Comprehensive Journal of Science
Volume (10), Issue (37), (NOV. 2025)
SICST2025, www.sicst.ly
ISSN: 3014-6266

مجلة العلوم الشاملة
عدد خاص بالمؤتمر الدولي الثالث للعلوم والتقنية
المجلد (10)، العدد (37)، (نوفمبر2025)
ردمد: 3014-6266

A proposed model for medical records managing using blockchain: an analytical study

Ibrahim Mohamed Alzaidi *, Dr. Juma Ibrahim

Postgraduate office, software development technology, college of Computer Technology Tripoli (CCTT), Libya

*Corresponding author: iz2303001@cctt.edu.ly

نموذج مقترح لإدارة السجلات الطبية باستخدام البلوك تشين: دراسة تحليلية

إبراهيم محمد الزائدي، جمعه إبراهيم
مكتب الدراسات العليا، قسم هندسه تطوير البرمجيات، كليه تقنيه الحاسوب طرابلس، ليبيا

Received: 30-09-2025; Revised: 10-10-2025; Accepted: 31-10-2025; Published: 25-11-2025

Abstract :

Electronic medical records (EMRs) represent a cornerstone of modern healthcare systems; however, challenges such as data fragmentation in paper and electronic formats, inefficient management, limited accessibility, and security and privacy concerns remain significant obstacles to building an integrated health system. This paper proposes a blockchain-based model, specifically utilizing **Hyperledger Fabric**, to aggregate patients' medical records from multiple sources within a unified and secure framework. The proposed model leverages blockchain features—transparency, decentralization, and immutability—while granting patients full control over access permissions through a direct consent mechanism implemented via smart contracts and digital signatures. Physicians can request access to a patient's data, which the patient may approve or reject, while laboratory results are shared through private channels to preserve confidentiality and ensure regulatory compliance. The system defines distinct roles for hospitals, insurance companies, and the Ministry of Health in administrative and financial processes without granting direct access to medical records. A prototype experiment demonstrated the efficiency of the model in enhancing data protection and achieving transparency, paving the way for broader practical applications. The paper also highlights challenges related to system performance, integration with existing infrastructures, and legal considerations, while outlining the expected impact on improving healthcare quality and enabling secure, real-time access to patients' medical histories.

Keywords:
Electronic Medical Records (EMRs) ,Hyperledger Fabric ,Smart Contracts ,Healthcare Data Privacy , Access Control Management ,Digital Healthcare

الملخص:

تشكل السجلات الطبية الإلكترونية محورًا أساسيًا في أنظمة الرعاية الصحية الحديثة، إلا أن تجزئة البيانات الورقية والإلكترونية، وضعف إدارتها وصعوبة الوصول إليها، إضافة إلى تحديات الأمان والخصوصية، لا تزال تمثل عوائق أمام بناء نظام صحي متكامل. في هذه الورقة، نقترح نموذجًا تقنيًا يعتمد على تقنيات البلوك تشين، وتحديدًا منصة Hyperledger Fabric، لتجميع السجلات الطبية للمرضى من مصادر متعددة ضمن إطار موحد وآمن. يقوم النموذج على خصائص البلوك تشين مثل الشفافية، اللامركزية، وعدم القابلية للتغيير، مع منح المريض سيطرة كاملة على صلاحيات الوصول إلى بياناته عبر نظام موافقة مباشر يُنفذ

باستخدام العقود الذكية والتوقيعات الرقمية. يتيح هذا النموذج للأطباء طلب الاطلاع على بيانات المرضى، بينما يحتفظ المريض بحق القبول أو الرفض، كما يتيح تبادل نتائج المختبرات عبر قنوات خاصة تحافظ على الخصوصية وتحقق الامتثال القانوني. يتضمن النظام أدوارًا محددة للمستشفيات، شركات التأمين، ووزارة الصحة في الجوانب الإدارية والمالية، دون وصول فعلي إلى السجلات الطبية نفسها. أظهرت التجربة المصغرة للنظام كفاءته في تعزيز حماية البيانات وتحقيق الشفافية، مما يفتح المجال لتطبيقات عملية أوسع. كما تناقش الورقة التحديات المتعلقة بالأداء، تكامل الأنظمة، والجوانب القانونية، وتستعرض الآثار المتوقعة في تحسين جودة الرعاية الصحية وتسهيل الوصول الفوري والآمن إلى التاريخ الطبي للمرضى.

الكلمات المفتاحية:
السجلات الطبية الإلكترونية، بلوك تشين،Hyperledger Fabric ، العقود الذكية، خصوصية البيانات الصحية، إدارة صلاحيات الوصول، الرعاية الصحية الرقمية

المقدمة (Introduction):

تُعد السجلات الطبية الإلكترونية (Electronic Medical Records – EMR) عنصرًا جوهريًا في البنية التحتية لأنظمة الرعاية الصحية الحديثة، حيث تمكّن مقدمي الخدمات الطبية من تسجيل وتبادل المعلومات الصحية للمريض بطريقة رقمية تسهم في تحسين جودة الرعاية وسرعة اتخاذ القرار الطبي. ومع ذلك، وعلى الرغم من هذا التقدم، لا تزال المؤسسات الصحية تعاني من تحديات جوهرية في تجميع السجلات الطبية للمريض من مصادر متعددة، سواء على مستوى المستشفيات أو العيادات أو المختبرات، مما يؤدي إلى تجزئة البيانات الطبية وصعوبة الوصول الشامل إلى تاريخ المريض الصحي.

تعود هذه التحديات غالبًا إلى غياب البنية التقنية الموحدة، واختلاف أنظمة إدارة السجلات بين المؤسسات، بالإضافة إلى المخاوف المتعلقة بأمان البيانات وخصوصيتها (Esposito, De Santis, Tortora, Chang, & Choo, 2018). وفي ظل تنامي هذه التحديات، برزت الحاجة إلى حلول مبتكرة تضمن تجميعًا آمنًا وموثوقًا وشاملًا للسجلات الطبية، بما يحقق الكفاءة التشغيلية ويحافظ في الوقت ذاته على خصوصية المرضى وحقوقهم.

في هذا السياق، ظهرت تقنية البلوك تشين (Blockchain) كأحد أبرز الحلول المحتملة في المجال الصحي، نظرًا لما توفره من شفافية، ولا مركزية، وعدم قابلية للتلاعب في البيانات (Mettler, 2016). تتيح البلوك تشين إمكانية تسجيل المعاملات الطبية بطريقة مشفّرة وآمنة، وتُمكّن المريض من التحكم في الوصول إلى بياناته، كما توفر للمؤسسات الطبية طريقة موحدة لتبادل المعلومات دون الاعتماد على طرف مركزي واحد.

