

قضايا بحثية 3

مهمة الأسبوع الثامن

إعداد الطالب :

فهد بن صالح السعوي
242001442



أثر تطبيق تقنية سلاسل الكتل
(Blockchain) في مشاركة البيانات
الصحية على خفض مخاطر الخصوصية
وتسرب البيانات: دراسة تحليلية تطبيقية



المقدمة

يُمثّل التحول الرقمي في القطاع الصحي أحد أبرز الملامح المعاصرة للثورة الصناعية الرابعة، حيث أصبحت البيانات الصحية تُشكّل شريان الحياة لمنظومة الرعاية الصحية الحديثة بما تتضمنه من سجلات طبية إلكترونية ونتائج فحوصات مخبرية وصور أشعة وبيانات أجهزة المراقبة عن بُعد وغيرها من المعلومات الحساسة التي تتدفق باستمرار بين المؤسسات الصحية المختلفة. وقد فرض هذا الواقع الرقمي المتنامي حاجة ملحة إلى مشاركة هذه البيانات بين المستشفيات والمراكز البحثية والجهات التنظيمية وشركات التأمين لتحقيق تكامل الرعاية الصحية وتحسين جودة القرارات العلاجية، غير أن هذه المشاركة المتزايدة أفرزت في المقابل تحديات جوهرية تتعلق بأمن البيانات وحماية خصوصية المرضى في ظل اعتماد معظم المؤسسات الصحية على أنظمة مركزية تقليدية لم تُصمّم أصلاً لمواكبة هذا الحجم المتصاعد من تبادل البيانات. (Yaqoob et al., 2022)

المقدمة

و برزت تقنية سلاسل الكتل (Blockchain) بوصفها إحدى أكثر التقنيات الناشئة إثارة للاهتمام في مجال إدارة البيانات الصحية، إذ تقوم فلسفتها على مبدأ اللامركزية في تخزين البيانات ومعالجتها عبر شبكة موزعة من العقد تُسجل المعاملات في سجل رقمي غير قابل للتعديل ومحمي بتقنيات تشفير متقدمة. وتتميز هذه التقنية بخصائص جوهرية تجعلها ملائمة للسياق الصحي، من أبرزها التشفير اللامركزي الذي يُوزع البيانات عبر شبكة واسعة بدلاً من تخزينها في نقطة واحدة، والعقود الذكية التي تُؤتمت عمليات التحكم في الوصول وفق قواعد محددة مسبقاً دون الحاجة إلى وسطاء، وخاصية عدم قابلية التعديل التي تحفظ سلامة السجلات من أي تلاعب، فضلاً عن آليات إدارة الموافقة التي تمنح المرضى سيطرة مباشرة على بياناتهم (عبدالمحسن وآخرون ، 2023)

المقدمة

ولقد شهدت التطبيقات العملية لتقنية سلاسل الكتل في المجال الصحي اهتماماً بحثياً متزايداً على المستوى الدولي، حيث استُكشفت إمكانياتها في تأمين تبادل المعلومات الصحية بين المؤسسات المختلفة، وتمكين المرضى من التحكم في بياناتهم ومنح أو سحب صلاحيات الوصول بشكل فوري وشفاف، وتعزيز التشغيل البيئي بين الأنظمة الصحية المتباينة دون المساس بسرية المعلومات. كما أثبتت الدراسات أن دمج تقنيات التشفير المتقدمة مع البنية اللامركزية لسلاسل الكتل يُمكنه أن يُعيد تشكيل نماذج حماية السجلات الصحية من خلال توفير حماية شاملة من طرف إلى طرف تشمل مراحل التخزين والنقل والمعالجة (Vanin et al., 2022).

تُعدّ مخاطر الخصوصية وتسرب البيانات الصحية من أخطر التهديدات التي تواجه المنظومة الصحية الرقمية المعاصرة، إذ تتسم البيانات الصحية بحساسية استثنائية كونها تتضمن معلومات شخصية وطبية ونفسية ومالية يُمكن أن يؤدي كشفها إلى أضرار بالغة بالمرضى تتراوح بين الضرر المعنوي والتمييز في التأمين والتوظيف والابتزاز الإلكتروني. وتتنوع مصادر هذه المخاطر بين الهجمات السيبرانية الخارجية والتهديدات الداخلية الناجمة عن سوء استخدام صلاحيات الوصول ونقاط الضعف في البنى المركزية التقليدية التي تجعل من قواعد البيانات الموحدة هدفاً مغرياً للمهاجمين (Adeghe et al., 2024).

المقدمة

تتجه هذه الدراسة إلى استقصاء أثر تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية بأبعاده الأربعة على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية، ساعيةً إلى تقديم إسهام علمي وعملي يُثري الأدبيات العربية في هذا المجال البحثي الناشئ ويُزوّد صنّاع القرار في القطاع الصحي السعودي برؤى مبنية على أدلة بحثية حول جدوى تبني هذه التقنية الواعدة في حماية البيانات الصحية وتعزيز خصوصية المرضى .

