر إلى فصل واضح وموثّق للأدوار بين المفاتيح.

في المقابل، يتميّز المشروع المقترح باعتماده على بروتوكول SRPالقياسي، الذي يوفّر مصادقة قائمة على إثبات المعرفة الصفرية دون إرسال كلمة المرور أو مشتقاتها، ويضمن مصادقة متبادلة بين العميل والخادم. كما يقدّم المشروع بنية واضحة لإدارة المفاتيح تعتمد على فصل KEK وDEK، مما يقلّل من أثر أي اختراق محتمل ويعزّز متانة النظام الأمنية.

وعلى صعيد التوثيق متعدد العوامل، يتجاوز المشروع المقترح الحلول التقليدية من خلال دمج التحقق البيومتري المحلي ضمن بنية تحافظ على الخصوصية، حيث تتم معالجة البيانات البيومترية على جهاز المستخدم دون نقلها إلى الخادم. ويُعد هذا التوجّه متوافقًا مع توصيات الدراسات الحديثة التي تشدّد على تقليل سطح الهجوم وحماية البيانات الحساسة.

2.6.2 الفجوة البحثية وإسهام المشروع

من خلال التحليل السابق، يمكن تحديد الفجوة البحثية في غياب نظام متكامل يجمع بين:

- مصادقة قائمة على كلمة المرور وفق مبدأ انعدام المعرفة،
- إدارة مفاتيح هرمية موثّقة أكاديميًا،
- توثيق متعدد العوامل مع تحقق بيومتري يحافظ على الخصوصية،
- ودعم الوصول الآمن من أجهزة متعددة دون ربط الحساب بجهاز محدد.

يسعى المشروع المقترح إلى سدّ هذه الفجوة من خلال تصميم وتنفيذ نموذج أمني متكامل، يجمع بين هذه العناصر ضمن إطار موحّد وقابل للتطوير، مما يجعله إضافة علمية وتطبيقية في مجال أمن المعلومات وأنظمة إدارة كلمات المرور. [2][5][9][17]

3 الفصل الثالث

تصميم وتطوير النظام المقترح

1.3 تمهيد

يهدف هذا الفصل إلى عرض التصميم التفصيلي للنظام المقترح وتوضيح آليات تطويره، بالاعتماد على الأسس النظرية التي تم تناولها في الفصل الأول، والتحليل المقارن للدراسات السابقة في الفصل الثاني. وينتقل هذا الفصل من الجانب النظري والتحليلي إلى الجانب التطبيقي، من خلال شرح البنية المعمارية للنظام، وتحديد مكوّناته الرئيسة، وآليات المصادقة، وإدارة المفاتيح، والتحكم بالوصول، ضمن إطار أمني متكامل.

يركّز تصميم النظام على تحقيق مستوى عالٍ من الأمان وحماية الخصوصية، من خلال اعتماد بنية قائمة على مبدأ انعدام المعرفة(Zero-Knowledge Architecture) ، وتقليل الثقة بالخادم، وعدم نقل أو تخزين أي بيانات حساسة بصيغة مكشوفة. كما يراعي التصميم دعم الوصول الآمن من أجهزة متعددة، مع دمج التوثيق متعدد العوامل والتحقق البيومتري بطريقة تحافظ على خصوصية المستخدم ولا تزيد من سطح الهجوم.

2.3 البنية العامة للنظام

يعتمد النظام المقترح على بنية Client–Server Architecture، يتم فيها توزيع المسؤوليات الأمنية والوظيفية بشكل واضح بين طرف المستخدم (Client) والخادم(Server) . ويهدف هذا التوزيع إلى تقليل الاعتماد على الخادم ، وحصر العمليات الحساسة قدر الإمكان ضمن جهاز المستخدم.

في هذه البنية، يقوم جهاز المستخدم بتنفيذ جزء من العمليات الحرجة، مثل التحقق البيومتري وبدء عملية المصادقة، في حين يقتصر دور الخادم على إدارة الجلسات، وتنفيذ سياسات الوصول، والتعامل مع البيانات المشفّرة فقط. ويسهم هذا النهج في تقليل المخاطر الناتجة عن اختراق الخادم أو تسريب قاعدة البيانات.

1.2.3 مكوّنات النظام

يتكوّن النظام المقترح من مجموعة من المكوّنات الرئيسة التي تعمل معًا لتحقيق الوظائف المطلوبة مع الحفاظ على المتطلبات الأمنية، ويمكن تلخيص هذه المكوّنات بما يلي:

- *الواجهة الأمامية (Frontend)*

تمثّل الواجهة الأمامية نقطة التفاعل المباشر بين المستخدم والنظام، وتشمل واجهات تسجيل الدخول، إنشاء الحساب، إدارة كلمات المرور، وتنفيذ التوثيق متعدد العوامل. يتم تنفيذ التحقق البيومتري، وتحديدًا التعرّف على الوجه، محليًا على جهاز المستخدم، دون إرسال الصور أو التمثيلات البيومترية إلى الخادم، وذلك التزامًا بمبدأ حماية الخصوصية.

- *الواجهة الخلفية (Backend)*

تُعد الواجهة الخلفية مسؤولة عن تنفيذ منطق النظام، بما يشمل إدارة الجلسات، وتنفيذ بروتوكول المصادقة الآمن، والتعامل مع البيانات المشفّرة، وتطبيق سياسات التحكم بالوصول. تم تطوير هذه الواجهة باستخدام إطار العمل FastAPI، لما يوفّره من كفاءة وأداء عالٍ في بناء واجهات برمجية آمنة وقابلة للتوسّع.

- *قاعدة البيانات (Database)*

تُستخدم قاعدة البيانات لتخزين البيانات المشفّرة ، والمفاتيح المغلّفة، وسجلات الدخول. ولا يتم تخزين أي كلمة مرور أو بيانات بيومترية بصيغة خام داخل قاعدة البيانات، مما يقلّل من أثر أي اختراق محتمل.

- *وحدة إدارة المفاتيح (Key Management Module)*

تُعد وحدة إدارة المفاتيح من المكوّنات البنيوية الأساسية للنظام، حيث تتولى توليد وإدارة مفاتيح التشفير وفق بنية هرمية تعتمد على الفصل بين مفتاح تشفير المفاتيح (KEK) ومفتاح تشفير البيانات (DEK). وتضمن هذه الوحدة عدم تخزين أي مفتاح بصيغة مكشوفة، وتحقيق مبدأ انعدام المعرفة.

- *وحدة التحكم بالوصول (Access Control Module)*

تُعنى هذه الوحدة بتطبيق سياسات التحكم بالوصول المعتمدة في النظام، بما يشمل التحكم المستند إلى الدور (RBAC) والتحكم المستند إلى الصفات (ABAC). وتتيح هذه الآليات إدارة دقيقة للصلاحيات، خاصة فيما يتعلق بالحساب الإداري ومراقبة نشاط المستخدمين.

2.2.3 مبادئ التصميم المعتمدة

استند تصميم النظام إلى مجموعة من المبادئ الأمنية الأساسية التي تهدف إلى تعزيز متانة النظام وتقليل المخاطر المحتملة، ومن أبرزها:

- *انعدام المعرفة (Zero-Knowledge):*

  لا يتم إرسال كلمة المرور أو مفاتيح التشفير عبر الشبكة، ولا يمتلك الخادم معلومات تمكّنه من فك تشفير بيانات المستخدم بشكل مستقل.

- *تقليل الثقة بالخادم (Minimized Trust):*

  يقتصر دور الخادم على إدارة الجلسات وتخزين البيانات المشفّرة فقط، دون التعامل مع بيانات حساسة بصيغة مكشوفة.

- *الفصل بين المفاتيح (Key Separation):*

  استخدام مفاتيح مختلفة لأغراض مختلفة، مما يقلّل من أثر أي اختراق محتمل.

- *حماية الخصوصية منذ التصميم (Privacy by Design):*

  تنفيذ التحقق البيومتري محليًا على جهاز المستخدم، وعدم نقل البيانات البيومترية إلى الخادم.

- *المرونة وقابلية التوسّع:*

  دعم الوصول الآمن من أجهزة متعددة، مع إمكانية إضافة عوامل تحقق مستقبلية دون تعديل جوهري في بنية النظام.

3.3 آلية تسجيل المستخدم وإنشاء الحساب (User Registration Process)

تُعد آلية تسجيل المستخدم وإنشاء الحساب المرحلة الأولى في دورة حياة المستخدم داخل النظام، وتمثّل نقطة تأسيس البنية الأمنية الخاصة بكل مستخدم. لذلك، تم تصميم هذه الآلية بعناية لضمان عدم تعريض أي بيانات حساسة للخطر منذ اللحظة الأولى، مع الالتزام بمبادئ انعدام المعرفة وحماية الخصوصية.

تعتمد عملية التسجيل في النظام المقترح على فصل واضح بين التحقق من صحة المدخلات، وإعداد المفاتيح التشفيرية، وتهيئة عوامل التوثيق الإضافية، بحيث لا يتم إنشاء الحساب أو تخزين أي بيانات إلا بعد اكتمال جميع الخطوات بنجاح.

1.3.3 مرحلة إدخال بيانات التسجيل والتحقق الأولي

تبدأ عملية التسجيل بقيام المستخدم بإدخال البيانات الأساسية المطلوبة لإنشاء الحساب، والتي تشمل اسم المستخدم، البريد الإلكتروني، وكلمة المرور. ويتم في هذه المرحلة التحقق من استيفاء كلمة المرور لسياسات الأمان المعتمدة، مثل الحد الأدنى للطول، واحتوائها على أحرف كبيرة وصغيرة، وأرقام، ورموز خاصة.

يهدف هذا التحقق الأولي إلى تقليل مخاطر اختيار كلمات مرور ضعيفة، دون تخزين كلمة المرور أو إرسالها بصيغة مكشوفة إلى الخادم. وتُعد هذه الخطوة تمهيدية ولا ينتج عنها أي تخزين دائم للبيانات الحساسة.

2.3.3 توليد المفاتيح التشفيرية الخاصة بالمستخدم

بعد اجتياز مرحلة التحقق الأولي، يتم الانتقال إلى مرحلة إعداد المفاتيح التشفيرية، والتي تُعد جوهر العملية الأمنية في النظام. في هذه المرحلة:

- يتم اشتقاق مفتاح تشفير المفاتيح (Key Encryption Key – KEK) من كلمة المرور باستخدام خوارزمية اشتقاق مفاتيح قوية، مع قيمة عشوائية(Salt) باستخدام الـ Argon2.
- يتم توليد مفتاح تشفير البيانات (Data Encryption Key – DEK) بشكل عشوائي ومستقل.

يُستخدم KEK حصريًا لتغليفDEK ، بينما يُستخدم DEK لاحقًا لتشفير جميع البيانات الحساسة الخاصة بالمستخدم. ولا يتم تخزين KEK داخل النظام، في حين يُخزَّن DEK بعد تغليفه فقط، مما يمنع الوصول إليه دون امتلاك كلمة المرور الصحيحة.

3.3.3 عداد التوثيق متعدد العوامل(MFA)

بعد إعداد المفاتيح التشفيرية، يُطلب من المستخدم تفعيل التوثيق متعدد العوامل بوصفه جزءًا إلزاميًا من عملية التسجيل. وفي هذا المشروع، يعتمد النظام على دمج كلمة المرور مع عامل بيومتري، حيث يُتاح للمستخدم اختيار تفعيل التحقق باستخدام التعرّف على الوجه.

يتم تنفيذ عملية التحقق البيومتري محليًا على جهاز المستخدم، حيث تُعالج بيانات الوجه وتُحوّل إلى تمثيل رقمي، ثم تُشفّر باستخدام مفتاح DEK قبل أي عملية تخزين. ولا يتم إرسال الصور الخام أو التمثيلات البيومترية غير المشفّرة إلى الخادم، التزامًا بمبدأ حماية الخصوصية.

4.3.3 انشاء الحساب وتخزين البيانات المشفّرة

بعد اكتمال جميع الخطوات السابقة بنجاح، يتم إنشاء حساب المستخدم بشكل نهائي. في هذه المرحلة، يقوم النظام بتخزين:

- بيانات المستخدم غير الحساسة (مثل اسم المستخدم والبريد الإلكتروني).
- مفتاح DEK بعد تغليفه باستخدامKEK .
- البيانات البيومترية بعد تشفيرها.
- إعدادات التوثيق والصلاحيات الافتراضية.

ولا يتم في أي مرحلة تخزين كلمة المرور بصيغة صريحة أو قابلة للاسترجاع، كما لا يتم تخزين أي بيانات بيومترية بصيغتها الخام، مما يضمن مستوىً عاليًا من الأمان منذ لحظة إنشاء الحساب.