وقد قدمت دراسات مبكرة مثل مشروع MedRec نموذجًا عمليًا لإدارة صلاحيات الوصول إلى البيانات الصحية باستخدام البلوك تشين، مما أثبت فعالية هذه التقنية في تعزيز موثوقية السجلات الطبية (Azaria, Ekblaw, Vieira, & Lippman, 2016). وبالرغم من تعدد المبادرات التي استخدمت تقنيات البلوك تشين في القطاع الصحي، إلا أن معظمها إما لم يُطبق فعليًا على نطاق واسع، أو لم يُحقق التكامل المنشود بين مقدمي الرعاية الصحية.

ولذلك، تأتي هذه الورقة لتقديم نموذج مقترح لتجميع السجلات الطبية باستخدام البلوك تشين، يعتمد على تصميم معماري يُسهم في توحيد مصادر البيانات الصحية للمريض، ويضمن أمنها وإمكانية الوصول إليها بطريقة مرنة ومنظمة. تهدف الورقة إلى تحليل هذا النموذج من الناحية التقنية والأمنية، واستعراض مزاياه مقارنة بالأنظمة التقليدية، بالإضافة إلى مناقشة الجوانب القانونية والأخلاقية المرتبطة به. كما تتضمن الورقة دراسة حالة مصغّرة لتوضيح آلية عمل النموذج المقترح في بيئة صحية واقعية.

ويعتمد النموذج المقترح على منصةHyperledger Fabric ، وهي أحد أبرز أطر البلوك تشين الموجهة للمؤسسات، بما يُمكّنه من تحقيق درجات عالية من الخصوصية وقابلية التوسع، مما يجعله مناسبًا للبيئات الطبية متعددة الأطراف.(Hyperledger Foundation, 2023)

بيان المشكلة (Problem Statement):

على الرغم من الانتشار الواسع للسجلات الطبية الإلكترونية(EMRs) ، إلا أن معظم المؤسسات الصحية تواجه **تجزئة البيانات وصعوبة دمج السجلات الطبية** من مصادر متعددة، سواء كانت مستشفيات، عيادات، أو مختبرات، مما يؤدي إلى **إضعاف جودة الرعاية الصحية** وصعوبة الوصول الشامل لتاريخ المريض الطبي (Nguyen et al., 2014; Adler-Milstein & Jha, 2017).

كما أن الاعتماد على أنظمة مركزية لتخزين السجلات يعرض البيانات لمخاطر **الأمن السيبراني** ويحد من قدرة المريض على التحكم في بياناته، خاصة عند التنقل بين مؤسسات مختلفة.(Roehrs et al., 2017)

على الرغم من الاهتمام المتزايد بتقنية البلوك تشين في المجال الصحي، فإن معظم الحلول الحالية لم تصل بعد إلى **التطبيق العملي واسع النطاق**، أو لم تحقق التكامل المطلوب بين مقدمي الرعاية الصحية المتعددين، كما تواجه تحديات مرتبطة بـ **الأداء، قابلية التوسع، والأطر القانونية والتنظيمية** (Azaria et al., 2016; Angraal et al., 2017; Agbo et al., 2019).

بالتالي، تكمن المشكلة البحثية في:

الحاجة إلى نموذج تقني متكامل لتجميع السجلات الطبية باستخدام البلوك تشين، يضمن الأمان والخصوصية، ويمنح المرضى تحكمًا مباشرًا في بياناتهم، مع قابلية للتطبيق في بيئات الرعاية الصحية متعددة الأطراف

أسئلة البحث:(Research Questions)

- **ما هي التحديات التقنية، الأمنية، والقانونية التي تواجه النماذج الحالية لتجميع السجلات الطبية الإلكترونية(EMRs) ؟**
- **إلى أي مدى يمكن لتقنية البلوك تشين، وخاصة المنصات المرخصة مثل Hyperledger Fabric ، معالجة هذه التحديات؟**
- **كيف يمكن تصميم نموذج تقني قائم على Hyperledger Fabric يحقق:**
  - التكامل بين أنظمة الرعاية الصحية المختلفة،
  - حماية خصوصية المرضى،
  - تعزيز الأمان والتحكم بالبيانات؟
- **ما هي آلية عمل النموذج المقترح عند تطبيقه في سيناريو افتراضي يضم أطرافًا متعددة (مستشفيات، مختبرات، شركات تأمين، مرضى)؟**
- **ما هي الجوانب الأمنية والأخلاقية والقانونية التي يجب أخذها بعين الاعتبار لضمان امتثال النموذج لمعايير مثل HIPAA وGDPR؟**

مراجعة الأدبيات(Literature Review)

- **السجلات الطبية الإلكترونية(EMRs)**

شهدت نظم السجلات الطبية الإلكترونية (EMRs) تطورًا ملحوظًا خلال العقود الماضية، إذ أصبحت الوسيلة الأساسية لحفظ معلومات المريض الصحية بطريقة رقمية قابلة للتحديث والمشاركة. تهدف هذه الأنظمة إلى تحسين جودة الرعاية الصحية، وتقليل الأخطاء الطبية، وتسريع الوصول إلى البيانات السريرية (Nguyen et al., 2014).

رغم ذلك، لا تزال العديد من المؤسسات الصحية تُعاني من تجزئة البيانات وصعوبة دمج السجلات الطبية المُنتجة عبر مزودين مختلفين للرعاية، مما يُؤثر سلبًا على كفاءة التشخيص واتخاذ القرار العلاجي(Adler-Milstein & Jha, 2017).

كما أن الاعتماد على أنظمة مركزية لتخزين السجلات يزيد من مخاطر الأمن السيبراني، ويقلل من مرونة المريض في إدارة بياناته الصحية، خاصة عند تنقله بين مؤسسات متعددة.(Roehrs et al., 2017)

- **تقنية البلوك تشين(Blockchain)**

تُعد تقنية البلوك تشين من الابتكارات التقنية التي فرضت حضورها في عدة مجالات، لاسيما في القطاع المالي، ثم امتد استخدامها إلى الرعاية الصحية. تقوم هذه التقنية على سجل موزع لا مركزي، يُسجّل المعاملات بطريقة

مشفّرة ومترابطة زمنيًا، مما يجعل التلاعب بالمعلومات أو حذفها أمرًا شبه مستحيل.(Zheng et al., 2018)
من أبرز خصائص البلوك تشين التي تجعلها ملائمة للسجلات الصحية:

- الشفافية :حيث يمكن تتبع كل عملية على السجل.
- اللامركزية :مما يحد من الاعتماد على جهة مركزية واحدة.
- عدم قابلية التعديل :(Immutability) مما يضمن سلامة البيانات.