مشكلة الدراسة

يشهد القطاع الصحي على المستوى العالمي والمحلي تحولاً رقمياً متسارعاً أفضى إلى تضاعف حجم البيانات الصحية المتولّدة والمتبادلة بين المؤسسات الصحية بصورة غير مسبقة، إذ تُشير تقارير المنتدى الاقتصادي العالمي إلى أن القطاع الصحي يُنتج ما يقارب 30% من إجمالي حجم البيانات العالمية، مع توقعات بأن يصل معدل النمو السنوي المركّب لهذه البيانات إلى 36% بحلول عام 2025. وقد أدّى هذا التضخم الهائل في البيانات الصحية، المقترن بتزايد الحاجة إلى مشاركتها بين المستشفيات والمراكز البحثية وشركات التأمين والجهات التنظيمية، إلى تصاعد مخاطر الخصوصية وتسرب البيانات بشكل يندّر بتهديدات جسيمة تطلّ سلامة المرضى وسرية معلوماتهم وثقتهم في المنظومة الصحية برمتها.

مشكلة الدراسة

وتكشف الإحصاءات الدولية عن خطورة هذا الواقع، حيث أظهر تقرير IBM Security العام 2024 أن متوسط تكلفة اختراق البيانات في القطاع الصحي بلغ نحو 10.93 مليون دولار أمريكي لكل حادثة، وهو الأعلى بين جميع القطاعات للعام الرابع عشر على التوالي. كما وثّق مكتب الحقوق المدنية التابع لوزارة الصحة والخدمات الإنسانية الأمريكية أكثر من 725 حادثة اختراق كبيرة للبيانات الصحية خلال عام 2023 وحده، أثرت على أكثر من 133 مليون سجل صحي. وعلى المستوى المحلي، فإن المملكة العربية السعودية ليست بمعزل عن هذه التحديات، إذ تُصنّف ضمن الدول الأكثر استهدافاً بالهجمات السيبرانية في منطقة الشرق الأوسط، وقد نبّهت الهيئة الوطنية للأمن السيبراني في تقاريرها إلى تصاعد التهديدات الموجهة للقطاع الصحي السعودي، لا سيما في ظل التوسع المتسارع في رقمنة الخدمات الصحية تنفيذاً لمستهدفات رؤية المملكة 2030 وبرنامج التحول الصحي.

مشكلة الدراسة

وتتمحور جذور هذه المشكلة في أن أنظمة إدارة البيانات الصحية التقليدية تعتمد في معظمها على بنى مركزية تُخزن البيانات في قواعد بيانات موحّدة، مما يجعلها عرضة لنقطة فشل واحدة تُتيح للمهاجمين الوصول إلى كميات ضخمة من البيانات الحساسة في حادثة اختراق واحدة. كما أن آليات التحكم في الوصول وإدارة صلاحيات المشاركة في هذه الأنظمة غالباً ما تفتقر إلى الشفافية والمرونة الكافية، حيث لا يملك المرضى سيطرة فعلية على بياناتهم ولا يمكنهم تتبّع من يصل إليها أو يتداولها. ويزداد هذا الوضع تعقيداً مع غياب آليات موحّدة لضمان سلامة البيانات وعدم التلاعب بها أثناء عمليات النقل والمشاركة بين المؤسسات الصحية المتعددة، فضلاً عن ضعف أنظمة إدارة الموافقة التي تُعاني من بطء الإجراءات وعدم القدرة على التحقق التلقائي من صلاحيات الوصول.

مشكلة الدراسة

وعليه، تتبلور مشكلة الدراسة في السؤال الجوهرى التالي: ما أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية؟

أسئلة الدراسة

ما أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية؟

الأسئلة الفرعية:

ما أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

ما أثر العقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

ما أثر سلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

ما أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

أهداف الدراسة

تهدف هذه الدراسة إلى التعرف على أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية.

ويتفرع من هذا الهدف الرئيسي الأهداف الفرعية التالية:

التعرف على أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

التعرف على أثر العقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

التعرف على أثر سلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

التعرف على أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

تقديم إطار مقترح لتبني تقنية سلاسل الكتل في مشاركة البيانات الصحية بما يُعزّز حماية الخصوصية ويُخفّض مخاطر تسرب البيانات في المؤسسات الصحية السعودية.