5.3.3 الخصائص الأمنية لآلية التسجيل

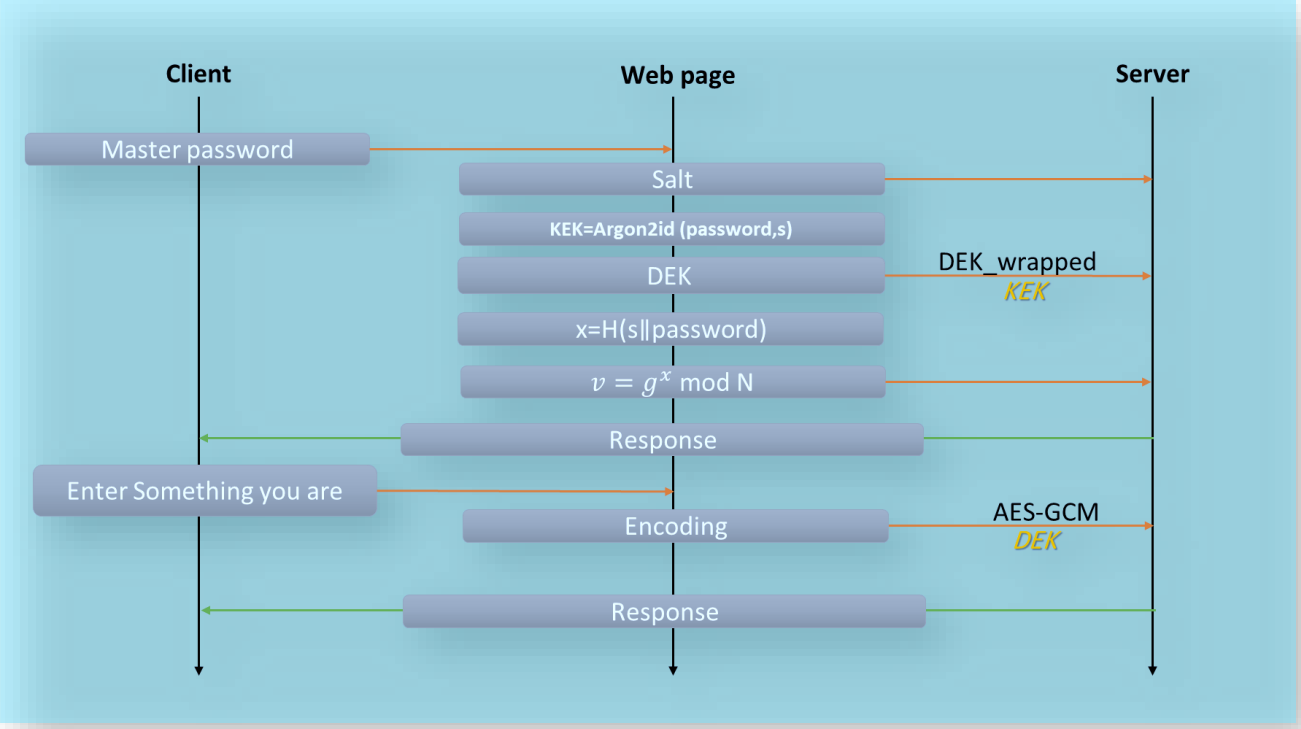
تتميّز آلية تسجيل المستخدم في النظام المقترح بعدد من الخصائص الأمنية المهمة، من أبرزها:

- عدم إرسال كلمة المرور أو تخزينها بصيغة مكشوفة.
- توليد مفاتيح تشفير مستقلة لكل مستخدم.
- فصل واضح بين مفاتيح التشفير وأدوارها.
- تفعيل التوثيق متعدد العوامل كجزء من عملية التسجيل.
- تنفيذ التحقق البيومتري محليًا للحفاظ على الخصوصية.

تُسهم هذه الخصائص في بناء أساس أمني قوي لكل حساب مستخدم، وتمنع استغلال الحسابات الجديدة كنقطة ضعف في النظام.

6.3.3 مخطط تسلسل عملية التسجيل

يوضّح الشكل (3-1) التسلسل العام لعملية تسجيل المستخدم وإنشاء الحساب في النظام المقترح.



شكل رقم 3-1 مخطط تسلسل عملية التسجيل

4.3 آلية تسجيل الدخول والتحقق من الهوية(Authentication Process)

تُعد آلية تسجيل الدخول والتحقق من الهوية المرحلة الأكثر حساسية في النظام، إذ تمثّل البوابة التي تسبق الوصول إلى البيانات المشفّرة والموارد المحمية. لذلك، تم تصميم هذه الآلية بحيث توفّر مصادقة قوية قائمة على مبدأ انعدام المعرفة، وتمنع إرسال كلمة المرور أو أي معلومات حساسة عبر الشبكة، مع دمج التوثيق متعدد العوامل لتعزيز مستوى الأمان.

تعتمد عملية تسجيل الدخول في النظام المقترح على تسلسل واضح من الخطوات، يبدأ بالمصادقة القائمة على كلمة المرور باستخدام بروتوكولSRP ، وينتهي بالتحقق البيومتري بوصفه عامل تحقق إضافي، قبل السماح بالوصول إلى الحساب.

1.4.3 المصادقة القائمة على كلمة المرور باستخدامSRP

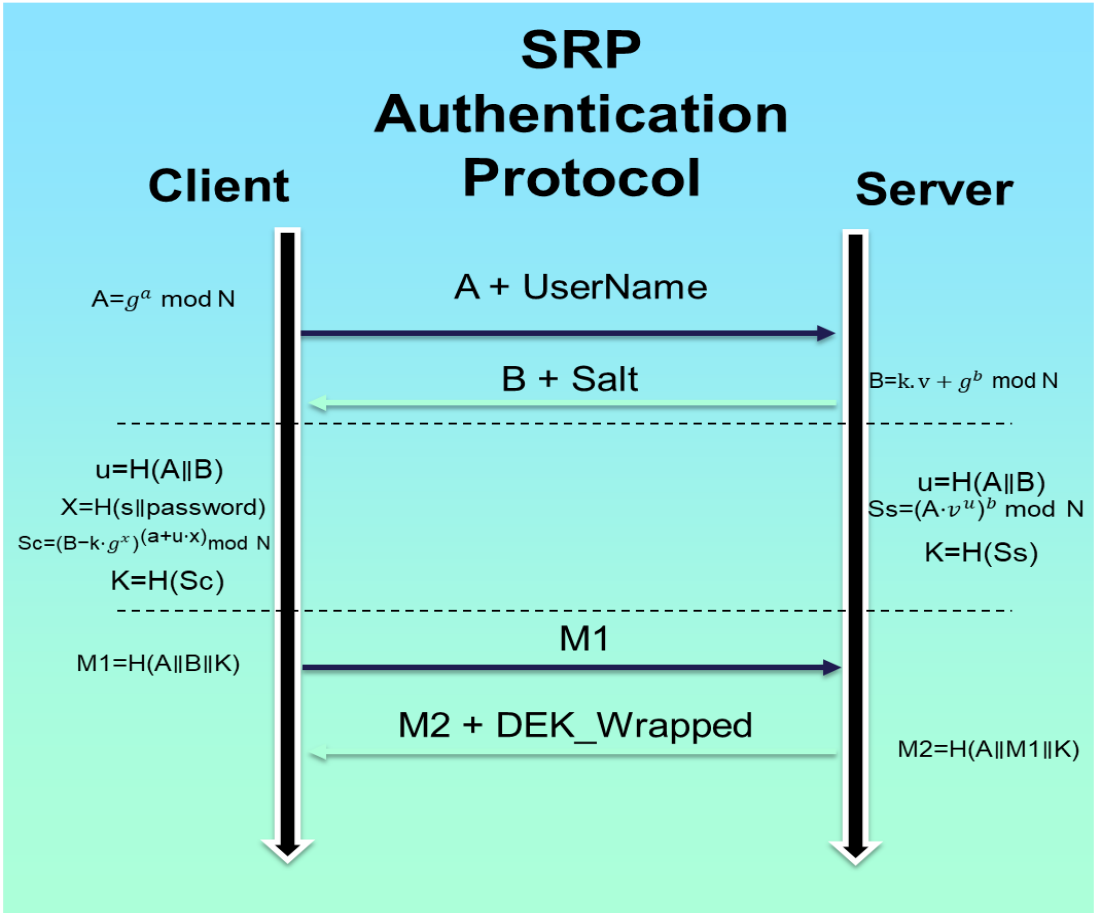
تبدأ عملية تسجيل الدخول بقيام المستخدم بإدخال اسم المستخدم وكلمة المرور. إلا أن كلمة المرور لا تُرسل إلى الخادم في أي مرحلة من مراحل المصادقة. بدلًا من ذلك، يتم استخدام

بروتوكول **(Secure Remote Password Protocol) SRP** لإجراء عملية مصادقة قائمة على إثبات المعرفة الصفرية.

خلال هذه المرحلة، يتم تبادل مجموعة من القيم الحسابية بين العميل والخادم، تمكّن الطرفين من التحقق المتبادل من امتلاك كلمة المرور الصحيحة، دون كشفها أو إرسال أي مشتقات مباشرة قابلة للاستغلال. وتؤدي هذه الآلية إلى إنشاء سياق مصادقة آمن يُستخدم لاحقًا لاستكمال بقية خطوات التحقق.

تضمن هذه المرحلة مقاومة فعّالة لهجمات الرجل في المنتصف وهجمات إعادة التشغيل، كما تمنع استغلال البيانات المتبادلة لإجراء هجمات تخمين غير متصل.

كما هو موضح بالشكل (2-3) تحقق باستخدام بروتوكول SRP



شكل رقم 2-3 تحقق باستخدام بروتوكول SRP

2.4.3 اشتقاق المفاتيح بعد المصادقة الناجحة

بعد نجاح المصادقة باستخدامSRP ، يتم الانتقال إلى مرحلة اشتقاق المفاتيح التشفيرية الخاصة بالمستخدم. في هذه المرحلة:

- يتم اشتقاق مفتاح تشفير المفاتيح (KEK) اعتمادًا على كلمة المرور وقيمة ال Salt، باستخدام الـ Argon2، ضمن بيئة آمنة، دون تخزينه داخل النظام.
- يُستخدم KEK لفك تغليف مفتاح تشفير البيانات (DEK) المخزّن في قاعدة البيانات بصيغة مشفّرة.

ولا يتم تنفيذ أي عملية فك تشفير للبيانات الحساسة قبل اجتياز هذه المرحلة بنجاح، مما يضمن أن الوصول إلى البيانات مرتبط ارتباطًا مباشرًا بالمصادقة الصحيحة.

3.4.3 التوثيق متعدد العوامل والتحقق البيومتري

بعد التحقق من صحة كلمة المرور واشتقاق المفاتيح اللازمة، يُطلب من المستخدم استكمال عملية تسجيل الدخول من خلال التوثيق متعدد العوامل. وفي هذا المشروع، يعتمد النظام على عامل بيومتري إضافي يتمثل في التعرّف على الوجه.

يتم تنفيذ عملية التحقق البيومتري محليًا على جهاز المستخدم، حيث تُلتقط صورة الوجه ثم تُقارن بالقيم المرجعية بعد فك تشفيرها باستخدام مفتاحDEK. ولا يتم إرسال الصورة أو التمثيلات البيومترية إلى الخادم، بل يقتصر دور النظام على استقبال نتيجة التحقق (نجاح أو فشل).

يسهم هذا النهج في حماية الخصوصية وتقليل سطح الهجوم، مع ضمان أن امتلاك كلمة المرور وحده غير كافٍ للوصول إلى الحساب.

4.4.3 إنشاء الجلسة وتطبيق سياسات الوصول

في حال نجاح جميع مراحل التحقق، يقوم النظام بإنشاء جلسة مستخدم آمنة، ويتم تطبيق سياسات التحكم بالوصول المعتمدة، مثل التحكم المستند إلى الدور (RBAC) والتحكم المستند إلى الصفات (ABAC). وبناءً على هذه السياسات، يُسمح للمستخدم بالوصول إلى الوظائف والموارد المصرّح بها فقط.

أما في حال فشل أي مرحلة من مراحل التحقق، سواء كانت المصادقة بكلمة المرور أو التحقق البيومتري، فيتم رفض عملية تسجيل الدخول دون الكشف عن أي معلومات إضافية قد تفيد المهاجم.

5.3 إدارة المفاتيح والتشفير في النظام

تُعد إدارة المفاتيح والتشفير الركيزة الأساسية لحماية البيانات الحساسة في النظام المقترح، إذ يرتبط أمن كلمات المرور المُدارة والبيانات البيومترية مباشرةً بكيفية توليد المفاتيح، واستخدامها، وحمايتها من الوصول غير المصرّح به. لذلك، اعتمد النظام بنية تشفير متقدمة قائمة على الفصل بين المفاتيح، وتكامل محكم مع آلية المصادقة، بما يضمن تحقيق مبدأ انعدام المعرفة وحماية الخصوصية.

1.5.3 بنية إدارة المفاتيح المعتمدة(KEK / DEK)

يعتمد النظام على بنية هرمية لإدارة المفاتيح (Key Hierarchy) تقوم على الفصل الوظيفي بين نوعين من المفاتيح:

- *مفتاح تشفير المفاتيح(Key Encryption Key – KEK):*
  مفتاح مشتق من كلمة مرور المستخدم باستخدام خوارزمية اشتقاق قوية، ويُستخدم حصريًا لتغليف وفك تغليف مفتاحDEK . لا يتم تخزين KEK داخل النظام.

- *مفتاح تشفير البيانات(Data Encryption Key – DEK):*
  مفتاح عشوائي يُنشأ لكل مستخدم، ويُستخدم لتشفير البيانات الحساسة فقط، مثل كلمات المرور المُدارة والتمثيلات الرقمية للبيانات البيومترية. يُخزَّن DEK بعد تغليفه باستخدام.KEK

يسهم هذا الفصل الواضح في تقليل أثر أي اختراق محتمل، إذ لا يؤدّي الوصول إلى قاعدة البيانات وحده إلى كشف البيانات المشفّرة دون امتلاك كلمة المرور الصحيحة وتنفيذ المصادقة كاملة.

2.5.3 اشتقاق مفتاح KEK باستخدامArgon2id

يتم اشتقاق مفتاح KEK من كلمة مرور المستخدم باستخدام خوارزمية Argon2id، وهي خوارزمية حديثة موصى بها لمهام اشتقاق المفاتيح من كلمات المرور. تعتمد عملية الاشتقاق على دمج كلمة المرور مع قيمة عشوائية(Salt) ، مما يزيد من مقاومة الهجمات المعتمدة على التخمين أو الجداول الجاهزة.

يوفّر هذا النهج الخصائص التالية:

- عدم تخزين KEK داخل النظام.
- توليد KEK ديناميكيًا بعد المصادقة الناجحة.
- رفع الكلفة الحسابية للهجمات المعتمدة على العتاد المتخصص.

وبذلك، لا يمكن استنتاج KEK أو إعادة توليده دون امتلاك كلمة المرور الصحيحة، حتى في حال تسريب قاعدة البيانات.