إضافة إلى ذلك، تدعم بعض تطبيقات البلوك تشين العقود الذكية(Smart Contracts) ، والتي تُسهم في إدارة أذونات الوصول إلى البيانات الطبية بشكل آلي ودقيق.(Azaria et al., 2016)
ومن أبرز الأطر المؤسسية، تبرز منصة Hyperledger Fabric، والتي طورتها مؤسسة Linux بدعم من IBM. تتميز هذه المنصة بكونها مصرّح بها(Permissioned) ، أي أن المشاركين في الشبكة معروفون ومعتمدون، وهو أمر بالغ الأهمية عند التعامل مع البيانات الصحية الحساسة. كما تسمح Fabric باستخدام قنوات خاصة (Private Channels) لتبادل البيانات بين أطراف محددة، مما يوفر درجة عالية من الخصوصية والتخصيص.(Androulaki et al., 2018)

- **تطبيقات البلوك تشين في المجال الطبي**

برزت عدة مشاريع بحثية وتجارية حاولت دمج البلوك تشين في إدارة السجلات الطبية. من أبرزها:

- مشروع MedRec منMIT ، الذي اعتمد على Ethereum لتسجيل بيانات المرضى وتمكين الأطباء من الوصول إليها بإذن من المريض.(Azaria et al., 2016)
- Patientory، وهي منصة قائمة على البلوك تشين تهدف إلى تمكين المرضى من التحكم الكامل في سجلاتهم الصحية ومشاركتها مع مقدمي الخدمة.
- Medicalchain، التي توفر سجلًا طبيًا موزعًا يمكن للأطباء والمرضى الوصول إليه بطريقة مشفّرة وآمنة.

رغم هذه المبادرات، لا تزال معظم الأنظمة في مرحلة التجريب أو الاستخدام المحدود، ويواجه بعضها تحديات في قابلية التوسع والتكامل مع البنى التحتية الحالية والامتثال للتشريعات الصحية (Angraal et al., 2017; Rifi et al., 2017).

الفجوات البحثية

على الرغم من الجهود المبذولة، تشير الدراسات إلى وجود فجوات واضحة في تصميم وتنفيذ حلول فعّالة لتجميع السجلات الطبية باستخدام البلوك تشين، من أبرزها:

- غياب نماذج معيارية قابلة للتنفيذ على نطاق واسع.(Agbo et al., 2019)

- عدم وضوح الأطر القانونية والتنظيمية في معظم الدول.
- محدودية الدراسات التي تجمع بين الجوانب التقنية والأمنية والقانونية في آنٍ واحد (Kuo et al., 2017).
- تحديات قابلية التوسع والأداء مع ازدياد حجم البيانات الطبية.(Rifi et al., 2017)

تُظهر هذه الفجوات الحاجة إلى تطوير نموذج متكامل، يُراعي الجوانب التقنية والأمنية والأخلاقية، ويُسهم في تجميع السجلات الطبية بطريقة موثوقة، وآمنة، وقابلة للتطبيق، وهو ما تسعى إليه هذه الورقة.

أهداف البحث (Research Objectives)

استنادًا إلى مراجعة الأدبيات وفجوات البحث السابقة، تهدف هذه الورقة البحثية إلى:

- تصميم نموذج تقني لتجميع السجلات الطبية باستخدام Blockchainمع توفير سيطرة كاملة للمريض على بياناته.
- استعراض البنية التقنية والأمنية للنظام المقترح، مع التركيز على منصة Hyperledger Fabric وتطبيق العقود الذكية.(Smart Contracts)
- تحليل مزايا النموذج المقترح مقارنة بالأنظمة التقليدية، بما في ذلك الشفافية، قابلية التوسع، وموثوقية البيانات.
- مناقشة التحديات القانونية والأخلاقية المتعلقة بتطبيق النموذج في بيئات الرعاية الصحية متعددة الأطراف.
- تقديم دراسة حالة مصغرة (Pilot Study) لتوضيح آلية عمل النموذج في بيئة صحية واقعية.

المنهجية (Methodology)

تعتمد هذه الدراسة منهجًا تحليليًا–تصميميًا (Analytical–Design Approach)يهدف إلى اقتراح نموذج تقني مبتكر لمعالجة التحديات المتعلقة بتجميع السجلات الطبية باستخدام تقنية البلوك تشين.
لا تعتمد الدراسة على جمع بيانات ميدانية، بل تُركّز على تحليل نقدي للأدبيات السابقة وتصميم نموذج نظري/عملي يستند إلى أسس علمية وتقنية راسخة، مع مراعاة البُعد الأمني والقانوني لتطبيقه في بيئة الرعاية الصحية متعددة الأطراف.(Azaria et al., 2016; Nguyen et al., 2014)
تتبنى الدراسة أيضًا منهجًا تحليليًا–تطبيقيًا (Analytical–Applied Approach)، حيث تُقدَّم دراسة تصميمية عملية باستخدام منصة Hyperledger Fabric كإطار تقني لتنفيذ المفهوم.(Androulaki et al., 2018)

- **اختيار منصة (Hyperledger Fabric)**

تم اختيار (Hyperledger Fabric) لكونها منصة بلوك تشين مصرّح بها (**Permissioned**) تتناسب مع الاستخدامات المؤسسية في القطاع الصحي، وذلك لما توفره من:

- إدارة الهويات باستخدام .(Membership Service Provider (MSP
- قنوات خاصة (Private Channels) لتبادل البيانات بسرية بين أطراف محددة.
- دعم العقود الذكية (Chaincode) بلغات مثل Go و .Node.js
- إمكانية وضع سياسات وصول صارمة والتحكم في صلاحيات المشاركين.
- دعم مبدأ التجزئة (Partitioning) الذي يُعزز الخصوصية ويقلل من المخاطر الأمنية (Androulaki et al., 2018).

- **أهداف المنهجية**

- تحليل الفجوات في النماذج الحالية لتجميع السجلات الطبية، بما في ذلك التحديات التقنية، الأمنية، والقانونية.(Nguyen et al., 2014)
- دراسة خصائص البلوك تشين المناسبة لتطبيقات السجلات الطبية مثل العقود الذكية، القنوات الخاصة، وعدم قابلية التغيير .(Azaria et al., 2016)
- تصميم نموذج مقترح قادر على تحقيق:
  - ❖ التكامل بين أنظمة الرعاية الصحية المختلفة.
  - ❖ حماية خصوصية المرضى وحقوقهم في التحكم بالبيانات.
  - ❖ تحسين الوصول إلى المعلومات الصحية بطريقة مرنة وآمنة.
- توضيح آلية عمل النموذج من خلال دراسة حالة افتراضية، تُظهر كيفية تعامل مختلف الأطراف (المستشفيات، المختبرات، شركات التأمين، المرضى) مع البيانات.(Roehrs et al., 2017)
- إجراء تحليل أمني وأخلاقي لضمان توافقه مع معايير الخصوصية مثل HIPAA و GDPR (Roehrs et al., 2017).