أهمية الدراسة

أهمية علمية

- تُسهم هذه الدراسة في سدّ فجوة واضحة في الأدبيات العربية التي تفتقر إلى دراسات تربط بين تقنية سلاسل الكتل ومشاركة البيانات الصحية في إطار تحليلي متكامل، إذ تُعدّ من الدراسات العربية الأولى التي تتناول هذا الموضوع بأبعاده الأربعة مجتمعة في السياق الصحي.
- تُقدّم الدراسة إطاراً مفاهيمياً يجمع بين أبعاد تقنية سلاسل الكتل (التشفير اللامركزي، العقود الذكية، سلامة البيانات، إدارة الموافقة (وعلاقتها بخفض مخاطر الخصوصية وتسرب البيانات، مما يُوفّر أساساً نظرياً يمكن للباحثين البناء عليه في دراسات مستقبلية).
- تُسهم الدراسة في تعميق الفهم العلمي لكيفية تأثير الخصائص الجوهرية لتقنية البلوكتشين (كاللامركزية وعدم قابلية التعديل) على حماية البيانات الصحية من الاختراقات والتسريبات.
- تُضيف الدراسة إلى المعرفة العلمية من خلال استكشاف التحديات الواقعية التي تواجه تطبيق تقنية سلاسل الكتل في القطاع الصحي، بما يُمكن الباحثين من تحديد الثغرات البحثية واقتراح حلول مبتكرة.

أهمية الدراسة

الأهمية التطبيقية:

- تُوفّر الدراسة نتائج وتوصيات عملية يُمكن لصنّاع القرار في القطاع الصحي السعودي الاستفادة منها في اتخاذ قرارات مدروسة بشأن تبني تقنية سلاسل الكتل لتعزيز حماية البيانات الصحية.
- تتوافق الدراسة مع مستهدفات رؤية 2030 في التحول الرقمي للقطاع الصحي، حيث تُقدّم رؤية حول كيفية الاستفادة من التقنيات الناشئة في تحسين أمن البيانات الصحية وحماية خصوصية المرضى.
- تُقدّم الدراسة إرشادات عملية تُساعد المؤسسات الصحية على الامتثال لمتطلبات نظام حماية البيانات الشخصية الصادر في المملكة العربية السعودية من خلال تبني حلول تقنية متقدمة.
- تُسهم نتائج الدراسة في توعية المؤسسات الصحية بالأثر الاقتصادي لتسرب البيانات الصحية وتقديم حلول تقنية قائمة على البلوكتشين لخفض هذه التكاليف والمخاطر القانونية.

فروض الدراسة

يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده مجتمعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية.

الفروض الفرعية:

الفرض الفرعي الأول: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للتشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الثاني: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للعقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الثالث: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لسلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الرابع: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لآليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

المنهجية وطرق البحث

ستعتمد هذه الدراسة على المنهج الوصفي التحليلي باعتباره المنهج الأكثر ملاءمة لطبيعة الدراسة وأهدافها، إذ يُتيح وصف الظاهرة موضع الدراسة وصفاً دقيقاً وتحليل العلاقات بين متغيراتها تحليلاً كمياً. ويُعدّ هذا المنهج مناسباً لقياس أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده الأربعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية، وذلك من خلال جمع البيانات من مصادرها الأولية وتحليلها إحصائياً للوصول إلى نتائج قابلة للتعميم.

مصادر جمع البيانات

ستعتمد الدراسة على نوعين من مصادر جمع البيانات:

المصادر الثانوية: وتشمل الكتب والمراجع العلمية المتخصصة، والدوريات والمجلات العلمية المحكمة العربية والأجنبية، والرسائل الجامعية (ماجستير ودكتوراه)، وأبحاث المؤتمرات العلمية، وقواعد البيانات الإلكترونية مثل (دار المنظومة، Scopus، Web of Science، PubMed، IEEE Xplore)، والتقارير والوثائق الرسمية الصادرة عن وزارة الصحة السعودية والمركز الوطني للمعلومات الصحية والهيئة الوطنية للأمن السيبراني. وستُستخدم هذه المصادر في بناء الإطار النظري وتحديد أبعاد المتغيرات وتطوير أداة الدراسة.

المصادر الأولية: وتتمثل في الاستبانة الإلكترونية التي ستُصمّم خصيصاً لهذه الدراسة وتُوزّع على أفراد العينة لجمع

أدوات الدراسة

ستُصمَّم استبانة إلكترونية بوصفها الأداة الرئيسية لجمع البيانات الأولية، وستتكون من ثلاثة أقسام رئيسية:

القسم الأول: البيانات الديموغرافية

ويتضمن المتغيرات الشخصية والوظيفية لأفراد العينة (المؤهل العلمي، سنوات الخبرة، طبيعة الوظيفة، حجم المؤسسة الصحية).

القسم الثاني: المتغير المستقل — تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية ويتكون من أربعة أبعاد تشمل (16)

فقرة

القسم الثالث: المتغير التابع — خفض مخاطر الخصوصية وتسرب البيانات

وهو محور أحادي يتكون من (10) فقرات تقيس مستوى خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية.