3.5.3 تشفير البيانات باستخدامAES-GCM

يعتمد النظام على خوارزمية AES-GCM (Advanced Encryption Standard – Galois/Counter Mode)لتشفير البيانات الحساسة باستخدام مفتاحDEK. ويُعد هذا النمط من أنماط التشفير الموثّق، إذ يوفّر في آنٍ واحد:

- **السرية(Confidentiality) :** لمنع الاطلاع غير المصرّح به،
- **السلامة(Integrity) :** للكشف عن أي تعديل غير مصرح به،
- **التحقق(Authentication) :** لضمان صحة البيانات المشفّرة.

يسهم اختيار AES-GCM في تقليل تعقيد التنفيذ مقارنةً باستخدام AES مع آليات تحقق منفصلة، ويحدّ من احتمالية الأخطاء البرمجية، مع الحفاظ على أداء مرتفع مناسب للأنظمة الحديثة.

4.5.3 تكامل إدارة المفاتيح مع آلية المصادقة

تتكامل إدارة المفاتيح في النظام المقترح بشكل مباشر مع آلية تسجيل الدخول والتحقق من الهوية. إذ لا يتم اشتقاق KEK أو فك تغليف DEK إلا بعد نجاح المصادقة القائمة على كلمة المرور باستخدام بروتوكولSRP ، واستكمال التوثيق متعدد العوامل.

يضمن هذا التكامل أن الوصول إلى البيانات المشفّرة مرتبط ارتباطًا وثيقًا بهوية المستخدم المصادَق عليها، ويمنع أي محاولة لفك تشفير البيانات خارج سياق جلسة مصادقة صحيحة.

5.5.3 الخصائص الأمنية لبنية التشفير

تتميّز بنية إدارة المفاتيح والتشفير في النظام المقترح بعدد من الخصائص الأمنية الجوهرية، من أبرزها:

- عدم تخزين أي مفتاح تشفير بصيغة مكشوفة.
- فصل واضح بين مفاتيح التشفير وأدوارها.
- حماية البيانات حتى في حال اختراق قاعدة البيانات.
- دعم مبدأ انعدام المعرفة وتقليل الثقة بالخادم.
- قابلية التوسّع لإضافة آليات تشفير أو مفاتيح مستقبلية.

وبذلك، تشكّل إدارة المفاتيح والتشفير الأساس الذي تُبنى عليه بقية طبقات الحماية في النظام، وتُعد عنصرًا حاسمًا في تحقيق الأهداف الأمنية للمشروع.

6.3 التوثيق متعدد العوامل والتحقق البيومتري

يُعد التوثيق متعدد العوامل (MFA) طبقة أمان إضافية تهدف إلى تعزيز عملية التحقق من هوية المستخدم من خلال دمج أكثر من عامل تحقق مستقل، بحيث لا يكون امتلاك كلمة المرور وحده كافيًا للوصول إلى النظام. وقد تم دمج MFA في النظام المقترح بوصفه آلية تحقق مكمّلة لمرحلة المصادقة الأساسية، بما ينسجم مع متطلبات الأمان العالية لأنظمة إدارة كلمات المرور.

يعتمد النظام على الجمع بين عامل معرفي (كلمة المرور) وعامل بيومتري (التعرّف على الوجه)، مع تنفيذ التحقق البيومتري محليًا على جهاز المستخدم، حفاظًا على الخصوصية وتقليل سطح الهجوم.

1.6.3 دور التوثيق متعدد العوامل ضمن النظام

في سياق هذا المشروع، يأتي التوثيق متعدد العوامل بعد إتمام المصادقة القائمة على كلمة المرور باستخدام بروتوكولSRP ، وقبل السماح بالوصول النهائي إلى البيانات المشفّرة. ويهدف هذا الترتيب إلى ضمان أن المستخدم الذي اجتاز المصادقة يمتلك أيضًا خاصية فيزيائية فريدة تؤكّد هويته. يتميّز هذا الدمج بما يلي:

- تقليل مخاطر اختراق الحسابات في حال تسريب كلمة المرور.
- منع الوصول غير المصرّح به حتى مع امتلاك بيانات الاعتماد الأساسية.
- تعزيز مقاومة النظام لهجمات التصيّد وهجمات القوة الغاشمة.

2.6.3 آلية التحقق باستخدام التعرّف على الوجه

يعتمد النظام المقترح على التعرّف على الوجه بوصفه العامل البيومتري المطبّق فعليًا. وتتم عملية التحقق وفق تسلسل يحافظ على الخصوصية ويمنع نقل البيانات الحساسة عبر الشبكة، على النحو الآتي:

- تنفيذ عملية التعرّف على الوجه محليًا داخل متصفح المستخدم باستخدام نماذج مخصّصة.
- استخراج تمثيل رقمي للوجه (Face Encoding) بدلًا من تخزين الصورة الخام.
- تشفير التمثيل الرقمي باستخدام مفتاحDEK .
- مقارنة التمثيل الناتج بالقيمة المرجعية بعد فك تشفيرها محليًا.
- إرسال نتيجة التحقق فقط (نجاح/فشل) إلى الخادم.

ولا يتم في أي مرحلة إرسال الصورة الخام أو التمثيل البيومتري غير المشفّر إلى الخادم، مما ينسجم مع مبادئ Privacy by Designو Zero-Knowledge Architecture.

3.6.3 التعامل مع البيانات البيومترية وحماية الخصوصية

نظرًا لحساسية البيانات البيومترية، تم اعتماد مجموعة من الضوابط الصارمة للتعامل معها داخل النظام، من أبرزها:

- عدم تخزين أي بيانات بيومترية بصيغتها الخام(Raw Data) .

- تشفير التمثيلات الرقمية باستخدام خوارزمية تشفير موثّقة.
- ربط الوصول إلى البيانات البيومترية بفك تغليف مفتاح DEK بعد مصادقة ناجحة.
- منع الخادم من الاطلاع على البيانات البيومترية أو معالجتها.

تسهم هذه الضوابط في تقليل المخاطر المرتبطة بتسريب البيانات البيومترية، وتضمن أن أي اختراق للخادم لا يؤدي إلى كشف معلومات حساسة عن المستخدمين.

4.6.3 الآفاق المستقبلية للتحقق البيومتري

تشير الدراسات إلى إمكانية دمج عوامل بيومترية إضافية، مثل بصمة الإصبع أو التعرّف على الصوت، ضمن أنظمة التوثيق متعدد العوامل. وفي هذا الإطار، يمكن اعتبار إضافة بصمة الإصبع أحد الآفاق المستقبلية لتطوير النظام المقترح، دون الحاجة إلى تعديل جوهري في بنيته المعمارية، نظرًا لاعتماد التحقق البيومتري كآلية مستقلة وقابلة للتوسّع.

5.6.3 خلاصة القسم

يبيّن هذا القسم أن التوثيق متعدد العوامل يشكّل طبقة حماية أساسية في النظام المقترح، من خلال الجمع بين المصادقة القائمة على كلمة المرور والتحقق البيومتري المحلي. ويسهم هذا الدمج في تعزيز متانة النظام الأمنية، مع الحفاظ على خصوصية المستخدم وعدم زيادة الاعتماد على الخادم، مما يجعل التحقق البيومتري عنصرًا داعمًا للأمان دون التأثير على بنية النظام الأساسية.

7.3 التحكم بالوصول وإدارة الصلاحيات(Access Control: RBAC / ABAC)

يُعد التحكم بالوصول أحد العناصر الجوهرية في تصميم الأنظمة الآمنة، إذ يحدّد من يحق له الوصول إلى الموارد والوظائف المختلفة داخل النظام، وتحت أي شروط. وفي أنظمة إدارة كلمات المرور على وجه الخصوص، تكتسب إدارة الصلاحيات أهمية مضاعفة نظرًا لحساسية البيانات المُدارة وخطورة إساءة استخدامها.

اعتمد النظام المقترح على دمج نموذجين للتحكم بالوصول، هما التحكم المستند إلى الدور (Role-Based Access Control – RBAC) والتحكم المستند إلى الصفات

(Attribute-Based Access Control – ABAC) ، بهدف تحقيق توازن بين البساطة الإدارية والدقة الأمنية.

1.7.3 التحكم المستند إلى الدور(RBAC)

يعتمد نموذج RBAC على إسناد الصلاحيات إلى أدوار (Roles) محدّدة، ومن ثم إسناد هذه الأدوار إلى المستخدمين. وبهذا الشكل، لا يتم منح الصلاحيات مباشرةً لكل مستخدم، بل تُدار على مستوى الأدوار، مما يسهل عملية الإدارة ويقلّل من احتمالية الأخطاء.

في النظام المقترح، تم تعريف مجموعة من الأدوار الأساسية، من أبرزها:

- المستخدم العادي(User) : يمتلك صلاحيات إدارة خزنة كلمات المرور الخاصة به، مثل إضافة كلمات مرور جديدة، تعديلها، أو حذفها.
- المستخدم الإداري(Admin) : يمتلك صلاحيات إضافية تشمل إدارة المستخدمين، مراقبة سجلات الدخول، وتعطيل أو تقييد الحسابات المشبوهة.

يوفّر هذا النموذج وضوحًا في توزيع الصلاحيات، ويُعد مناسبًا للمهام العامة والمتكررة التي لا تتطلب شروطًا سياقية معقّدة.

2.7.3 التحكم المستند إلى الصفات(ABAC)

على الرغم من بساطةRBAC ، إلا أنه قد يكون غير كافٍ في بعض السيناريوهات التي تتطلب قرارات وصول أكثر ديناميكية. لذلك، تم دعم النظام بنموذج ABAC، الذي يعتمد على تقييم مجموعة من الصفات (Attributes) قبل السماح بالوصول. تشمل هذه الصفات، على سبيل المثال:

- صفات المستخدم (مثل حالة الحساب أو مستوى الثقة).
- صفات المورد المطلوب الوصول إليه.
- صفات السياق (مثل وقت الطلب أو حالة الجلسة).

يسمح ABAC باتخاذ قرارات وصول دقيقة تعتمد على سياق الاستخدام، مما يعزّز من مرونة النظام وقدرته على التعامل مع سيناريوهات أمنية متقدمة، مثل تقييد بعض العمليات الحساسة بشروط إضافية.

3.7.3 تكامل RBAC و ABACفي النظام المقترح

يعتمد النظام المقترح على دمج RBAC و ABACضمن إطار موحّد لإدارة الصلاحيات. ففي هذا الإطار:

- يُستخدم RBACلتحديد الصلاحيات الأساسية المرتبطة بدور المستخدم.
- يُستخدم ABACلتقييد أو توسيع هذه الصلاحيات بناءً على صفات وسياقات محدّدة.

يتيح هذا التكامل الجمع بين سهولة الإدارة التي يوفّرهاRBAC ، والدقة والمرونة التي يقدّمها ABAC، دون زيادة التعقيد غير الضروري في تصميم النظام.

4.7.3 دور التحكم بالوصول في حماية النظام

يسهم تطبيق آليات التحكم بالوصول في النظام المقترح في تحقيق عدد من الأهداف الأمنية، من أبرزها:

- منع الوصول غير المصرّح به إلى الموارد الحساسة.
- تقليل الأثر المحتمل لاختراق حساب مستخدم محدود الصلاحيات.
- تمكين الإدارة من الاستجابة السريعة للحوادث الأمنية عبر تعطيل الحسابات أو تقييد الصلاحيات.

وبذلك، يُعد التحكم بالوصول وإدارة الصلاحيات طبقة حماية أساسية تُكمّل آليات المصادقة والتشفير، وتُسهم في بناء نظام متكامل قادر على مواجهة التهديدات الأمنية الحديثة.

8.3 سيناريوهات الاستخدام الأساسية(Core Use Cases)

يهدف هذا القسم إلى عرض سيناريوهات الاستخدام الأساسية للنظام المقترح، بهدف توضيح كيفية تفاعل المستخدمين مع وظائف النظام المختلفة ضمن إطار أمني متكامل. تُستخدم سيناريوهات الاستخدام بوصفها أداة تحليلية تُسهّل فهم المتطلبات الوظيفية، وتربط التصميم المعماري بالعمليات الفعلية التي ينفّذها المستخدم.

تركّز السيناريوهات المعروضة على الوظائف الجوهرية التي تمثّل دورة الاستخدام الكاملة لنظام إدارة كلمات المرور، بدءًا من إنشاء الحساب وحتى إدارة البيانات والخروج الآمن من النظام.

1.8.3 سيناريو إنشاء حساب مستخدم جديد

الوصف:

يمثّل هذا السيناريو الخطوة الأولى في استخدام النظام، حيث يقوم المستخدم بإنشاء حساب جديد وإعداد البنية الأمنية الخاصة به.

التسلسل العام:

1. إدخال بيانات التسجيل الأساسية.
2. التحقق من سياسات كلمة المرور.
3. توليد مفاتيح التشفير الخاصة بالمستخدم.
4. تفعيل التوثيق متعدد العوامل.
5. تخزين البيانات المشفّرة وإنشاء الحساب.

الهدف الأمني:

ضمان إنشاء حساب آمن دون تخزين أو نقل بيانات حساسة بصيغة مكشوفة.

2.8.3 سيناريو تسجيل الدخول والتحقق من الهوية

الوصف:

يُستخدم هذا السيناريو للوصول إلى الحساب بعد إنشائه، ويجمع بين المصادقة القائمة على كلمة المرور والتوثيق متعدد العوامل.

التسلسل العام:

1. إدخال اسم المستخدم وكلمة المرور.
2. تنفيذ المصادقة باستخدام بروتوكول آمن.
3. اشتقاق المفاتيح وفك تغليفها.
4. تنفيذ التحقق البيومتري.

5. إنشاء جلسة مستخدم وتطبيق سياسات الوصول.

الهدف الأمني:

منع الوصول غير المصرّح به حتى في حال تسريب كلمة المرور.