البنية المقترحة للنظام

يتكون النظام من عدة أطراف، لكل منها عقدة (Node) داخل شبكة:Hyperledger Fabric

الطرف	الوظيفة
المريض	يتحكم في صلاحيات مشاركة بياناته الصحية.
الطبيب	يطلب الوصول إلى السجلات بعد موافقة المريض.

الطرف	الوظيفة
المستشفى	تتحقق من الامتثال القانوني والإداري.
المختبر	يرسل نتائج الفحوصات والتحاليل.
شركة التأمين	تربط بين الموافقات والتغطية المالية.
وزارة الصحة	تراقب الامتثال للقوانين والمعايير.

- **يعتمد النموذج المقترح على دمج أنظمة الهوية البيومترية (Biometric Identity Systems)** ضمن بيئة Hyperledger Fabric بهدف تعزيز مستوى الأمان ومنع الوصول غير المصرح به. يتم ربط الهوية الرقمية لكل مستخدم داخل الشبكة بمُعرّف بيومتري يتم تسجيله والتحقق منه من خلال Membership Service Provider (MSP)، بحيث لا يتم السماح بتنفيذ أي طلب وصول إلى السجلات الطبية دون تطابق البصمة البيومترية مع الهوية المسجلة.

  يحقق هذا الدمج:

  - حماية أعلى من انتحال الهوية.
  - تعزيز الثقة بين أطراف الشبكة.
  - تقليل المخاطر المرتبطة بالوصول غير القانوني.
  - دعم الامتثال التشريعي الخاص بحماية البيانات الطبية.

- **إدارة بيانات الطوارئ(Emergency Data Management)**

يتضمن النموذج المقترح وحدة متخصصة لإدارة بيانات الطوارئ، يتم من خلالها تخزين نسخة مشفرة من البيانات الأساسية للمريض داخل قناة خاصة .Emergency Private Channel ولا يتم فك تشفير هذه البيانات إلا عند:

- وجود حالة طبية طارئة تستدعي الوصول السريع؛
- قيام الجهة المخولة (مثل طبيب الطوارئ) بتفعيل طلب وصول؛
- تحقق العقد الذكي (Smart Contract Trigger)من شروط الإذن؛
- تسجيل كافة تفاصيل العملية داخل السجل الموزع لضمان الشفافية والمساءلة.

يسمح هذا النظام بالاستجابة الفورية للحالات الطارئة دون المساس بخصوصية المريض أو الكشف عن بيانات غير ضرورية.

- **إعداد الشبكة وتنفيذ النموذج**
- **إنشاء الشبكة:(Network Bootstrapping)**
  - إعداد ملف التكوين configtx.yaml لتعريف المنظمات والقنوات.
  - استخدام Fabric CA لإصدار شهادات الهويات الرقمية.
  - تهيئة Orderer باستخدام خوارزمية التوافق) مثل.(RAFT
- **تكوين القنوات:(Channels)**
  - قناة عامة: لتسجيل التفاعلات الإدارية.
  - قناة خاصة: بين المريض والطبيب بعد الموافقة.
- **نشر العقود الذكية:(Chaincode)**
  - عقدة :AccessRequestContractلإدارة طلبات الوصول.
  - عقدة :ConsentContractلتخزين الموافقات والتحقق منها.
  - عقدة :InsuranceContractالربط التغطية التأمينية بالموافقات.
- **خطوات التنفيذ التجريبي(Pilot Study)**
  - **بيئة التطوير Docker :، Fabric CLI، .Visual Studio Code**
  - **سيناريو المحاكاة:**
    - ❖ تسجيل (3 مرضى، 3 أطباء، 2 مختبر).
    - ❖ تنفيذ 20 عملية طلب/موافقة.
- **المؤشرات المقاسة:**
  - زمن الموافقة.(Request-to-Approval Time)
  - زمن إنشاء القناة الخاصة.
  - معدل استهلاك الموارد على الشبكة.
- **دمج تقنيات الهوية البيومترية (Biometric Identity Systems)** يمثل جزءًا محوريًا ضمن المنهجية المعتمدة في هذه الدراسة، حيث تعتمد عملية التحقق من المستخدمين (المرضى، الأطباء، المختبرات وغيرهم) على بصمات بيومترية موثوقة مثل بصمة الإصبع

أو بصمة الوجه أو قزحية العين. يهدف هذا الدمج إلى رفع مستوى الأمان ومنع انتحال الهوية عند الوصول إلى السجلات الطبية.

كما تشمل المنهجية تصميم **وحدة إدارة بيانات الطوارئ Emergency Data Access) (Module**، والتي تتيح الوصول المقنن والفوري إلى بيانات حرجة من السجل الطبي للمريض في الحالات الطارئة فقط. ويجري هذا الوصول وفق آلية تحقق متعددة المستويات تعتمد على **العقود الذكية (Smart Contracts)** للتحقق من أن الجهة الطالبة مخولة قانونيًا، مع تسجيل كامل لجميع الطلبات ضمن السجل غير القابل للتغيير لضمان الشفافية والامتثال الأخلاقي.

حدود الدراسة

- النموذج لم يتم اختباره على شبكة عامة واسعة النطاق.
- لا يغطي الجوانب الاقتصادية أو التشغيلية.
- لم يتم دمج الهوية البيومترية أو سجلات الطوارئ حتى الآن.

النتائج المتوقعة

- توفير تصميم نظري–عملي يمكن اعتماده كأساس لتطبيق واقعي.
- إظهار دور البلوك تشين في تعزيز أمان وخصوصية السجلات الطبية.
- فتح آفاق لدراسات مستقبلية تشمل:
  - اختبار عملي على نطاق مؤسسي/وطني.
  - تقييم الأداء عند التوسع بعدد كبير من المستخدمين.
  - دمج أدوات هوية رقمية متقدمة مثل الهوية السيادية الذاتية.(SSI)

نموذج المعمارية وتدفق البيانات(Model Architecture & Data Flow)

- **نظرة عامة على المعمارية**

يعتمد النموذج المقترح على **منصة Hyperledger Fabric** لتجميع السجلات الطبية بطريقة آمنة وشفافة، مع منح المريض السيطرة الكاملة على بياناته الصحية. تتضمن المعمارية العناصر التالية:

- **المريض :(Patient)** يمتلك السجل الطبي الرقمي الكامل ويمكنه منح أو رفض الوصول للبيانات باستخدام العقود الذكية.
- **مقدمو الرعاية الصحية :(Healthcare Providers)** مستشفيات، عيادات، ومختبرات، يمكنهم طلب الوصول للبيانات وفق أذونات المريض.

- **العقود الذكية :(Smart Contracts)** تتحكم في آلية منح الوصول ومصادقة المستخدمين، وتضمن تسجيل كل عملية بطريقة لا قابلة للتعديل.
- **قنوات خاصة :(Private Channels)** تتيح تبادل البيانات بين الأطراف المحددة دون الإفصاح الكامل للسجل، مما يحافظ على الخصوصية.
- **سجل موزع :(Distributed Ledger)** يحتفظ بسجل لجميع المعاملات والوصولات، ويضمن **عدم التلاعب بالبيانات** والشفافية.