إجمالي فقرات الاستبانة: (26) فقرة، بالإضافة إلى فقرات البيانات الديموغرافية.

وسيُستخدم مقياس ليكرت الخماسي (Likert Scale) لقياس استجابات أفراد العينة، وفقاً للتدرج التالي: (موافق بشدة = 5، موافق = 4،

محايد = 3، غير موافق = 2، غير موافق بشدة = 1).

مجتمع وعينة الدراسة

سيتكون مجتمع الدراسة من جميع العاملين في مجالات تقنية المعلومات والأمن السيبراني وإدارة البيانات الصحية والسجلات الطبية الإلكترونية في المؤسسات الصحية الحكومية والخاصة بالمملكة العربية السعودية، وتحديداً في المستشفيات الكبرى ومراكز المعلومات الصحية التابعة لوزارة الصحة والمركز الوطني للمعلومات الصحية (NPHIES) ومستشفيات الشؤون الصحية بالحرس الوطني ومستشفيات القطاع الخاص الكبرى. ويُقدّر حجم مجتمع الدراسة بنحو (4,500) متخصص يعملون في هذه المجالات وفقاً للبيانات المتاحة من وزارة الصحة السعودية والهيئة السعودية للتخصصات الصحية، ممن يمتلكون معرفة مباشرة بأنظمة إدارة البيانات الصحية وإجراءات مشاركتها وحمايتها.

مجتمع وعينة الدراسة

ونظراً لصعوبة حصر جميع أفراد مجتمع الدراسة والوصول إليهم، ستعتمد الدراسة على أسلوب العينة العشوائية التطبيقية النسبية لضمان تمثيل متوازن لفئات المجتمع المختلفة (حسب نوع المؤسسة الصحية وطبيعة الوظيفة والمنطقة الجغرافية). وسيتم تحديد حجم العينة وفقاً لمعادلة ستيفن ثومبسون (Steven Thompson للمجتمعات المحدودة، حيث يُقدّر الحد الأدنى لحجم العينة بنحو (354) مفردة عند مستوى ثقة 95% وهامش خطأ 5%. وستسعى الدراسة إلى توزيع (420) استبانة لتعويض نسبة الاستبانات غير المستردة أو غير الصالحة للتحليل، بحيث يُستهدف الحصول على (354) استبانة صالحة كحد أدنى لضمان التمثيل الإحصائي الملائم..

حدود الدراسة

- الحدود الموضوعية: ستقتصر الدراسة على قياس أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده الأربعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات.
- الحدود المكانية: ستُطبَّق الدراسة على المؤسسات الصحية الحكومية والخاصة في المملكة العربية السعودية، وتحديدًا المستشفيات الكبرى ومراكز المعلومات الصحية في مناطق الرياض وجدة والدمام.
- الحدود الزمانية: ستُجرى الدراسة الميدانية خلال الفصل الدراسي الثاني من العام الجامعي 1447/1448 هـ الموافق 2025/2026 م.

الأساليب الإحصائية المستخدمة

- ستُحلَّل البيانات باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS V.26) وبرنامج (4 SmartPLS لنمذجة المعادلات البنائية، وسيتم توظيف الأساليب الإحصائية التالية:
- التحليل الوصفي: التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لوصف خصائص العينة واتجاهات الاستجابات.
- اختبارات الصدق والثبات: معامل ألفا كرونباخ (Cronbach's Alpha) لقياس ثبات أداة الدراسة، والصدق الظاهري (عرض الاستبانة على محكِّمين متخصصين)، وصدق الاتساق الداخلي (معامل ارتباط بيرسون) للتحقق من صدق البناء.
- تحليل الانحدار المتعدد (Multiple Regression Analysis): لاختبار أثر أبعاد المتغير المستقل مجتمعة ومنفردة على المتغير التابع واختبار الفروض الأربعة الأولى.
- معامل الارتباط (Pearson Correlation): لقياس قوة واتجاه العلاقة بين المتغيرات المستقلة والمتغير التابع.
- معامل تضخم التباين (VIF) واختبار التباين المسموح (Tolerance) للتحقق من عدم وجود ازدواجية خطية بين المتغيرات المستقلة.
- تحليل التباين الأحادي (One-Way ANOVA): لاختبار الفروق في استجابات أفراد العينة تبعاً للمتغيرات الديموغرافية متعددة المستويات (سنوات الخبرة، حجم المؤسسة).

الدراسات السابقة

دراسة (العنزي والرابغي، 2025): حماية المعرفة في المدن الصحية الذكية بين مشاركة البيانات وضمان الأمن والخصوصية.