3.8.3 سيناريو إضافة كلمة مرور جديدة إلى الخزنة

الوصف:

يتيح هذا السيناريو للمستخدم إضافة بيانات اعتماد جديدة إلى خزنة كلمات المرور الخاصة به.

التسلسل العام:

1. إدخال اسم الموقع واسم المستخدم.
2. اختيار توليد كلمة مرور عشوائية أو إدخالها يدويًا.
3. تشفير البيانات باستخدام مفتاح التشفير الخاص بالمستخدم.
4. تخزين البيانات المشفّرة في قاعدة البيانات.

الهدف الوظيفي:

تمكين المستخدم من إدارة كلمات المرور دون الحاجة إلى حفظها يدويًا.

4.8.3 سيناريو توليد كلمة مرور عشوائية

الوصف:

يُستخدم هذا السيناريو لتوليد كلمات مرور قوية وفق معايير يحدّدها المستخدم.

التسلسل العام:

1. تحديد طول كلمة المرور.
2. اختيار أنواع المحارف المسموح بها.
3. توليد كلمة المرور وعرضها للمستخدم.

4. حفظها بشكل مشفّر عند الطلب.

الهدف الأمني:

تعزيز ممارسات إنشاء كلمات مرور قوية وتقليل الاعتماد على كلمات مرور ضعيفة أو متكررة.

5.8.3 سيناريو تسجيل الخروج وإنهاء الجلسة

الوصف:

يُمكّن هذا السيناريو المستخدم من إنهاء جلسته بشكل آمن.

التسلسل العام:

1. طلب تسجيل الخروج.
2. إنهاء الجلسة الحالية.
3. حذف البيانات المؤقتة من الذاكرة.
4. إعادة المستخدم إلى واجهة تسجيل الدخول.

الهدف الأمني:

منع إساءة استخدام الجلسة في حال ترك الجهاز دون مراقبة.

6.8.3 سيناريوهات المستخدم الإداري

الوصف:

يوفّر النظام سيناريوهات استخدام خاصة بالحساب الإداري.

أمثلة:

- عرض قائمة المستخدمين المسجّلين.
- تعطيل أو تقييد حسابات مشبوهة.

- الاطلاع على سجلات الدخول والنشاطات.

الهدف الأمني:

تمكين الإدارة من مراقبة النظام والاستجابة للحوادث الأمنية.

9.3 اعتبارات الأمان والخصوصية(Security and Privacy Considerations)

يُعد تضمين اعتبارات الأمان والخصوصية عنصرًا محوريًا في تصميم النظام المقترح، نظرًا لحساسية البيانات التي يتعامل معها، والتي تشمل بيانات اعتماد المستخدمين والبيانات البيومترية. وقد تم اعتماد نهج أمني متكامل يهدف إلى تقليل المخاطر المحتملة، وحماية خصوصية المستخدم، وضمان سلامة البيانات في جميع مراحل الاستخدام.

1.9.3 مبدأ انعدام المعرفة وتقليل الثقة بالخادم

يعتمد النظام على بنية انعدام المعرفة(Zero-Knowledge Architecture) ، حيث لا يمتلك الخادم أي معلومات تمكّنه من الاطلاع على بيانات المستخدم الحساسة أو فك تشفيرها بشكل مستقل. فلا يتم إرسال كلمة المرور أو تخزينها بصيغة قابلة للاسترجاع، كما لا يتم تخزين مفاتيح التشفير الأساسية داخل النظام.

يسهم هذا النهج في تقليل الثقة بالخادم إلى الحد الأدنى، ويحدّ من الأثر الأمني في حال تعرّض الخادم أو قاعدة البيانات للاختراق، إذ تبقى البيانات المشفّرة غير قابلة للاستخدام دون المصادقة الصحيحة من طرف المستخدم.

2.9.3 حماية البيانات المخزّنة والمُنقولة

تم اعتماد خوارزميات تشفير موثّقة ومعتمدة لحماية البيانات المخزّنة والمُنقولة داخل النظام. تُشفَّر جميع البيانات الحساسة باستخدام مفاتيح خاصة بكل مستخدم، ولا يتم فك تشفيرها إلا ضمن جلسة مصادقة صحيحة.

كما يتم تأمين الاتصال بين الواجهة الأمامية والخلفية باستخدام قنوات اتصال مشفّرة، مما يمنع اعتراض البيانات أو التلاعب بها أثناء النقل. ويُعد هذا الإجراء ضروريًا لحماية النظام من هجمات التنصّت وهجمات الرجل في المنتصف.

3.9.3 حماية الخصوصية في التحقق البيومتري

نظرًا للطبيعة الحساسة للبيانات البيومترية، تم تصميم آلية التحقق البيومتري بما يراعي الخصوصية منذ المراحل الأولى للتصميم. إذ يتم تنفيذ التعرّف على الوجه محليًا على جهاز المستخدم، دون إرسال الصور أو التمثيلات البيومترية إلى الخادم.

ولا يتم تخزين أي بيانات بيومترية بصيغتها الخام، بل تُحوَّل إلى تمثيلات رقمية تُشفَّر قبل التخزين. وبذلك، يقتصر دور الخادم على استقبال نتيجة التحقق فقط، مما يقلّل من المخاطر المرتبطة بتسريب البيانات البيومترية ويعزّز ثقة المستخدم بالنظام.

4.9.3 مبدأ الحد الأدنى من الصلاحيات

يطبّق النظام مبدأ الحد الأدنى من الصلاحيات (Principle of Least Privilege) من خلال آليات التحكم بالوصول المعتمدة. إذ يُمنح كل مستخدم الصلاحيات اللازمة فقط لتنفيذ مهامه، دون تجاوز غير مبرّر.

يسهم هذا المبدأ في تقليل الأضرار المحتملة في حال اختراق حساب مستخدم، ويحدّ من انتشار الأثر داخل النظام، خاصة عند دمجه مع نماذج التحكم المستند إلى الدور والصفات.

5.9.3 مقاومة الهجمات الشائعة

تم تصميم النظام ليكون مقاومًا لعدد من الهجمات السيبرانية الشائعة، من أبرزها:

- **هجمات القوة الغاشمة:**

  من خلال عدم الاعتماد على كلمة المرور وحدها ودمج التوثيق متعدد العوامل.

- **هجمات التصيّد :**

  عبر منع استخدام كلمة المرور مباشرةً في عملية المصادقة.

- **هجمات الرجل في المنتصف :**

  باستخدام بروتوكولات مصادقة وتشفير آمنة.

- **اختراق قواعد البيانات :**

  بفضل تخزين البيانات والمفاتيح بصيغ مشفّرة وغير قابلة للاستغلال المباشر.

6.9.3 خلاصة القسم

يُظهر هذا القسم أن النظام المقترح لا يكتفي بتطبيق خوارزميات تشفير قوية، بل يعتمد رؤية شاملة للأمان والخصوصية تبدأ من التصميم المعماري وتمتد إلى جميع مراحل الاستخدام.
ويُسهم هذا النهج في بناء نظام إدارة كلمات مرور يتمتع بدرجة عالية من المتانة الأمنية، ويواكب متطلبات حماية الخصوصية في الأنظمة الرقمية الحديثة.

10.3 خاتمة

تناول هذا الفصل تصميم وتطوير النظام المقترح لإدارة كلمات المرور، مع التركيز على البنية المعمارية والآليات الأمنية التي يعتمدها النظام لضمان حماية بيانات المستخدمين وخصوصيتهم. وقد تم عرض المكوّنات الرئيسة للنظام وتوضيح أدوارها، إلى جانب شرح آليات تسجيل المستخدم، وتسجيل الدخول، وإدارة المفاتيح، والتوثيق متعدد العوامل، والتحكم بالوصول، ضمن إطار أمني متكامل.

أظهر الفصل كيف تم توظيف بروتوكولات مصادقة حديثة وبنية تشفير هرمية قائمة على الفصل بين المفاتيح، بما يحقق مبدأ انعدام المعرفة ويقلّل من الثقة بالخادم. كما تم إبراز دور التحقق البيومتري المحلي في تعزيز الأمان مع الحفاظ على الخصوصية، دون التأثير على مرونة النظام أو قابليته للتوسّع.

وبذلك، يوفّر هذا الفصل الأساس النظري والتقني الذي يُبنى عليه الجانب العملي للنظام. وفي الفصل التالي، سيتم الانتقال إلى عرض التطبيق العملي للنظام وواجهاته، مع توضيح كيفية ترجمة هذا التصميم إلى نظام فعلي قابل للاستخدام والتقييم.

4 الفصل الرابع

التطبيق العملي وعرض الواجهات

1.4 تمهيد

يهدف هذا الفصل إلى عرض التطبيق العملي للنظام المقترح لإدارة كلمات المرور، وبيان كيفية ترجمة التصميم المعماري والآليات الأمنية التي تم تناولها في الفصل الثالث إلى نظام فعلي قابل للاستخدام. كما يتناول الفصل النتائج العملية التي تم التوصل إليها بعد تنفيذ النظام، مع تحليل مدى تحقيقه للأهداف الوظيفية والأمنية المحددة مسبقًا.

يركّز هذا الفصل على الجوانب التطبيقية للنظام، بما يشمل بيئة التطوير، وتنفيذ الواجهة الخلفية والواجهة الأمامية، وآليات المصادقة والتوثيق متعدد العوامل، والتحكم بالوصول. كما يتم توثيق واجهات المستخدم المختلفة باستخدام لقطات شاشة توضيحية، بهدف إظهار تسلسل الاستخدام وتوضيح كيفية تفاعل المستخدم مع النظام في بيئة واقعية.

2.4 البيئة التطوير والأدوات المستخدمة

تم تطوير النظام المقترح لإدارة كلمات المرور باستخدام مجموعة من الأدوات والتقنيات البرمجية الحديثة التي تلبّي متطلبات الأمان العالي، وقابلية التوسّع، وسهولة الصيانة. وقد تم اختيار بيئة التطوير بعناية لتكون متوافقة مع طبيعة النظام الحسّاسة، خاصةً فيما يتعلق بالمصادقة، وإدارة المفاتيح، وحماية الخصوصية.

1.2.4 لغة البرمجة

تم اعتماد لغة Pythonفي تطوير الواجهة الخلفية للنظام، لما تتمتع به من مرونة وبساطة في الصياغة، إضافةً إلى دعمها الواسع لمكتبات التشفير وبروتوكولات الأمان. كما تُعد Python خيارًا مناسبًا لتطوير الأنظمة التي تتطلب موثوقية عالية وسرعة في التطوير دون التضحية بالجودة.

2.2.4 إطار العمل المستخدم

تم استخدام إطار العمل FastAPIبوصفه الإطار الرئيسي لتطوير الواجهة الخلفية للنظام. ويعود اختيار FastAPI إلى عدد من المزايا، من أبرزها:

- الأداء العالي في معالجة الطلبات.
- دعم بناء واجهات برمجية RESTful بطريقة منظمة.

- سهولة دمج آليات التوثيق، إدارة الجلسات، والتحقق من الصلاحيات.
- وضوح البنية البرمجية وقابليتها للتوسّع.

يسهم FastAPI في بناء واجهة خلفية واضحة تفصل بين منطق الأعمال، والأمن، والتعامل مع البيانات.

3.2.4 قاعدة البيانات

تم استخدام MySQL كنظام لإدارة قواعد البيانات، حيث تُستخدم لتخزين البيانات الضرورية للنظام بصيغة مشفّرة فقط. وتشمل هذه البيانات:

- معلومات المستخدمين غير الحساسة.
- القيم اللازمة لبروتوكول المصادقة (Salt وVerifier).
- مفاتيح التشفير بعد تغليفها.
- بيانات الخزنة الرقمية.
- سجلات الدخول والأحداث الأمنية.

وقد تم اختيار MySQL لما توفّره من استقرار واعتمادية عالية، إضافةً إلى سهولة تكاملها مع تطبيقات الويب.

4.2.4 تقنيات الواجهة الأمامية

تم تطوير الواجهة الأمامية باستخدام تقنيات الويب القياسية، وهي:

- **HTML:** لبناء هيكل الصفحات.
- **CSS:** لتنسيق الواجهات وتحسين تجربة المستخدم.
- **JavaScript**: لتنفيذ التفاعل الديناميكي بين المستخدم والنظام.

كما تم استخدام مكتبات JavaScript متخصصة لتنفيذ التحقق البيومتري محليًا داخل المتصفح (Client-side)، دون إرسال الصور أو التمثيلات البيومترية إلى الخادم. ولا يشارك الخادم في أي مرحلة من مراحل المعالجة أو المقارنة البيومترية، وذلك التزامًا بمبدأ حماية الخصوصية وتقليل الثقة بالخادم.

5.2.4 أدوات ومكتبات داعمة

إضافةً إلى ما سبق، تم الاستعانة بعدد من الأدوات والمكتبات الداعمة لتنفيذ وظائف النظام، مثل:

- مكتبات التشفير لتنفيذ خوارزميات AES-GCM واشتقاق المفاتيح.
- أدوات لإدارة الجلسات والتحكم في الوصول.
- بيئة تطوير مناسبة لاختبار النظام والتحقق من صحته.

وقد تم اختيار هذه الأدوات بعناية لتكون متوافقة مع متطلبات الأمان العالي، وداعمة لبروتوكولات المصادقة الآمنة، مع تجنّب الاعتماد على أدوات تتطلب معالجة بيانات حساسة خارج بيئة النظام.

3.4 تنفيذ الواجهة الخلفية(Backend Implementation)

تُشكّل الواجهة الخلفية النواة الأساسية للنظام المقترح، إذ تتولى تنفيذ منطق المصادقة، وإدارة المفاتيح، والتعامل مع البيانات المشفّرة، وتطبيق سياسات التحكم بالوصول. وقد تم تنفيذ الواجهة الخلفية بما ينسجم مع التصميم المعماري الموضّح في الفصل الثالث، مع الالتزام الصارم بمبادئ انعدام المعرفة وحماية الخصوصية.