- **تدفق البيانات(Data Flow)**

يُوضح تدفق البيانات كيفية تبادل المعلومات بين المريض ومقدمي الخدمة الصحية:

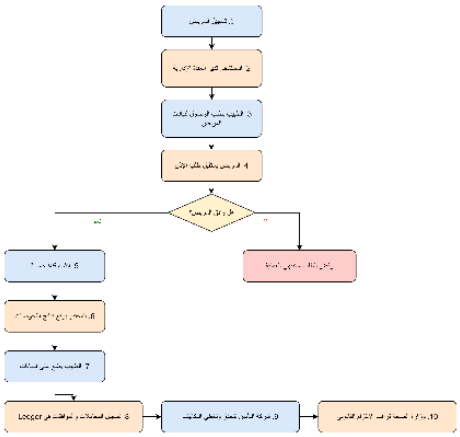
- يقوم **مقدم الرعاية الصحية** بطلب الوصول إلى بيانات محددة من سجل المريض.
- يتم إرسال الطلب إلى **العقد الذكي** الذي يتحقق من هوية مقدم الطلب ومن أذونات المريض.
- **المريض يوافق أو يرفض الطلب** باستخدام توقيع رقمي.
- عند الموافقة، يتم تسليم البيانات عبر **قناة خاصة** بين المريض ومقدم الخدمة، دون أن يطلع أي طرف آخر على التفاصيل.
- يتم تسجيل العملية كاملة على **السجل الموزع** لضمان الشفافية ومراجعة العمليات لاحقًا عند الحاجة.

مثال توضيحي: إذا أراد طبيب مختبر الوصول إلى نتائج تحاليل المريض، يرسل طلبًا للعقد الذكي، الذي يرسل إشعارًا للمريض. بعد موافقة المريض، يتم تسليم النتائج عبر القناة الخاصة مع تسجيل كل خطوة في السجل الموزع.

- **مزايا النموذج**

- **تحكم كامل للمريض** في بياناته، مع إمكانية منح وصول محدود المدة أو الغرض.
- **حماية الخصوصية** باستخدام القنوات الخاصة والعقود الذكية.
- **توحيد مصادر البيانات** من مختلف مقدمي الخدمة الصحية دون الاعتماد على جهة مركزية واحدة.
- **الشفافية والمراجعة** لكل المعاملات دون المخاطرة بسرية البيانات.
- **قابلية التوسع** في المستقبل لتغطية مؤسسات صحية متعددة مع الحفاظ على الأداء والأمان.

- **رسم تخطيطي مقترح للنموذج**



- **خطوات سير العملية في النظام:**
  - **تسجيل المريض في النظام** (إنشاء هوية رقمية)
  - **المستشفى تدير العقدة الإدارية** وتؤكد هوية الطبيب.
  - **الطبيب يطلب الوصول** لبيانات المريض عبر العقد الذكي.
  - **المريض يستقبل طلب الإذن** ويراجع التفاصيل.
  - **المريض يوافق أو يرفض** طلب الوصول.
  - **في حالة الموافقة:**
    - ❖ تنشأ قناة خاصة بين المريض والطبيب.
    - ❖ يرفع المختبر نتائج الفحوصات إلى القناة.
  - **الطبيب يطلع على البيانات** ويقدم التشخيص أو العلاج.
  - **تسجيل كل المعاملات والموافقات** في الـLedger.
  - **شركة التأمين تتحقق** من بيانات الموافقة وتتم معالجة المطالبات.
  - **وزارة الصحة تراقب** التزام النظام بالقوانين والسياسات.

النموذج المقترح لتجميع السجلات الطبية باستخدام Hyperledger Fabric

- **نظرة عامة على النموذج**

يهدف النموذج المقترح إلى إنشاء نظام موثوق وآمن لتجميع السجلات الطبية الإلكترونية (EMRs) من مصادر مختلفة داخل شبكة واحدة قائمة على تقنية **Hyperledger Fabric.** يُمكّن النظام المريض من التحكم الكامل في مشاركة ملفه الطبي مع الأطباء، مع ضمان أن أي عملية وصول لا تتم إلا بموافقته

الصريحة عبر العقود الذكية. كما يسمح للجهات المزودة مثل المختبرات الطبية بإرسال نتائج التحاليل مباشرة إلى السجل الطبي للمريض، في بيئة رقمية لامركزية وآمنة.

- **مكونات النظام الرئيسية (محدث)**

يتكوّن النظام من العقد التالية، والتي تمثل مختلف الجهات ضمن شبكة:Hyperledger Fabric

الجهة	الدور
المريض(Patient Node)	صاحب البيانات، يُخزّن ملفه الطبي فيLedger ، ويتحكم في مشاركته.
الطبيب(Doctor Node)	يرسل طلبات الوصول لبيانات المريض؛ لا يملك أي صلاحية افتراضية.
المستشفى (Hospital Node)	تمتلك عقدة بالشبكة، لكنها تؤدي دورًا إداريًا وقانونيًا فقط: التأكد من أن دخول الطبيب إلى حالة المريض قانوني (مثلاً أنه ضمن المستشفى). لا تملك حق الاطلاع على بيانات المريض.
شركات التأمين (Insurance Node)	تتحقق من الأهلية التأمينية وتقوم بالتسوية المالية دون الاطلاع على تفاصيل الملف الطبي.
المختبر(Lab Node)	يرفع نتائج الفحوصات مباشرة إلى سجل المريض عبر قناة خاصة معه فقط.
وزارة الصحة (Regulatory Node)	تمثل جهة إشرافية لتنظيم العمليات وضمان الامتثال القانوني.
Certificate Authority (CA)	تُصدر الهويات الرقمية وتُدير إدارة الدخول.(MSP)
Smart Contracts (Chaincode)	تدير كل السياسات (مشاركة البيانات، الموافقات، التسويات المالية، إلخ).
Private Channels	تُستخدم لتبادل البيانات بين المريض والطبيب فقط، لا المستشفى.

- **آلية عمل النظام**

تسلسل العمليات الرئيسية:

- **تسجيل المشاركين في النظام:**
  - ❖ تُصدر CA الشهادات الرقمية لجميع الأطراف.
  - ❖ المريض يُسجّل كمستخدم مستقل بهويته الرقمية(Digital Identity)
- **الإجراءات الإدارية (داخل المستشفى):**
  - ❖ المريض يزور المستشفى ويطلب مقابلة الطبيب.

❖ تقوم المستشفى بتوثيق الجلسة طبيًا وقانونيًا (إثبات أن الدكتور يحق له طلب بيانات).