هدفت الدراسة إلى التعرف على واقع حماية المعرفة في المدن الصحية الذكية بأبعاده (مشاركة البيانات الصحية، أمن المعلومات الصحية، خصوصية البيانات) وتأثيرها على تحقيق التوازن بين إتاحة البيانات للمستخدمين وحمايتهم من المخاطر الأمنية في بيئة المدن الذكية. واستخدمت الدراسة المنهج الوصفي التحليلي لتحليل الأدبيات والدراسات المتعلقة بالموضوع. وتوصلت نتائج الدراسة إلى أن المدن الصحية الذكية تواجه تحديات جوهرية في تحقيق التوازن بين مشاركة البيانات الصحية وضمان أمنها وخصوصيتها، وأن التقنيات الحديثة مثل التشفير والبلوكشين تُسهم في تعزيز حماية المعرفة الصحية، غير أن غياب الأطر التنظيمية الموحدة يُشكّل عائقاً أمام تحقيق الحماية الشاملة. وأوصت الدراسة بضرورة تطوير سياسات واضحة ومتكاملة لحماية البيانات الصحية في المدن الذكية، وتبني الحلول التقنية المتقدمة القائمة على التشفير والبلوكشين، وتعزيز التعاون بين الجهات الصحية والتقنية لتحقيق مشاركة آمنة وفعّالة للبيانات.

الدراسات السابقة

دراسة (السلمي، 2022): واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بالمملكة العربية السعودية.

هدفت الدراسة إلى التعرف على واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بأبعاده (البنية التحتية للبيانات، آليات التكامل، تحديات الإدارة) ومدى قدرته على تحقيق تكامل فعّال في إدارة المعلومات الصحية في المملكة العربية السعودية . واستخدمت الدراسة منهج دراسة الحالة لتحليل واقع التكامل في المركز الوطني للمعلومات الصحية. وتوصلت نتائج الدراسة إلى أن المركز الوطني يبذل جهوداً ملموسة في تكامل البيانات الصحية الضخمة من مصادر متعددة، إلا أنه يواجه تحديات تتعلق بتوحيد المعايير بين المؤسسات الصحية المختلفة، وضمان جودة البيانات وسلامتها، فضلاً عن التحديات المتعلقة بالخصوصية والأمن. وأوصت الدراسة بتطوير أطر تنظيمية موحدة لتكامل البيانات الصحية، وتبني تقنيات متقدمة لضمان جودة البيانات وحمايتها، وتعزيز التعاون بين الجهات الصحية المختلفة لتحقيق تكامل شامل.

الدراسات السابقة

دراسة (المزيد، 2024): واقع استخدام سلاسل الكتل "Block Chain" في المصارف السعودية: دراسة حالة مصرف الراجحي.

هدفت الدراسة إلى التعرف على واقع استخدام تقنية سلاسل الكتل في المصارف السعودية بأبعاده (الشفافية، أمان المعاملات، كفاءة العمليات المصرفية) وذلك من خلال دراسة حالة مصرف الراجحي. واستخدمت الدراسة منهج دراسة الحالة القائم على التحليل الوصفي. وتوصلت نتائج الدراسة إلى أن تطبيق تقنية البلوكتشين في المصارف يُسهم في زيادة شفافية وأمان المعاملات المالية وتحسين كفاءة العمليات المصرفية، كما تُسهّل عمليات التحويل وتخفض التكاليف عبر القضاء على الوساطة في القطاع المصرفي، فضلاً عن مساهمتها في حماية البيانات وتعزيز موثوقية مجال إنترنت الأشياء. وأوصت الدراسة بتكثيف الجهود والأبحاث لتطوير هذه التقنية وتكييفها مع المصارف الإسلامية وفق مبادئ الشريعة الإسلامية، والاهتمام بإيجاد حلول للتحديات التي تواجه تطبيقها.

الدراسات السابقة

دراسة (الضعيلة وعوض، 2024): أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية.

هدفت الدراسة إلى التعرف على أثر استخدام تقنية سلاسل الكتل بأبعاده (اللامركزية، التشفير، العقود الذكية، الشفافية) على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من العاملين في الإدارات ذات الصلة بسلاسل التوريد وتكنولوجيا المعلومات في شركات الأدوية الأردنية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية لاستخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد، حيث تسهم في تعزيز الشفافية وتتبع المنتجات الدوائية وخفض مخاطر التزوير والتلاعب. وأوصت الدراسة بضرورة تبني شركات الأدوية لتقنية البلوكتشين لتحسين كفاءة سلاسل التوريد، وتطوير البنية التحتية التقنية اللازمة، وتدريب الكوادر البشرية على استخدام هذه التقنية.

دراسة (Adeghe, Okolo & Ojeyinka, 2024): Evaluating the Impact of Blockchain Technology in Healthcare Data Management: A Review of Security, Privacy, and Patient Outcomes.