1.3.4 البنية البرمجية للواجهة الخلفية

تم تنظيم الواجهة الخلفية باستخدام بنية طبقية واضحة تعتمد على الفصل المنطقي بين المسؤوليات، وتشمل بشكل عام:

- **طبقةRoutes :** لمعالجة طلبات واجهة البرمجة.(API Endpoints)
- **طبقةModels :** لتمثيل الكيانات والارتباط مع قاعدة البيانات.
- **طبقةDatabase :** لإدارة الاتصال بقاعدة البيانات والجلسات.
- **طبقةSecurity :** لتنفيذ المصادقة، التشفير، وإدارة المفاتيح.
- **طبقةServices / Helpers :** لاحتواء المنطق المساعد ومنطق الأعمال.

يساعد هذا التنظيم في تحسين قابلية الصيانة، وتسهيل التوسّع، وعزل المنطق الأمني عن بقية أجزاء النظام.

2.3.4 تنفيذ المصادقة باستخدام بروتوكولSRP

تم تنفيذ المصادقة في الواجهة الخلفية باستخدام بروتوكول SRP (Secure Remote Password Protocol) بشكل كامل بين العميل والخادم. يقتصر دور الخادم في هذا السياق على:

- تخزين قيم Salt وVerifier فقط.
- المشاركة في التبادل الحسابي اللازم لإتمام المصادقة.
- التحقق من صحة عملية المصادقة دون استلام كلمة المرور أو أي مشتقات مباشرة عنها.

ويتم استخدام SRP ليس فقط عند تسجيل الدخول، بل أيضًا عند تنفيذ عمليات حساسة مثل تغيير كلمة المرور، وذلك للتحقق من صحة كلمة المرور القديمة قبل إعادة تغليف مفتاح التشفير.

3.3.4 تنفيذ إدارة المفاتيح(KEK / DEK)

تعتمد الواجهة الخلفية على بنية إدارة مفاتيح هرمية دون امتلاك أي مفتاح تشفير بصيغة مكشوفة. في هذا الإطار:

- يتم اشتقاق KEK محليًا على جهاز المستخدم اعتمادًا على كلمة المرور.
- لا يعرف الخادم قيمة KEK ولا يقوم بتخزينها.
- يتعامل الخادم فقط مع DEK بعد تغليفه.

يُولَّد DEK مرة واحدة عند إنشاء الحساب، ولا يُعاد توليده عند تغيير كلمة المرور، بل يتم فقط إعادة تغليفه باستخدام KEK جديد، مما يحافظ على استمرارية البيانات المشفّرة دون الحاجة لإعادة تشفيرها.

4.3.4 التشفير والتخزين الآمن

يتم استخدام خوارزمية AES-GCM حصريًا لتشفير البيانات الحساسة، وتشمل:

- عناصر الخزنة الرقمية (كلمات المرور المخزنة).
- التمثيلات الرقمية للبيانات البيومترية بعد معالجتها.

يوفّر هذا الأسلوب حماية متكاملة للسرية والسلامة، ويمنع أي تعديل غير مصرح به على البيانات المخزّنة.

5.3.4 إدارة الجلسات

بعد إتمام المصادقة باستخدام SRP والتحقق البيومتري، تقوم الواجهة الخلفية بإنشاء Session IDمخصّص لإدارة جلسة المستخدم. ولا يتم إنشاء الجلسة إلا بعد نجاح جميع مراحل التحقق، مما يضمن تطبيق مفهوم التوثيق متعدد العوامل بشكل كامل.

يتم التحقق من الجلسة عند كل طلب حساس، ويتم رفض أي طلب غير مرتبط بجلسة صالحة.

6.3.4 تنفيذ التحكم بالوصول(RBAC / ABAC)

تم دمج آليات التحكم بالوصول ضمن الواجهة الخلفية للتحقق من صلاحيات المستخدم عند كل طلب يتعلّق بموارد حساسة. ويتم تحديد دور المستخدم (مثل Admin أو User) من خلال حقل صريح في قاعدة البيانات، مع تطبيق شروط إضافية عند الحاجة باستخدام نموذج التحكم المستند إلى الصفات.

7.3.4 تسجيل الأحداث والمراقبة

تتولى الواجهة الخلفية تسجيل الأحداث الأمنية المهمة، مثل:

- محاولات تسجيل الدخول.
- عمليات الدخول الإدارية.
- تعطيل أو تفعيل حسابات المستخدمين.
- تغييرات الصلاحيات.

وتُستخدم هذه السجلات لأغراض المراقبة والتدقيق، مع إتاحتها للحساب الإداري ضمن واجهة مخصصة.

8.3.4 حدود ودور الواجهة الخلفية

لا تشارك الواجهة الخلفية في أي مرحلة من مراحل التحقق البيومتري، ولا تستقبل صورًا أو تمثيلات بيومترية. ويقتصر دورها على استقبال نتيجة التحقق فقط، مما يحقّق مبدأ Privacy by Design وZero-Knowledge تجاه البيانات البيومترية.

9.3.4 الخلاصة

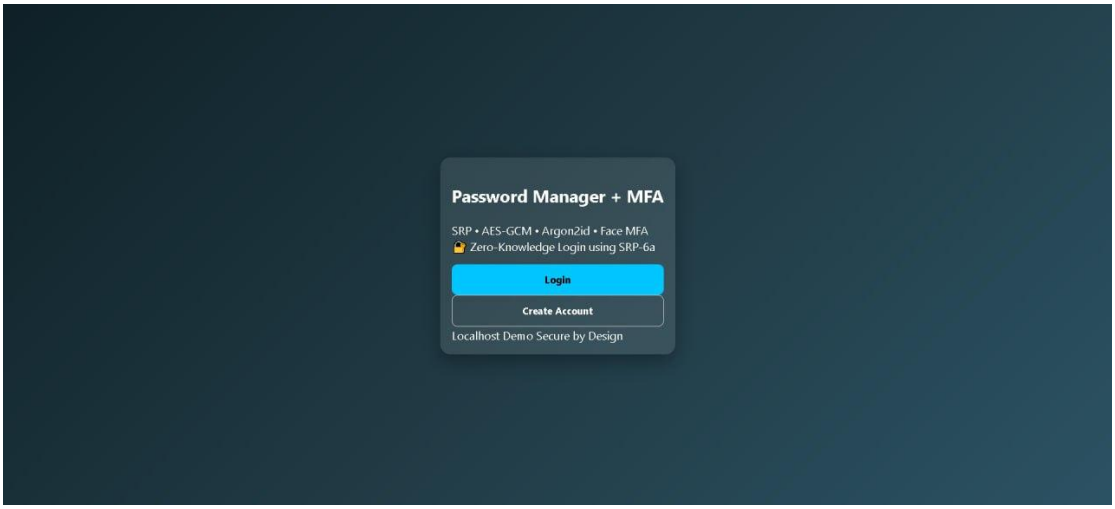
يوضّح هذا القسم كيف تم تنفيذ الواجهة الخلفية للنظام المقترح بطريقة تعكس التصميم الأمني والمعماري المعتمد، مع الالتزام الصارم بحماية الخصوصية وعدم تخزين أو معالجة أي بيانات حساسة بصيغة مكشوفة. ويشكّل هذا التنفيذ الأساس الذي تُبنى عليه الواجهة الأمامية والتفاعل العملي مع المستخدم، كما سيتم عرضه في القسم التالي.

4.4 تنفيذ الواجهة الأمامية(Frontend Implementation)

تهدف الواجهة الأمامية للنظام إلى توفير تجربة استخدام آمنة وسلسة، تمكّن المستخدم من التفاعل مع النظام وتنفيذ العمليات المختلفة دون تعقيد، مع الحفاظ على أعلى مستوى من الأمان. وقد تم تصميم الواجهات بما يتوافق مع تسلسل الاستخدام المنطقي للنظام، بدءًا من تسجيل الدخول أو إنشاء الحساب، وصولًا إلى إدارة كلمات المرور والوظائف الإدارية.

1.4.4 الواجهة الرئيسية للنظام (واجهة البداية)

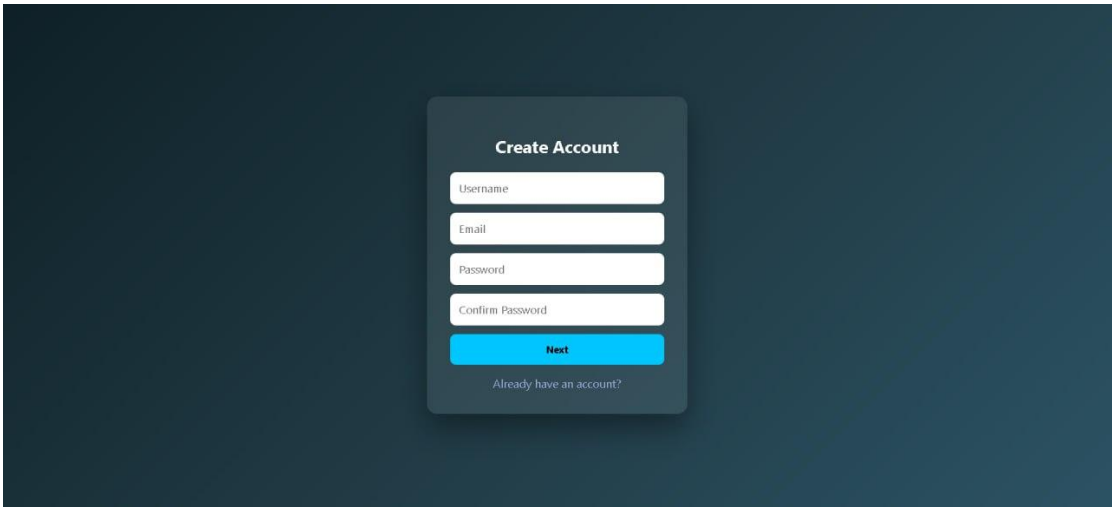
تُعد الواجهة الرئيسية نقطة الدخول الأولى للنظام، حيث تُقدَّم للمستخدم خيارات تسجيل الدخول أو إنشاء حساب جديد. كما توضّح هذه الواجهة بشكل مختصر التقنيات الأمنية المعتمدة في النظام، مثل بروتوكول SRP والتشفير باستخدام AES-GCM والتوثيق متعدد العوامل.



صورة رقم 4-1 واجهة البداية

2.4.4 واجهة إنشاء حساب جديد

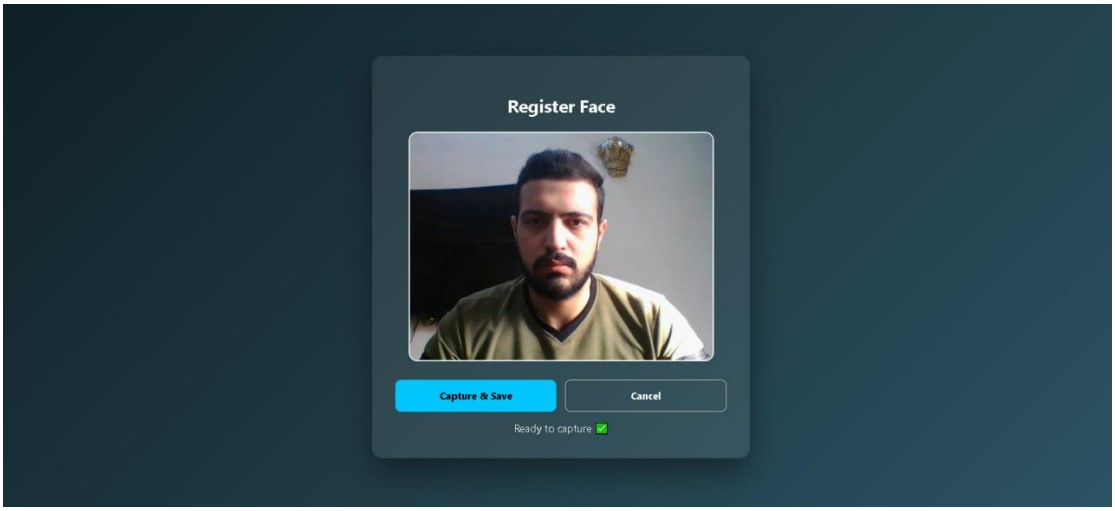
تتيح هذه الواجهة للمستخدم إدخال بياناته الأساسية، والتي تشمل اسم المستخدم، البريد الإلكتروني، وكلمة المرور، مع التأكد من مطابقة كلمة المرور لمتطلبات القوة الأمنية قبل الانتقال إلى الخطوة التالية. تم تصميم هذه الواجهة للتحقق المبدئي من صحة المدخلات قبل بدء عملية التسجيل البيومتري.