❖ تُسجّل المعاملة داخل الشبكة، ولكن دون كشف بيانات المريض لأي طرف.

- **طلب الوصول من الطبيب:**

❖ بعد تسجيل دخوله كحالة رسمية، يرسل الطبيب طلبًا لرؤية السجل الطبي من المريض مباشرة.

❖ الطلب يُعالج من خلال عقد ذكي، ينتظر موافقة المريض.

- **موافقة المريض:**

❖ يتلقى المريض إشعارًا بطلب الوصول، ويقوم بتحديد:

- نوع البيانات التي يريد مشاركتها (تشخيصات، تحاليل، صور...).
- مدة السماح بالوصول (مثلاً 48 ساعة).

❖ يتم إنشاء قناة خاصة بين المريض والطبيب، ويُرسل الإذن عبر العقد الذكي.

- **المختبرات وشركات التأمين:**

❖ المختبر يُرسل النتائج إلى المريض فقط.

❖ شركة التأمين تتلقى "بيانات مختصرة غير سرية" من العقد الذكي، مثل:

- هل تم العلاج؟
- ما الإجراء؟
- هل هو مشمول بالتغطية؟

❖ ولا تتلقى أي بيانات صحية مباشرة.

- **وزارة الصحة:**

❖ يُسمح لها فقط بالاطلاع على بيانات تحليلية عامة (إحصائيات مشفّرة) لأغراض التخطيط، وليس ملفات فردية.

دراسة حالة افتراضية

- **السيناريو:**

المريض "سلمان" يزور مستشفى "النور"، ويطلب حجز موعد مع الدكتور "زياد" (اختصاصي قلب). قبل الزيارة، سلمان يريد أن يشاركه نتائج الفحوصات التي أجراها في مختبر مستقل.

- **تسلسل التفاعل:**

- **المستشفى** تُسجّل أن الدكتور زياد مُصرّح له بعلاج سلمان قانونيًا (دون الاطلاع على ملفه).
- **الطبيب زياد** يُرسل طلبًا لرؤية نتائج الفحوصات.
- **سلمان** يُوافق عبر تطبيق، ويحدد أنه يريد مشاركة "تحاليل الدم فقط."
- **العقد الذكي** يُفعّل قناة خاصة بين سلمان والدكتور زياد تحتوي فقط على بيانات التحاليل.
- **شركة التأمين** تتحقق من أن سلمان مغطى تأمينيًا، وتتم معالجة المطالبة تلقائيًا دون كشف بيانات.

فوائد النموذج المقترح

- **التحكم الكامل للمريض** في إدارة خصوصية ملفه الطبي.
- **أمان عالٍ** بفضل التشفير، العقود الذكية، وإدارة الهوية الرقمية.
- **شفافية** عبر سجل يُظهر كل عمليات الدخول والطلب.
- **مرونة المشاركة** حسب نوع البيانات والمدة الزمنية.
- **تكامل البيانات** من مصادر متعددة في مكان موحّد وموثوق.

العقود الذكية (Smart Contracts) في نموذج (Hyperledger Fabric)

- **دور العقود الذكية في النموذج**

العقود الذكية في Hyperledger Fabric المعروفة أيضًا باسم (Chaincode) تلعب دورًا جوهريًا في تنفيذ السياسات التي تحكم:

- تسجيل طلبات الوصول للبيانات من الأطباء.
- تخزين حالات الموافقة أو الرفض من المرضى.
- تمكين مشاركة بيانات محددة فقط بين المريض والطبيب.
- ضمان تسجيل كل عمليات الوصول والموافقات بشكل شفاف وغير قابل للتلاعب.
- دعم آليات سحب الإذن أو انتهاء الصلاحية.

- **أنواع العقود الذكية المستخدمة**

يمكن تقسيم العقود الذكية في النظام إلى:

نوع العقد	الوصف
AccessRequestContract	يدير طلبات الأطباء للوصول إلى السجلات الطبية، ويتابع حالات الموافقة.

نوع العقد	الوصف
DataSharingContract	يُنظّم مشاركة البيانات بين المريض والطبيب ضمن القنوات الخاصة.
AuditContract	يسجل عمليات الطلب والموافقة وسحب الإذن في الـ Ledger لأغراض التدقيق.
InsuranceContract	يدير التحقق من صلاحية التأمين دون الوصول للبيانات الصحية.

حدوديل الأمني للنموذج المقترح

- **متطلبات الأمان الأساسية**
  - **الخصوصية** :حماية بيانات المريض من الاطلاع غير المصرح به.
  - **التكامل** :ضمان عدم تعديل البيانات أو الطلبات بشكل غير قانوني.
  - **التوافر** :إمكانية الوصول إلى البيانات من قبل الأطراف المصرح لها.
  - **عدم الإنكار** :توثيق كل العمليات حتى لا يستطيع أي طرف إنكار قيامه بها.
- **كيف يحقق النظام هذه المتطلبات؟**

المتطلب	التنفيذ في النظام
الخصوصية	–مشاركة البيانات تتم فقط عبر **قنوات خاصة** بين المريض والطبيب. –العقد الذكي يدير موافقات المشاركة ولا يخزن البيانات الصحية نفسها. –نظام الهويات الرقمية (MSP) يتحكم في الوصول. –المستشفى وشركات التأمين ليس لديها وصول مباشر للبيانات.
التكامل	–كل طلب وصول وموافقة يُسجل في دفتر الحسابات الموزع (Ledger) الذي لا يمكن تغييره. –استخدام التوقيعات الرقمية في Hyperledger للتحقق من صحة المعاملات.
التوافر	–شبكة متعددة العقد (Nodes) توفر استمرارية الخدمة. –اعتماد آلية توافق (Consensus) تضمن صحة البيانات عبر الشبكة.
عدم الإنكار	–كل إجراء (طلب، موافقة، رفض) يتم تسجيله وتوقيعه رقمياً. –إمكانية التدقيق الكامل في سجلات النظام.

- **تهديدات أمنية محتملة وكيفية التعامل معها**

التهديد	التفسير	التدابير
تسريب البيانات	وصول غير مصرح به للسجلات الطبية	–التحكم الصارم في الوصول باستخدام العقود الذكية. –استخدام التشفير أثناء التخزين والنقل. –مشاركة البيانات فقط بعد موافقة صريحة من المريض.
انتحال الهوية	هجوم يزعم أنه طبيب أو مريض	–استخدام شهادات رقمية صادرة عن CA موثوقة. –آليات تحقق متعددة العوامل في الدخول.
التلاعب بالبيانات	محاولة تعديل بيانات المريض أو الموافقات	–البلوك تشين يمنع تعديل المعاملات السابقة. –العقود الذكية تتحقق من صحة الطلبات.
رفض الخدمة(DoS)	محاولة تعطيل الشبكة أو العقد	–تصميم النظام لدعم التكرار والتحميل. –استخدام آليات كشف ومنع الهجمات.