هدفت الدراسة إلى التعرف على أثر تقنية البلوكتشين في إدارة البيانات الصحية بأبعاده (أمن البيانات وسلامتها، خصوصية المرضى والتحكم في بياناتهم، التشغيل البيئي وتحسين نتائج المرضى (وتقييم إمكانياتها التحويلية في قطاع الرعاية الصحية. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة المنهجية للأدبيات ودراسات الحالة الواقعية. وتوصلت نتائج الدراسة إلى أن تقنية البلوكتشين تضمن سلامة البيانات وعدم قابليتها للتغيير من خلال الهياكل اللامركزية والعقود الذكية، كما تمنح المرضى ملكية بياناتهم الصحية والتحكم فيها مع الحفاظ على السرية، فضلاً عن تعزيز التشغيل البيئي وتبسيط العمليات الصحية. وأوصت الدراسة بضرورة مواصلة البحث في معالجة التحديات التقنية والأخلاقية وتكامل البلوكتشين مع الأنظمة الصحية القائمة لتحقيق تبنٍّ واسع النطاق.

الدراسات السابقة

دراسة (Chianumba, Ikhalea, Mustapha, Forkuo & Osamika, 2022): Integrating AI, Blockchain, and Big Data to Strengthen Healthcare Data Security, Privacy, and Patient Outcomes.

هدفت الدراسة إلى التعرف على إمكانية دمج الذكاء الاصطناعي وسلاسل الكتل والبيانات الضخمة بأبعاده (حماية البيانات بالتشفير المدعوم بالذكاء الاصطناعي، سلامة البيانات عبر البلوكتشين اللامركزي، تحليلات البيانات الضخمة للتنبؤ بنتائج المرضى) لتعزيز أمن البيانات الصحية والخصوصية وتحسين نتائج المرضى. واستخدمت الدراسة المنهج الوصفي النظري القائم على بناء نموذج مفاهيمي تكاملي. وتوصلت نتائج الدراسة إلى أن الذكاء الاصطناعي يُعزّز أمن البيانات من خلال التشفير المتقدم واكتشاف التهديدات الأمنية، وأن البلوكتشين يضمن سلامة البيانات من خلال التخزين اللامركزي والعقود الذكية، وأن تحليلات البيانات الضخمة تُسهم في التنبؤ بنتائج المرضى وضمان الامتثال لمعايير الخصوصية. وأوصت الدراسة بتبني استراتيجيات شاملة لدمج هذه التقنيات في البنية التحتية الصحية مع التركيز على معالجة التحديات التنظيمية والتشغيلية.

دراسة (Handayani, Apriani, Mulyati, Zahra & Yusuf, 2023): Enhancing Security and Privacy

of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation.

هدفت الدراسة إلى التعرف على أثر تطبيق تقنية البلوكتشين بأبعاده (أمن البيانات، خصوصية البيانات، إدارة البيانات) على تعزيز أمن وخصوصية بيانات المرضى في منظومة الرعاية الصحية. واستخدمت الدراسة المنهج الكمي التحليلي باستخدام أسلوب SmartPLS لنمذجة المعادلات البنائية، وتكونت العينة من مؤسسات الرعاية الصحية التي طبقت تقنية البلوكتشين في إدارة بياناتها، حيث جُمعت البيانات من خلال استبيانات. وتوصلت نتائج الدراسة إلى وجود تأثير إيجابي ذي دلالة إحصائية لتطبيق تقنية البلوكتشين على تعزيز أمن وخصوصية بيانات المرضى، كما حدّدت الدراسة تحديات تتعلق بقابلية التوسع والتشغيل البيئي تحتاج إلى معالجة لضمان نجاح التطبيق. وأوصت الدراسة بضرورة معالجة تحديات التوسع والتكامل مع الأنظمة القائمة لتحقيق

الدراسات السابقة

(Yaqoob, Salah, Jayaraman & Al-Hammadi, 2022): Blockchain for دراسة
Healthcare Data Management: Opportunities, Challenges, and Future
Recommendations.

هدفت الدراسة إلى التعرف على كيفية الاستفادة من تقنية البلوكتشين في إدارة البيانات الصحية بأبعاده (الشفافية وتتبع المعاملات، أمن السجلات الصحية الإلكترونية، التشغيل البيئي ومشاركة البيانات، تتبع سلاسل التوريد الدوائية) في قطاع الرعاية الصحية. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة الشاملة للأدبيات وتحليل التجارب التطبيقية الدولية (مثل تجربة إستونيا والإمارات). وتوصلت نتائج الدراسة إلى أن أنظمة إدارة البيانات الصحية الحالية تواجه تحديات جوهرية في الشفافية والتتبع وسلامة البيانات، وأن تقنية البلوكتشين تُقدّم حلولاً فعّالة لهذه التحديات من خلال السجل الموزع غير القابل للتعديل، إلا أن عقبات مثل قابلية التوسع وتكاليف التنفيذ والامتثال التنظيمي لا تزال تُعيق التبني الواسع. وأوصت الدراسة بتطوير حلول بلوكتشين هجينة (عامة/خاصة) مُخصّصة للرعاية الصحية، والعمل على تحسين قابلية التوسع وخفض التكاليف التشغيلية.