صورة رقم 4-2 واجهة إنشاء حساب جديد

3.4.4 واجهة تسجيل بصمة الوجه

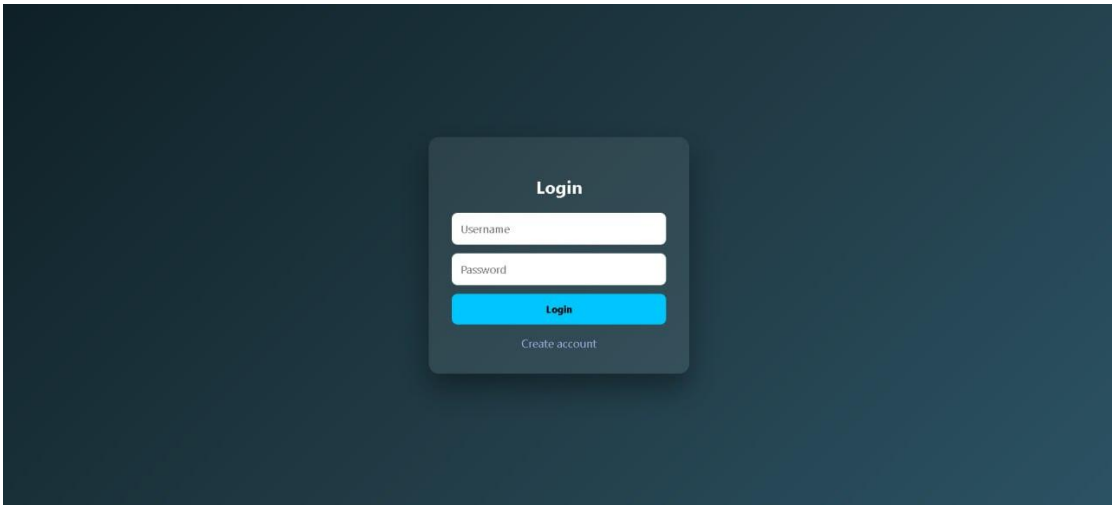
في هذه المرحلة، يتم تسجيل بصمة الوجه الخاصة بالمستخدم باستخدام كاميرا الجهاز. تتم عملية التعرّف ومعالجة الصورة محليًا داخل المتصفح، حيث يتم استخراج التمثيل الرقمي للوجه (Face Encoding) دون إرسال الصورة أو البيانات الخام إلى الخادم، التزامًا بمبدأ حماية الخصوصية.



صورة رقم 4-3 واجهة تسجيل بصمة الوجه أثناء إنشاء الحساب.

4.4.4 واجهة تسجيل الدخول

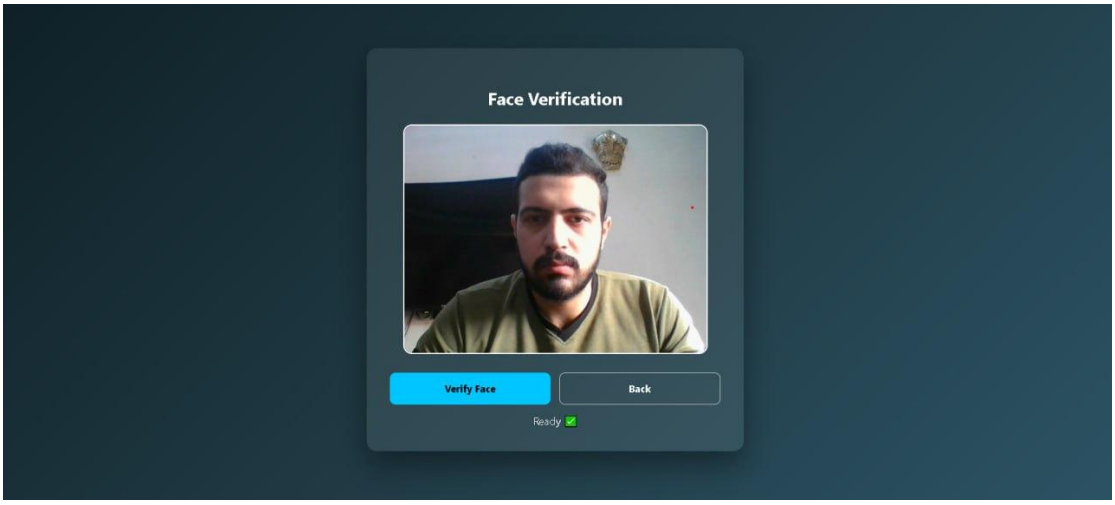
تُستخدم هذه الواجهة لإدخال اسم المستخدم وكلمة المرور. بعد إدخال البيانات، يتم تنفيذ بروتوكول SRPللتحقق من صحة كلمة المرور دون إرسالها إلى الخادم، قبل الانتقال إلى مرحلة التحقق البيومتري.



صورة رقم 4-4 واجهة تسجيل الدخول

5.4.4 واجهة التحقق من الوجه

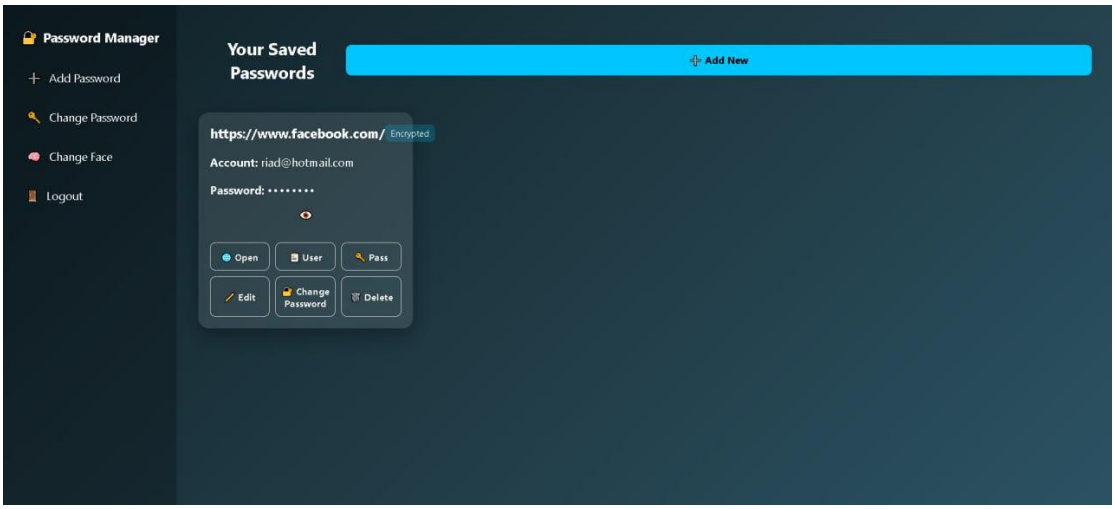
بعد نجاح التحقق من كلمة المرور، يتم الانتقال إلى واجهة التحقق البيومتري، حيث يُطلب من المستخدم التحقق من هويته باستخدام بصمة الوجه المسجّلة مسبقًا. تتم عملية المقارنة محليًا داخل المتصفح، ويُسمح بالوصول إلى النظام فقط في حال نجاح التحقق.



صورة رقم 4-5 واجهة التحقق من الوجه

6.4.4 الواجهة الرئيسية للمستخدم(Dashboard)

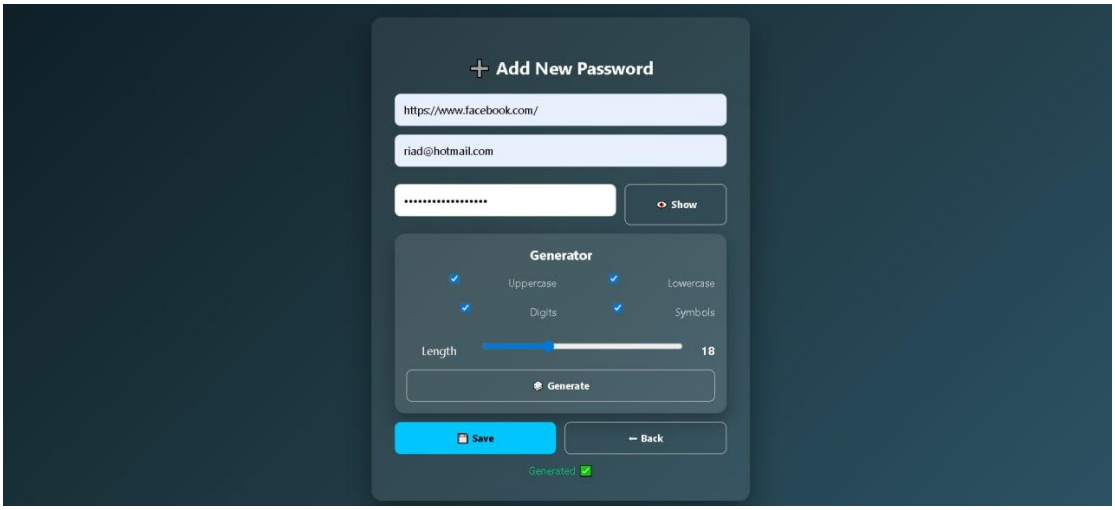
بعد إتمام جميع مراحل التحقق بنجاح، يتم توجيه المستخدم إلى الواجهة الرئيسية، حيث يمكنه عرض كلمات المرور المخزّنة، وإضافة عناصر جديدة، أو تنفيذ عمليات التعديل والحذف. كما تتضمن القائمة الجانبية خيارات إدارة الحساب.



صورة رقم 4-6 الواجهة الرئيسية للمستخدم وعرض كلمات المرور المخزّنة.

7.4.4 واجهة إضافة بطاقة جديدة

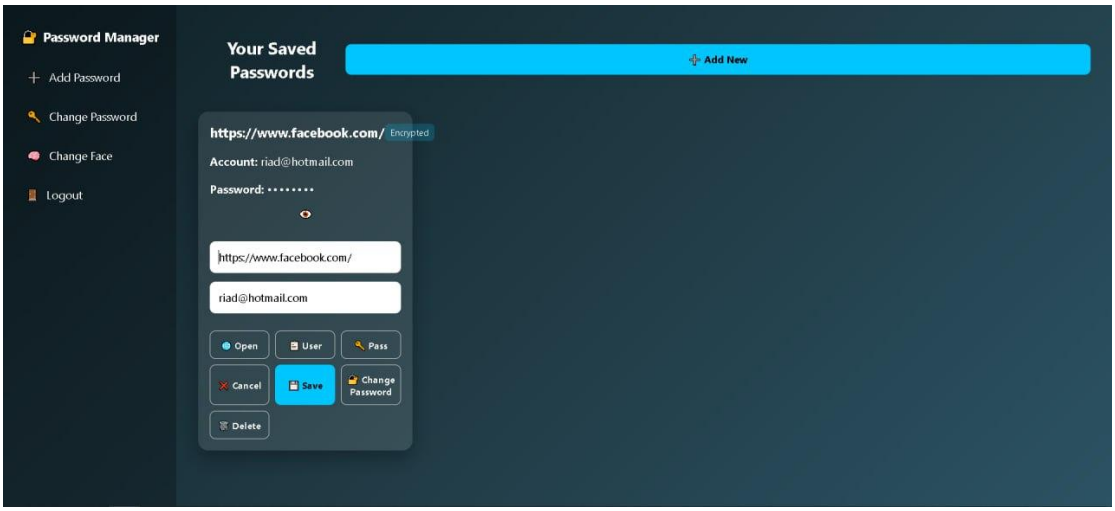
تتيح هذه الواجهة للمستخدم إضافة بيانات تسجيل دخول جديدة، مع إمكانية توليد كلمة مرور عشوائية قوية من خلال مولّد كلمات المرور المدمج، والذي يسمح بتحديد نوع الأحرف وطول الكلمة.



صورة رقم 4-7 واجهة إضافة بطاقة جديدة مع مولّد كلمات المرور.

8.4.4 واجهة إدارة بطاقات كلمات المرور

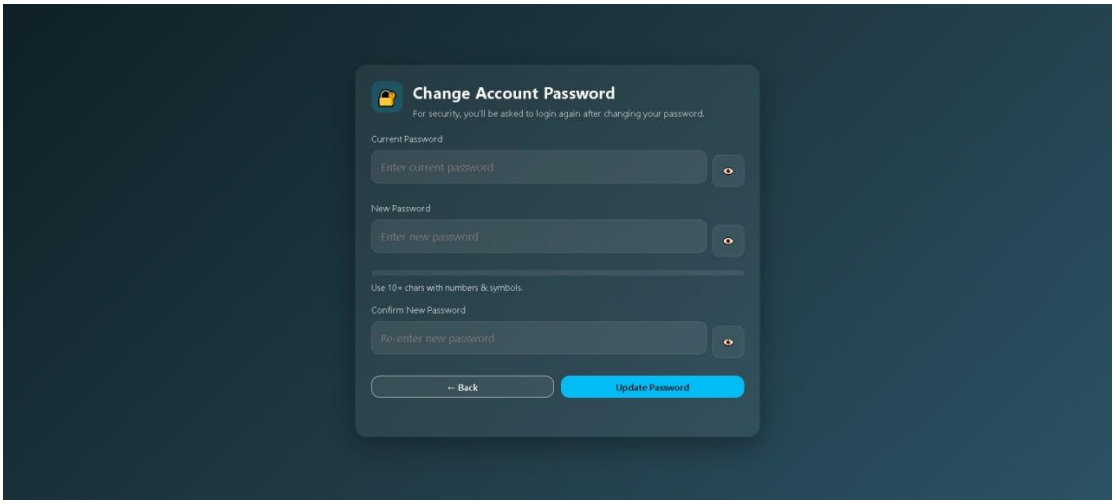
تمكّن هذه الواجهة المستخدم من عرض تفاصيل كل بطاقة كلمة مرور، مع تنفيذ عمليات مثل التعديل، الحذف، أو تغيير كلمة المرور المرتبطة بالخدمة، مع الحفاظ على تشفير البيانات في جميع المراحل.



صورة رقم 8-4 واجهة عرض وتعديل بطاقات كلمات المرور.