- **الالتزام بالمعايير والقوانين**
  - التزام النموذج بمعايير الخصوصية مثل **(HIPAA)** للولايات المتحدة أو **(GDPR)** للأوروبيين.
  - ضمان حق المريض في التحكم الكامل ببياناته.
  - توثيق العمليات الإدارية والقانونية بواسطة المستشفى وشركات التأمين ووزارة الصحة.

التحليل الأمني للنموذج المقترح(Security Analysis)

- **التهديدات الأمنية المحتملة**

عند تصميم نظام لإدارة السجلات الطبية الحساسة باستخدام البلوك تشين، يجب التعامل مع عدد من التهديدات المحتملة، منها:

التهديد	التأثير
الوصول غير المصرح به	خرق خصوصية بيانات المريض.
تزييف الموافقة	مشاركة بيانات دون إذن المريض.
هجمات الطرف الداخلي	إساءة استخدام الصلاحيات من قبل طبيب أو موظف.
تحليل البيانات المجمعة	التتبع والتحليل غير المصرح به للبيانات عبر السجل.
الهجمات على القنوات الخاصة	اختراق الاتصالات الآمنة بين الأطراف.
هجمات على العقود الذكية	استغلال ثغرات برمجية داخل الـchaincode.

آليات الحماية فيHyperledger Fabric

نموذج Hyperledger Fabric المستخدم يقدم ميزات أمنية على عدة مستويات:

- **إدارة الهوية(Identity Management)**
  - لكل طرف هوية رقمية فريدة عبر شهادات.X.509
  - يتم التحقق من هوية المتصل قبل أي عملية عبر .(Membership Service Provider) MSP
- **التحكم في الوصول(Access Control)**
  - يتم تحديد السياسات بدقة.(Access Control Lists – ACL)
  - يُمنح الطبيب حق الوصول فقط بعد موافقة المريض الموقعة رقميًا.
- **التشفير**
  - تشفير البيانات أثناء النقل.(TLS)
  - تشفير البيانات على السجل باستخدام تشفير غير متماثل.(Asymmetric Encryption)
- **القنوات الخاصة(Private Channels)**
  - البيانات لا تُشارك على مستوى الشبكة الكاملة.
  - كل قناة محددة بين أطراف مصرح لها فقط.
- **العقود الذكية المؤمنة**
  - كتابة العقود وفق أفضل الممارسات.
  - استخدام اختبارات وحدات (Unit Tests) وفحص الثغرات.
  - مراقبة الأحداث لتتبع أي سلوك غير طبيعي.

التحكم في الموافقات بخطوات الحماية:

- الطبيب يقدم طلبًا رقميًا موقعًا.
- المريض يتلقى إشعارًا ويقوم بالموافقة من خلال توقيع رقمي.
- العقد الذكي يتحقق من صلاحية التوقيع وتاريخ الصلاحية.
- يتم تسجيل جميع العمليات في دفتر السجل (Ledger) للرجوع والتحقيق لاحقًا.

- **تدقيق الأمان المستمر**
  - مراقبة الشبكة وتسجيل الأحداث باستخدام أدوات مثل **Prometheus**و.**ELK Stack**
  - إجراء اختبارات اختراق دورية (Penetration Testing) على الـ APIs والعقود الذكية.
  - تحديث دوري للهويات والشهادات الرقمية.
- **نقاط الضعف المحتملة**

نقطة الضعف	التخفيف المقترح
خطأ بشري من المستخدم	واجهات استخدام سهلة وتنبيهات للموافقات.
ثغرات في العقود الذكية	مراجعات أكواد وتحليل ثابت.(Static Code Analysis)
إساءة استخدام الوصول القانوني	نظام تنبيهات وتحقيقات دورية.
فقدان الجهاز أو المفاتيح	استخدام أنظمة مصادقة متعددة العوامل.(MFA)

الأبعاد الأخلاقية

- **احترام خصوصية المريض وحقوقه**
  - **التحكم الكامل للمريض في بياناته** يعزز حقه في الخصوصية والكرامة الإنسانية.
  - تمكين المريض من اختيار من يشاهد بياناته، ومتى، ولمدة كم، يدعم مبدأ **الموافقة المستنيرة.**
  - تقليل مخاطر **الإفشاء غير المصرح به** أو استغلال المعلومات الطبية الشخصية.
- **العدالة في الوصول إلى الرعاية**
  - النموذج يضمن أن مشاركة البيانات لا تُستخدم لتفرقة أو تمييز ضد المريض.
  - يجب التأكد من أن جميع المرضى، بغض النظر عن خلفياتهم، يمكنهم استخدام النظام بسهولة.

الشفافية والمساءلة

- تسجيل كل عمليات الوصول والموافقة يُسهم في **المساءلة**، مما يحمي المريض ويعزز الثقة.
- الجهات الإدارية (المستشفى، التأمين، وزارة الصحة) مسؤولة عن ضمان تطبيق السياسات دون تجاوز.

الأبعاد القانونية

- **الامتثال للقوانين واللوائح**
  - يلتزم النظام بقوانين حماية البيانات الشخصية مثل:

- ❖ **HIPAA** في الولايات المتحدة.
- ❖ **GDPR** في الاتحاد الأوروبي.
- ❖ قوانين حماية البيانات المحلية حسب البلد.

- ضمان توثيق موافقة المريض قانونيًا لتبادل البيانات.

- **الإطار القانوني للموافقة وإدارة البيانات**
  - موافقة المريض يجب أن تكون (صريحة، قابلة للإثبات، قابلة للسحب في أي وقت).
  - العقود الذكية تعمل كآليات تنفيذية للالتزام بالموافقة القانونية.
- **حماية البيانات من التلاعب والاختراق**
  - اعتماد تقنية البلوك تشين يمنح ضمانات ضد التلاعب بالبيانات.
  - مسؤولية الجهات الإدارية مراقبة الأنشطة وتنفيذ العقوبات القانونية في حال الانتهاكات.
- **الأدوار والمسؤوليات القانونية**

الجهة	المسؤوليات القانونية
المريض	إدارة صلاحيات الوصول لبياناته.
الطبيب	استخدام البيانات وفق الغرض المصرح.
المستشفى	التأكد من صحة الإجراءات الإدارية والوثائق القانونية.
شركات التأمين	معالجة المطالبات بما يتوافق مع بيانات الموافقة.
وزارة الصحة	مراقبة النظام والامتثال القانوني العام.

- **التحديات القانونية المحتملة**
  - تعريف قانوني دقيق لمسؤولية كل طرف عند حدوث خرق للبيانات.
  - التعامل مع اختلاف القوانين عبر الحدود إذا كان النظام يعمل على نطاق دولي.
  - تحديث القوانين لتواكب تقنيات العقود الذكية والبلوك تشين.