الإطار النظري

أولاً: تقنية سلاسل الكتل — (Blockchain) تُعرّف تقنية سلاسل الكتل بأنها سجل رقمي موزّع ولا مركزي يُستخدم لتسجيل المعاملات والبيانات عبر شبكة من الحواسيب المترابطة (العُقد)، بحيث تُخزّن كل مجموعة من المعاملات في كتلة (Block) مُشفّرة ترتبط بالكتلة التي تسبقها بتسلسل زمني من خلال بصمة تشفيرية فريدة (Hash)، مكوّنة بذلك سلسلة متصلة غير قابلة للكسر أو التعديل بأثر رجعي. ويعود الظهور الأول لهذه التقنية إلى عام 2008 حين قدّمها الشخص أو المجموعة المعروفة باسم "ساتوشي ناكاموتو" بوصفها البنية التحتية لعملة البيتكوين الرقمية، إلا أن تطبيقاتها سرعان ما تجاوزت نطاق العملات المشفّرة لتمدّد إلى قطاعات حيوية متعددة من بينها الرعاية الصحية والمالية وسلاسل التوريد والحوكمة الإلكترونية، وذلك بفضل ما تتمتع به من خصائص جوهرية تتمحور حول اللامركزية والشفافية وعدم قابلية التعديل والأمان التشفيري (عبدالمحسن، محمد، وعبدالمجيد، 2023).

الإطار النظري

مخاطر الخصوصية وتسرب البيانات الصحية تُعرّف مخاطر الخصوصية وتسرب البيانات الصحية إجرائياً في هذه الدراسة بأنها مجموعة التهديدات والاحتمالات التي تؤدي إلى كشف أو فقدان أو وصول غير مصرّح به أو استخدام غير مشروع للبيانات الصحية الشخصية للمرضى، سواء نتج ذلك عن هجمات سيبرانية خارجية أو تهديدات داخلية أو أخطاء بشرية أو ثغرات تقنية في أنظمة إدارة البيانات. وتشمل هذه المخاطر انتهاك سرية المعلومات الطبية والكشف عن هويات المرضى والتلاعب بالسجلات الصحية والوصول غير المصرّح به من قبل جهات غير مخوّلة، وهي مخاطر تتفاقم في البيئات الصحية الرقمية التي تتسم بتعدد الأطراف المشاركة في تداول البيانات (Adeghe,

Okolo & Ojeyinka, 2024).

الإطار النظري

العلاقة النظرية بين تقنية سلاسل الكتل وخفض مخاطر الخصوصية وتسرب البيانات

يرتكز الأساس النظري لهذه الدراسة على فرضية مفادها أن الخصائص البنيوية لتقنية سلاسل الكتل تمتلك القدرة على معالجة نقاط الضعف الجوهرية في أنظمة إدارة البيانات الصحية التقليدية التي تُشكّل المصدر الأساسي لمخاطر الخصوصية والتسرب. فالتشفير اللامركزي يُعالج مشكلة نقطة الفشل الواحدة الكامنة في البنى المركزية، والعقود الذكية تُعالج مشكلة ضعف آليات التحكم في الوصول وبطئها، وخاصية عدم قابلية التعديل تُعالج مشكلة إمكانية التلاعب بالسجلات الصحية، وآليات إدارة الموافقة تُعالج مشكلة غياب سيطرة المرضى على بياناتهم. وقد أكدت الدراسات الحديثة أن النماذج القائمة على البلوكتشين لحماية السجلات الصحية الشخصية أظهرت فاعلية ملموسة في خفض مخاطر الوصول غير المصرّح به وتسرب البيانات من خلال التشفير الشامل من طرف إلى طرف وإدارة الوصول اللامركزية. (Vanin et al., 2022) كما أن دمج تقنيات التشفير المتقدمة مع البنية اللامركزية للبلوكتشين يُقدّم إطاراً أمنياً متعدد الطبقات يُقلّل بشكل جوهري من احتمالات الاختراق والتسريب مقارنة بالأنظمة المركزية التقليدية (Afrihyia et al., 2025).