9.4.4 واجهة تغيير كلمة مرور الحساب

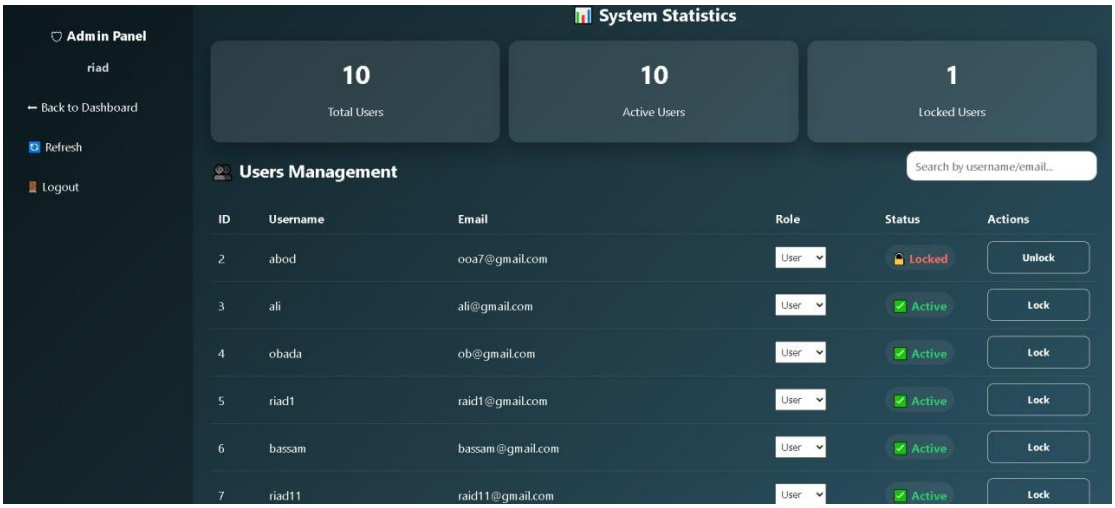
تتيح هذه الواجهة للمستخدم تغيير كلمة المرور الرئيسية للحساب، مع التحقق من كلمة المرور الحالية قبل اعتماد التغيير. وتؤدي هذه العملية إلى إعادة تغليف مفتاح DEK باستخدام KEK جديد دون إعادة تشفير البيانات المخزّنة.



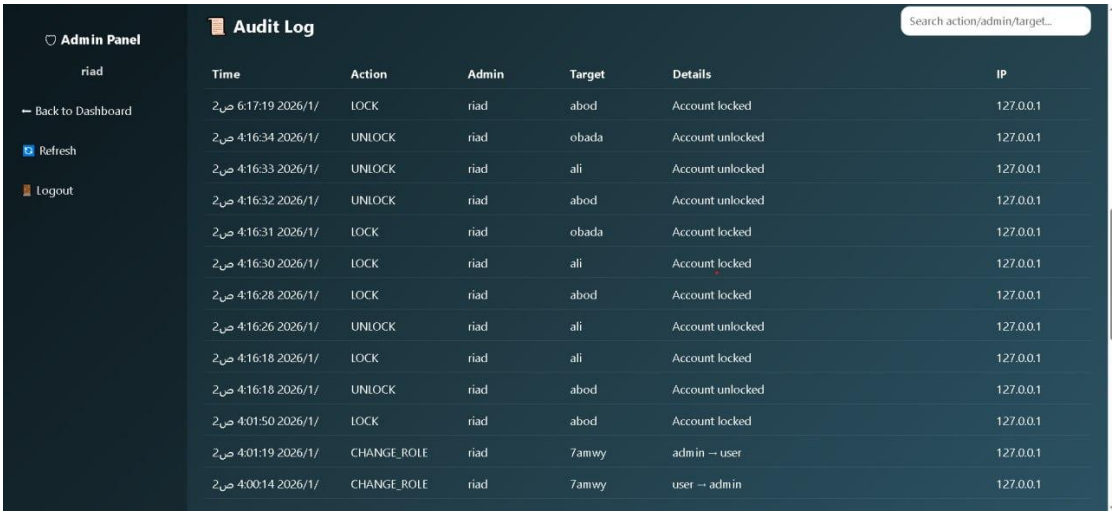
صورة رقم 9-4 واجهة تغيير كلمة مرور الحساب الرئيسي.

10.4.4 واجهة الإدارة(Admin Panel)

تظهر واجهة الإدارة فقط للمستخدمين الذين يمتلكون دور المدير (Admin)، حيث تتيح إدارة حسابات المستخدمين، قفل أو فتح الحسابات، تغيير الأدوار، إضافةً إلى عرض إحصاءات النظام وسجلات التدقيق (Audit Logs).



صورة رقم 10-4 واجهة الإدارة وإدارة المستخدمين.



صورة رقم 11-4 واجهة سجلات التدقيق.

11.4.4 الخلاصة

يُظهر هذا القسم كيفية تنفيذ الواجهة الأمامية للنظام بطريقة تعكس التصميم الأمني المعتمد، مع ضمان تجربة استخدام واضحة ومتدرجة، ودعم كامل للتوثيق متعدد العوامل، وحماية الخصوصية. وتُبرز الواجهات المعروضة التكامل بين سهولة الاستخدام والآليات الأمنية المتقدمة، مما يؤكد نجاح تحويل التصميم النظري إلى نظام عملي متكامل.

5.4 تنفيذ التوثيق متعدد العوامل عمليًا(Practical Implementation of MFA)

يُعد التوثيق متعدد العوامل (Multi-Factor Authentication – MFA) أحد الركائز الأساسية في النظام المقترح، حيث تم تنفيذه عمليًا بهدف تعزيز مستوى الأمان ومنع الوصول غير المصرّح به حتى في حال تسريب بيانات الاعتماد الأساسية. وقد تم اعتماد نموذج يجمع بين عاملين مستقلين للتحقق من هوية المستخدم، هما كلمة المرور والعامل البيومتري، ضمن تسلسل تحقّق صارم ومتكامل.

1.5.4 نموذج التوثيق المعتمد في النظام

يعتمد النظام على نموذج توثيق ثنائي العوامل يتكوّن من:

- **شيء يعرفه المستخدم :**كلمة المرور.
- **شيء يُمثّل المستخدم :**بصمة الوجه(Face Authentication) .

وقد تم اختيار هذا النموذج لتحقيق توازن فعّال بين الأمان العالي وسهولة الاستخدام، مع تجنّب الاعتماد على عوامل خارجية قد تؤثر على تجربة المستخدم أو تتطلب بنى تحتية إضافية.

2.5.4 التسلسل العملي لتنفيذMFA

يتم تنفيذ التوثيق متعدد العوامل وفق تسلسل منطقي محدّد، كما يلي:

1. **إدخال بيانات تسجيل الدخول:**

   يقوم المستخدم بإدخال اسم المستخدم وكلمة المرور عبر واجهة تسجيل الدخول.

2. **التحقق من كلمة المرور باستخدام:SRP**

   يتم تنفيذ بروتوكول SRP بين المتصفح والخادم للتحقق من صحة كلمة المرور دون إرسالها أو تخزينها بصيغة صريحة، مما يضمن المصادقة الآمنة القائمة على مبدأ انعدام المعرفة.

3. **الانتقال إلى التحقق البيومتري:**

   في حال نجاح التحقق من كلمة المرور، لا يتم إنشاء جلسة مستخدم مباشرة، بل يتم توجيه المستخدم إلى مرحلة التحقق البيومتري.

4. **التحقق من بصمة الوجه محليًا:**

يتم تشغيل كاميرا الجهاز، واستخراج التمثيل الرقمي للوجه (Face Encoding) داخل المتصفح، ثم مقارنته مع التمثيل المخزّن محليًا بعد فك تشفيره باستخدام مفتاحDEK .

5. **إنشاء الجلسة بعد نجاح العاملين:**

لا يتم إنشاء Session ID إلا بعد نجاح كلا العاملين، مما يضمن تطبيق مفهوم التوثيق متعدد العوامل بشكل كامل.

3.5.4 تنفيذ التحقق البيومتري ضمنMFA

تم تنفيذ التحقق البيومتري باستخدام بصمة الوجه فقط، مع الالتزام بالمعايير التالية:

- لا يتم إرسال صورة الوجه أو التمثيل الرقمي إلى الخادم.
- تتم جميع عمليات المعالجة والمقارنة محليًا داخل المتصفح.
- الخادم يستقبل فقط نتيجة التحقق (نجاح أو فشل).

يسهم هذا الأسلوب في تقليل سطح الهجوم، ومنع تسريب البيانات البيومترية، وتحقيق مبدأ Privacy by Designضمن نظام التوثيق متعدد العوامل.

4.5.4 معالجة حالات الفشل والأمان

في حال فشل أي مرحلة من مراحل التوثيق:

- يتم إيقاف عملية تسجيل الدخول فورًا.
- لا يتم إنشاء جلسة مستخدم.

يساعد هذا النهج في اكتشاف محاولات الدخول غير المصرّح بها.

5.5.4 الخلاصة

يُظهر هذا القسم كيفية تنفيذ التوثيق متعدد العوامل عمليًا ضمن النظام المقترح، مع دمج فعلي بين بروتوكول مصادقة آمن والعامل البيومتري، ضمن تسلسل تحقّق صارم. وقد أسهم هذا التنفيذ في رفع مستوى الأمان، وتقليل الاعتماد على كلمة المرور وحدها، وضمان عدم الوصول إلى البيانات المشفّرة إلا بعد التحقق الكامل من هوية المستخدم.

6.4 تنفيذ التحكم بالوصول وإدارة الصلاحيات(RBAC / ABAC)

يُعد التحكم بالوصول وإدارة الصلاحيات من العناصر الأساسية في تصميم الأنظمة الآمنة، خاصةً في الأنظمة التي تتعامل مع بيانات حساسة مثل أنظمة إدارة كلمات المرور. وقد تم في هذا المشروع تنفيذ نموذج تحكم متكامل يجمع بين التحكم المستند إلى الدور (Role-Based Access Control – RBAC) والتحكم المستند إلى الصفات (Attribute-Based Access Control – ABAC) ، بهدف تحقيق مرونة عالية ودقة في تحديد الصلاحيات.

1.6.4 نموذج التحكم بالوصول المعتمد

يعتمد النظام على دمج نموذجين للتحكم بالوصول:

- **التحكم المستند إلى الدور(RBAC) :**

  يتم تحديد الصلاحيات الأساسية للمستخدم بناءً على الدور المعيّن له داخل النظام، مثل دور المستخدم العادي (User) أو دور المدير(Admin) .

- **التحكم المستند إلى الصفات(ABAC) :**

  يتم تطبيق شروط إضافية تعتمد على صفات معينة، مثل حالة الحساب (نشط أو مقفول)، أو نوع العملية المطلوبة، قبل السماح بتنفيذها.

يسمح هذا الدمج بتوفير مستوى أعلى من الأمان مقارنة بالاعتماد على نموذج واحد فقط.

2.6.4 تنفيذ RBAC عمليًا

تم تنفيذ التحكم المستند إلى الدور من خلال:

- تعريف حقل صريح للدور (Role) داخل قاعدة البيانات.
- التحقق من دور المستخدم عند كل طلب يتعلّق بوظائف حساسة.
- تقييد الوصول إلى واجهة الإدارة والوظائف الإدارية بالمستخدمين الذين يمتلكون دور المدير فقط.

يُظهر هذا النهج بوضوح الفصل بين صلاحيات المستخدمين العاديين وصلاحيات الإدارة، ويمنع إساءة استخدام الصلاحيات.

3.6.4 تنفيذ ABAC عمليًا

إلى جانبRBAC ، تم تطبيق نموذج ABAC للتحكم الدقيق في الوصول، حيث يتم التحقق من مجموعة من الصفات قبل تنفيذ بعض العمليات، ومن أبرزها:

- حالة الحساب(Active / Locked) .
- نوع العملية المطلوبة (قراءة، تعديل، حذف).
- سياق الطلب (واجهة مستخدم عادية أو واجهة إدارية).

يؤدي هذا الأسلوب إلى منع تنفيذ العمليات حتى في حال امتلاك المستخدم للدور المناسب، إذا لم تتحقق الشروط الإضافية المطلوبة.

4.6.4 واجهة الإدارة(Admin Panel)

تُعد واجهة الإدارة جزءًا عمليًا من تنفيذ التحكم بالوصول، حيث تظهر فقط للمستخدمين الذين يمتلكون دور المدير. وتوفّر هذه الواجهة مجموعة من الوظائف الإدارية، من أبرزها:

- عرض قائمة المستخدمين المسجّلين.
- قفل أو فتح حسابات المستخدمين.
- تغيير أدوار المستخدمين.
- عرض إحصاءات عامة عن النظام.
- الاطلاع على سجلات التدقيق.(Audit Logs)

تُسهم هذه الواجهة في تمكين الإدارة من مراقبة النظام والتدخل عند الحاجة، دون التأثير على تجربة المستخدم العادي.

5.6.4 تسجيل العمليات الإدارية وسجلات التدقيق

تم ربط جميع العمليات الإدارية بسجلات تدقيق تُسجّل معلومات مثل:

- نوع العملية المنفّذة.
- الحساب الإداري الذي قام بها.

- الحساب المستهدف.
- توقيت العملية.
- عنوان IP المرتبط بها.

تُستخدم هذه السجلات لأغراض المراقبة والمساءلة، وتشكّل جزءًا أساسيًا من آليات الأمان في النظام.

6.6.4 التكامل مع بقية مكوّنات النظام

يتكامل نظام التحكم بالوصول مع بقية مكوّنات النظام بشكل وثيق، حيث:

- يتم التحقق من الصلاحيات بعد نجاح المصادقة والتوثيق متعدد العوامل.
- يمنع الوصول إلى الموارد المشفّرة في حال عدم تحقق الشروط المطلوبة.
- يدعم هذا التكامل بنية الأمان الشاملة للنظام.

7.6.4 خلاصة القسم

يوضّح هذا القسم كيفية تنفيذ التحكم بالوصول وإدارة الصلاحيات عمليًا ضمن النظام المقترح، من خلال دمج RBAC و ABACلتحقيق دقة ومرونة في تحديد الصلاحيات. وقد أسهم هذا التنفيذ في تعزيز أمان النظام، ومنع الوصول غير المصرّح به، وتوفير آليات مراقبة فعّالة لإدارة المستخدمين والعمليات الحساسة.

7.4 النتائج العملية للنظام(Practical Results)

بعد الانتهاء من تنفيذ النظام المقترح واختباره عمليًا، تم التوصل إلى مجموعة من النتائج التي تؤكد نجاح التطبيق العملي للتصميم المعماري والآليات الأمنية المعتمدة. وتُظهر هذه النتائج مدى قدرة النظام على تحقيق الأهداف الوظيفية والأمنية التي تم تحديدها في بداية المشروع.