المناقشة (Discussion)

يمثل النموذج المقترح نقلة نوعية في كيفية التعامل مع السجلات الطبية الإلكترونية، حيث يدمج بين **البلوك تشين** كإطار موثوق و**العقود الذكية** كأداة ديناميكية للتحكم في الأذونات.

من خلال مراجعة الأدبيات السابقة، يتضح أن معظم الحلول التقليدية تعاني من ثلاث مشكلات رئيسية:

- **مركزية التخزين** :مما يجعل النظام عرضة للاختراق أو فقدان البيانات.
- **ضعف التحكم في الخصوصية** :حيث غالبًا ما تُدار بيانات المرضى من قبل المؤسسات الطبية دون إشراك فعلي للمريض.
- **محدودية الشفافية** :إذ يصعب تتبع من قام بالوصول إلى البيانات وفي أي وقت.

النموذج المقترح يقدم إجابة عملية لهذه التحديات عبر:

- توفير **بنية موزعة** تعتمد على Hyperledger Fabric تقلل من مخاطر المركزية.
- تعزيز **دور المريض** ليصبح هو صاحب القرار الأول في مشاركة بياناته.
- تسجيل كل المعاملات على **سجل موزع غير قابل للتلاعب**، مما يزيد من الشفافية والمساءلة.

كما أن الاعتماد على **القنوات الخاصة** يضمن حماية البيانات الحساسة من الانتشار غير الضروري، بينما تسمح العقود الذكية بتخصيص الأذونات بناءً على الغرض والمدة، وهو ما يعكس مرونة النموذج.

الاستنتاجات والتوصيات(Conclusion and Recommandations)

- **تلخيص للنموذج والمزايا الأساسية**

في هذه الورقة قدمنا نموذجًا لتجميع السجل الطبي للمرضى باستخدام تقنية البلوك تشين عبر منصة **Hyperledger Fabric**، مع تركيز خاص على منح المريض السيطرة الكاملة على بياناته من خلال نظام موافقات مبني على العقود الذكية.

المزايا الأساسية للنموذج:

- **تحكم دقيق للمرضى** في من يمكنه الاطلاع على بياناتهم الطبية.
- **مشاركة البيانات الآمنة** عبر قنوات خاصة تضمن الخصوصية والسرية.
- **سجلات غير قابلة للتلاعب** لجميع عمليات الوصول والموافقات.
- **دور إداري وقانوني واضح** للمستشفيات وشركات التأمين ووزارة الصحة، دون الاطلاع المباشر على البيانات الصحية.
- **تعزيز الثقة والشفافية** بين جميع الأطراف المعنية.

- **الدروس المستفادة**
  - استخدام **العقود الذكية** يقلل الأخطاء البشرية ويسهل عمليات الموافقة القانونية.
  - تقنية **Hyperledger Fabric**توفر إطار عمل قابل للتوسع وآمن لإدارة السجلات الطبية.
  - توزيع المسؤوليات بين الجهات الإدارية والقانونية يضمن الامتثال للقوانين واللوائح.
  - تحديات الخصوصية يمكن معالجتها بفعالية من خلال القنوات الخاصة والتحكم في الوصول.
- **اقتراحات للتطوير أو الاختبار العملي**
  - إجراء **اختبارات ميدانية** في مستشفيات فعلية للتحقق من كفاءة النظام وملاءمته للبيئة العملية.
  - تطوير واجهات مستخدم سهلة ومرنة للمرضى والأطباء لإدارة الموافقات بسلاسة.
  - دمج تقنيات الذكاء الاصطناعي لتحليل سلوكيات الوصول وتنبيه الحالات غير العادية.
  - توسيع النظام ليشمل **الطوارئ الطبية** حيث يمكن مشاركة البيانات بشكل فوري مع إشعارات لاحقة للمريض.
  - دراسة الأداء عند استخدام النظام على نطاق جغرافي أوسع مع متطلبات تشريعية مختلفة.
- **التوصية بمزيد من الأبحاث**
  - البحث في تحسين آليات **إدارة الهوية الرقمية** وربطها بالأنظمة الحكومية والصحية.
  - دراسة تأثير استخدام **تقنيات التشفير المتقدمة** مثل التشفير التفاضلي أو التشفير متعدد الأطراف لتحسين الخصوصية.
  - استكشاف دمج تقنيات البلوك تشين مع قواعد البيانات التقليدية لتحقيق توازن بين الأداء والخصوصية.
  - تقييم استخدام العقود الذكية في حالات الاستخدام المختلفة مع تحليلات مخاطر موسعة.

شكر وتقدير (Acknowledgments)

أتقدم بجزيل الشكر والعرفان إلى كل من ساهم في دعم هذا البحث، سواء من الناحية الأكاديمية أو التقنية.أخص بالشكر مشرفي الأكاديمي د. جمعة إبراهيم على توجيهاته، كما أشكر الزملاء والمختصين الذين ساهموا بآرائهم البنّاءة خلال إعداد هذا النموذج. ولا يفوتني تقديم الامتنان لعائلتي على دعمهم المتواصل.

مراجع أساسية حول البلوك تشين والرعاية الصحية (References):

(Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act drove large gains in hospital electronic health record adoption. *Health Affairs, 36*(8), 1416–1422. https://doi.org/10.1377/hlthaff.2016.1651

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences, 9*(9), 1736. https://doi.org/10.3390/app9091736

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the 13th EuroSys Conference*, 1–15. https://doi.org/10.1145/3190508.3190538

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes, 10*(9), e003800. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. https://doi.org/10.1109/OBD.2016.11

Hyperledger Foundation. (2023). *Hyperledger Fabric documentation*. https://hyperledger-fabric.readthedocs.io/

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Nguyen, L., Bellucci, E., & Nguyen, L. T. (2014). Electronic health records implementation: An evaluation of information system impact and contingency

factors. *International Journal of Medical Informatics, 83*(11), 779–796. https://doi.org/10.1016/j.ijmedinf.2014.06.011

Nguyen, D. C., Raza, S., & Saad, W. (2014). A survey on healthcare data: Challenges and solutions with blockchain. *Journal of Network and Computer Applications, 105*, 1–20. https://doi.org/10.1016/j.jnca.2018.04.011

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017). Towards using blockchain technology for eHealth data access management. *IEEE International Conference on Services Computing (SCC)*, 193–200. https://doi.org/10.1109/SCC.2017.34

Roehrs, A., da Costa, C. A., da Rosa Righi, R., & de Oliveira, K. S. F. (2017). Personal health records: A systematic literature review. *Journal of Medical Internet Research, 19*(1), e13. https://doi.org/10.2196/jmir.5876

Roehrs, A., da Costa, C. A., da Rosa Righi, R., & da Silva, V. F. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics, 71*, 70–81. https://doi.org/10.1016/j.jbi.2017.05.012

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647