1.7.4 نتائج المصادقة والتوثيق

أثبت النظام فعاليته في تنفيذ آلية مصادقة آمنة قائمة على بروتوكولSRP ، حيث:

- تم التحقق من صحة كلمة المرور دون إرسالها أو تخزينها بصيغة مكشوفة.
- لم يتم إنشاء أي جلسة مستخدم قبل إتمام جميع مراحل التحقق.

- أظهر النظام مقاومة واضحة لمحاولات تسجيل الدخول غير المصرّح بها.

كما أسهم دمج التوثيق متعدد العوامل في رفع مستوى الأمان، إذ أصبح امتلاك كلمة المرور وحده غير كافٍ للوصول إلى الحساب.

2.7.4 نتائج التحقق البيومتري

أظهر التحقق البيومتري باستخدام بصمة الوجه نتائج إيجابية من حيث:

- سرعة تنفيذ عملية التحقق.
- دقة المطابقة بين التمثيل البيومتري الحالي والمخزّن.
- الحفاظ على الخصوصية من خلال تنفيذ جميع عمليات المعالجة والمقارنة محليًا داخل المتصفح.

وقد أثبت هذا الأسلوب فعاليته في تقليل المخاطر المرتبطة بنقل أو تخزين البيانات البيومترية على الخادم.

3.7.4 نتائج إدارة المفاتيح والتشفير

بيّنت النتائج العملية نجاح بنية إدارة المفاتيح المعتمدة، حيث:

- تم توليد مفتاح تشفير بيانات (DEK) فريد لكل مستخدم.
- لم يتم تخزين أي مفتاح تشفير بصيغة مكشوفة داخل قاعدة البيانات.
- أمكن إعادة تغليف DEK عند تغيير كلمة المرور دون الحاجة إلى إعادة تشفير البيانات المخزّنة.

كما أظهر استخدام خوارزمية AES-GCM فعالية عالية في حماية سرية البيانات وسلامتها.

4.7.4 نتائج إدارة كلمات المرور

نجح النظام في توفير وظائف متكاملة لإدارة كلمات المرور، شملت:

- إضافة كلمات مرور جديدة بسهولة.
- توليد كلمات مرور عشوائية قوية وفق معايير قابلة للتخصيص.

- عرض وتعديل وحذف بطاقات كلمات المرور ضمن بيئة مشفّرة بالكامل.

وقد ساعدت هذه الوظائف في تحسين تجربة المستخدم وتشجيعه على استخدام كلمات مرور قوية وفريدة.

5.7.4 نتائج التحكم بالوصول والإدارة

أظهرت النتائج أن آليات التحكم بالوصول المعتمدة كانت فعّالة في:

- الفصل الواضح بين صلاحيات المستخدم العادي وصلاحيات المدير.
- منع الوصول إلى الوظائف الإدارية من قبل مستخدمين غير مخوّلين.
- تمكين المدير من مراقبة النظام وإدارة المستخدمين من خلال واجهة إدارية واضحة.

كما ساهمت سجلات التدقيق في تعزيز الشفافية وإمكانية تتبع العمليات الحساسة.

6.7.4 تقييم عام للنتائج

بصورة عامة، أظهرت النتائج العملية أن النظام:

- يحقق مستوى عالٍ من الأمان دون التأثير السلبي على سهولة الاستخدام.
- يطبّق المفاهيم النظرية التي تم تناولها في الفصول السابقة بشكل فعلي.
- يقدّم نموذجًا عمليًا قابلًا للتطبيق والتوسّع في أنظمة إدارة كلمات المرور الحديثة.

7.7.4 خلاصة القسم

تؤكد النتائج العملية المتحصّل عليها نجاح النظام المقترح في تحقيق أهدافه الأمنية والوظيفية، حيث تم دمج المصادقة الآمنة، التوثيق متعدد العوامل، إدارة المفاتيح، والتحكم بالوصول ضمن نظام واحد متكامل. وتشكل هذه النتائج أساسًا مناسبًا للانتقال إلى تحليل النتائج ومناقشتها بصورة أعمق في القسم التالي.

8.4 تحليل النتائج ومناقشتها(Results Analysis and Discussion)

يهدف هذا القسم إلى تحليل النتائج العملية التي تم التوصل إليها بعد تنفيذ النظام المقترح، ومناقشتها في ضوء الأهداف الأمنية والوظيفية التي تم تحديدها في الفصول السابقة. ويساعد هذا التحليل

في تقييم فعالية النظام ومدى ملاءمته لمعالجة المشكلات المرتبطة بإدارة كلمات المرور في البيئات الرقمية الحديثة.

1.8.4 تحليل مستوى الأمان المحقق

تُظهر النتائج أن النظام نجح في تحقيق مستوى عالٍ من الأمان من خلال دمج عدة آليات متقدمة، أبرزها:

- استخدام بروتوكول SRP للتحقق من صحة كلمة المرور دون نقلها عبر الشبكة.
- تطبيق بنية انعدام المعرفة التي تمنع الخادم من الوصول المباشر إلى مفاتيح التشفير أو البيانات الحساسة.
- دمج التوثيق متعدد العوامل القائم على كلمة المرور والعامل البيومتري.

يسهم هذا التكامل في تقليل احتمالية الاختراق، حتى في حال تسريب قاعدة البيانات أو اعتراض الاتصالات.

2.8.4 مناقشة التحقق البيومتري وحماية الخصوصية

يُعد تنفيذ التحقق البيومتري محليًا داخل المتصفح من أهم نقاط القوة في النظام، إذ:

- يقلّل من مخاطر تسريب البيانات البيومترية.
- يحدّ من سطح الهجوم المرتبط بنقل الصور أو التمثيلات الرقمية.
- ينسجم مع مبادئ Privacy by Design و.Zero-Knowledge

وعلى الرغم من الاعتماد على جهاز المستخدم في هذه المرحلة، إلا أن النتائج أثبتت أن هذا الأسلوب يوفّر توازنًا فعّالًا بين الأمان والخصوصية.

3.8.4 تحليل إدارة المفاتيح والتشفير

أظهرت النتائج العملية نجاح بنية إدارة المفاتيح الهرمية، حيث:

- تم الفصل بوضوح بين مفاتيح التشفير ومفاتيح التغليف.
- لم يتم تخزين أي مفتاح تشفير بصيغة مكشوفة.
- أمكن تغيير كلمة المرور دون الحاجة إلى إعادة تشفير البيانات.

يعكس هذا النهج التزام النظام بأفضل الممارسات في مجال التشفير وحماية البيانات.

4.8.4 تحليل تجربة المستخدم

على الرغم من اعتماد النظام على آليات أمنية متقدمة، إلا أن تجربة المستخدم بقيت واضحة وسلسة، حيث:

- تم تقسيم عملية المصادقة إلى خطوات منطقية.
- لم تُفرض إجراءات معقّدة أو غير ضرورية على المستخدم.
- ساعد تصميم الواجهات على تقليل الأخطاء وتحسين التفاعل.

يشير ذلك إلى أن النظام نجح في الجمع بين الأمان العالي وسهولة الاستخدام، وهو تحدٍ رئيسي في أنظمة إدارة كلمات المرور.

5.8.4 مقارنة النتائج مع الأهداف المحددة

بمقارنة النتائج العملية مع الأهداف التي تم تحديدها في بداية المشروع، يتبيّن أن النظام:

- عالج مشكلة تخزين كلمات المرور غير الآمن.
- وفّر آلية مصادقة قوية تتجاوز الاعتماد على كلمة المرور فقط.
- أتاح إمكانية استخدام النظام من أجهزة متعددة دون فقدان مستوى الأمان.

وبذلك، يمكن القول إن الأهداف الرئيسية للمشروع قد تحققت بدرجة عالية.

6.8.4 حدود النظام والتحديات

على الرغم من النتائج الإيجابية، واجه النظام بعض التحديات، من أبرزها:

- الاعتماد على توفر كاميرا مناسبة لتنفيذ التحقق البيومتري.
- الحاجة إلى توافق المتصفح مع مكتبات التحقق البيومتري.
- زيادة زمن تسجيل الدخول نسبيًا نتيجة تعدد مراحل التحقق.

تُعد هذه التحديات طبيعية في الأنظمة ذات الحساسية الأمنية العالية، ويمكن معالجتها أو تحسينها في مراحل التطوير المستقبلية.

7.8.4 خلاصة القسم

يوضح هذا القسم أن النظام المقترح قد حقق توازنًا فعّالًا بين الأمان، الخصوصية، وسهولة الاستخدام. كما تؤكد النتائج والتحليل أن الدمج بين المصادقة الآمنة، التوثيق متعدد العوامل، وإدارة المفاتيح المتقدمة يشكّل أساسًا قويًا لبناء أنظمة إدارة كلمات مرور موثوقة في البيئات الحديثة.

9.4 خاتمة الفصل الرابع

تناول هذا الفصل التطبيق العملي للنظام المقترح لإدارة كلمات المرور، وبيّن كيفية تحويل التصميم المعماري والآليات الأمنية التي تم تناولها في الفصل الثالث إلى نظام فعلي قابل للاستخدام. وقد تم استعراض بيئة التطوير، وتنفيذ الواجهة الخلفية والواجهة الأمامية، مع توضيح آليات المصادقة، والتوثيق متعدد العوامل، وإدارة الصلاحيات، مدعومة بعرض واجهات الاستخدام المختلفة.

أظهرت النتائج العملية أن النظام نجح في تطبيق بروتوكولات مصادقة آمنة وبنية تشفير متقدمة تحقّق مبدأ انعدام المعرفة، مع الحفاظ على خصوصية المستخدم من خلال تنفيذ التحقق البيومتري محليًا. كما أثبت النظام فعاليته في إدارة كلمات المرور وتوفير وظائف متكاملة تجمع بين الأمان وسهولة الاستخدام، إضافةً إلى تمكين الإدارة من مراقبة النظام والتحكم بالصلاحيات عبر واجهة مخصّصة.

ومن خلال تحليل النتائج ومناقشتها، تبيّن أن النظام حقق الأهداف الأمنية والوظيفية المحددة، مع وجود بعض التحديات الطبيعية المرتبطة بالأنظمة ذات الحساسية الأمنية العالية، والتي يمكن معالجتها في مراحل تطوير لاحقة. وبذلك، يشكّل هذا الفصل جسرًا عمليًا يربط بين الإطار النظري والتطبيقي للمشروع، ويمهّد للانتقال إلى الخاتمة العامة التي تستعرض الاستنتاجات النهائية وآفاق التطوير المستقبلية.

5 المراجع

1.5 المراجع

1. *Barker, E., Chen, L., Roginsky, A., Vassilev, A., & Davis, R. (2023).* Recommendation for Pair-Wise Key-Establishment Using Discrete Logarithm Cryptography (SP 800-56A Rev. 5). *National Institute of Standards and Technology (NIST).*
2. *Wu, T. (1998).* The Secure Remote Password Protocol. *Proceedings of the Internet Society Network and Distributed System Security Symposium (NDSS).*
3. *Wu, T. (2000).* SRP-6: Improvements and Refinements to the Secure Remote Password Protocol. *Stanford University.*
4. *National Institute of Standards and Technology. (2020).* Digital Identity Guidelines (SP 800-63B). *NIST.*
5. *Biryukov, A., Dinu, D., & Khovratovich, D. (2016).* Argon2: The Memory-Hard Function for Password Hashing and Other Applications. *IEEE European Symposium on Security and Privacy.*
6. *National Institute of Standards and Technology. (2007).* Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (SP 800-38D). *NIST.*
7. *Green, M., & Smith, I. (2016).* The Cryptopals Crypto Challenges: Applied Cryptography in Practice. *Johns Hopkins University.*
8. *AgileBits Inc. (2022).* 1Password Security Design. *AgileBits Technical Documentation.*
9. *Oneal, S., & Goldberg, J. (2023).* Advances in Secure Remote Password Storage and Secret-Sharing: A Technical Overview of 1Password's Security Model. *1Password Security Whitepaper.*
10. *Bitwarden Inc. (2023).* Bitwarden Security Whitepaper. *Bitwarden Documentation.*
11. *LogMeIn Inc. (2022).* LastPass Security Architecture Whitepaper. *LogMeIn Security Documentation.*
12. *Jain, A. K., Ross, A., & Nandakumar, K. (2011).* Introduction to Biometrics. *Springer Science & Business Media.*
13. *ISO/IEC. (2019).* ISO/IEC 19794-5: Information Technology — Biometric Data Interchange Formats — Face Image Data. *International Organization for Standardization.*
14. *Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001).* Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal, 40(3), 614–634.*
15. *OWASP Foundation. (2023).* OWASP Authentication Cheat Sheet. *Open Web Application Security Project.*
16. *OWASP Foundation. (2023).* OWASP Cryptographic Storage Cheat Sheet. *Open Web Application Security Project.*

17. *Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2014).* Guide to Attribute Based Access Control (ABAC) Definition and Considerations (SP 800-162). *National Institute of Standards and Technology (NIST).*
18. *Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996).* Role-Based Access Control Models. *IEEE Computer, 29(2), 38–47.*
19. *Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012).* The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *IEEE Symposium on Security and Privacy.*
20. *Mozilla Developer Network (MDN). (2024).* Web Cryptography API Documentation. *Mozilla Foundation.*
21. *Barker, E., Chen, L., Roginsky, A., Vassilev, A., & Davis, R. (2023).* Recommendation for Pair-Wise Key-Establishment Using Discrete Logarithm Cryptography (SP 800-56A Rev. 5). *National Institute of Standards and Technology (NIST).*
22. *T. Wu, "The Secure Remote Password Protocol", Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium (NDSS), 1998.*
23. *Campbell, J. P. Speaker Recognition: A Tutorial, Proceedings of the IEEE, Vol. 85, No. 9, 1997.*
24. *Daugman, J. How Iris Recognition Works, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, 2004.*