- العنزي، حنان عواد، و الرباعي، ريم علي محمد. (2025). حماية المعرفة في المدن الصحية الذكية بين مشاركة البيانات وضمان الأمن والخصوصية. المجلة العربية للنشر العلمي، ع86 ، 254 - 272. مسترجع من <http://search.mandumah.com/Record/1657549>
- الهلال، محمد بن ناصر. (2020). مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-19 من وزارة الصحة السعودية: دراسة وصفية. مجلة دراسات المعلومات، ع25 ، 100 - 116. مسترجع من <http://search.mandumah.com/Record/1186328>
- السلمي، أماني عبدالقوي عبيد. (2022). واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بالمملكة العربية السعودية: دراسة حالة. كتاب أعمال الملتقى الافتراضي الثاني لجمعية المكتبات المتخصصة فرع الخليج العربي: مشاركة المعرفة بين المؤسسات ذات المصالح المشتركة - الفرص والتحديات والممارسات، المنامة: جمعية المكتبات المتخصصة فرع الخليج العربي، 9 - 28. مسترجع من <http://search.mandumah.com/Record/1301987>
- الفهمي، أصايل عبدالله، المالكي، ندى حمدان، و حمبشي، ناريمان خالد. (2025). دور تقنية سلاسل الكتل "Blockchain" في حفظ المخطوطات وإدارتها: دراسة نظرية. المؤتمر الثامن والعشرون: نحو استدامة المعرفة والحفاظ على الثقافة والتراث - إدارة الوثائق النادرة والمخطوطات والمواد التراثية في عصر التقنيات الناشئة والذكاء الاصطناعي، جدة: جمعية المكتبات المتخصصة فرع الخليج العربي، 261 - 274. مسترجع من <http://search.mandumah.com/Record/1653494>
- الخرايشة، محمد هاشم علي، الوشاح، سليمان راجي سليمان، و أبو حمور، أيمن محمود جميل. (2024). الأثر المتوقع لاستخدام تقنية سلاسل الكتل في جودة التقارير المالية: دراسة ميدانية: البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1497736>
- المزيد، عبدالعزيز بن حسين متعب. (2024). واقع استخدام سلاسل الكتل "Block Chain" في المصارف السعودية: دراسة حالة مصرف الراجحي. المجلة العلمية للدراسات التجارية والبيئية، مج15، ع3 ، 412 - 441. مسترجع من <http://search.mandumah.com/Record/1553038>
- عبدالمحسن، محمد عبدالمعز محمد، محمد، وائل فوزي عبدالباسط، و عبدالمجيد، عيد رشاد عبدالقادر. (2023). التحول الرقمي باستخدام تكنولوجيا سلاسل الكتل "Blockchain": دراسة نظرية. المجلة العلمية للاقتصاد والتجارة، ع3 ، 195 - 216. مسترجع من <http://search.mandumah.com/Record/1418060>
- الضعائيلة، معتز محمود بركات، و عوض، حسين أحمد. (2024). أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية (رسالة ماجستير غير منشورة). جامعة عمان العربية، عمان. مسترجع من <http://search.mandumah.com/Record/1580754>
- عبداللاه، محمود محمد عبدالمنعم. (2023). أثر تكنولوجيا سلاسل الكتل على كفاءة وفعالية الخدمات السياحية. مجلة كلية السياحة والفنادق، مج7، ع1 ، 27 - 48. مسترجع من <http://search.mandumah.com/Record/1479854>
- الزهراني، سعيد بن محمد. (2024). تقنية سلاسل الكتل "البلوكتشين" ومهنة المحاسبة. مجلة المحاسبة، س25، ع67 ، 25 - 26. مسترجع من <http://search.mandumah.com/Record/1534653>
- عبدالقادر، محمد فتحي أحمد. (2022). أثر تطبيق تقنية سلاسل الكتل على المراجعة الخارجية. مجلة الدراسات والبحوث التجارية، س42، ع4 ، 1 - 43. مسترجع من <http://search.mandumah.com/Record/1405445>
- سراج، سامح عبدالمنعم. (2024). أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل الإمداد لدعم الميزة التنافسية: دراسة تطبيقية على شركات الأدوية العاملة في السوق المصرية. المجلة العلمية للدراسات والبحوث المالية والتجارية، مج5، ع1 ، 1487 - 1533. مسترجع من <http://search.mandumah.com/Record/1616726>

- Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology*, 10(2), 013–020.
- Chianumba, E. C., Ikhalea, N., Mustapha, A. Y., Forkuo, A. Y., & Osamika, D. (2022). Integrating AI, blockchain, and big data to strengthen healthcare data security, privacy, and patient outcomes. *Journal of Frontiers in Multidisciplinary Research*, 3(1), 124–129
- Handayani, I., Apriani, D., Mulyati, M., Zahra, A. R. A., & Yusuf, N. A. (2023). Enhancing security and privacy of patient data in healthcare: A smartpls analysis of blockchain technology implementation. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 5(1), 8–17
- Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14), 11475–11490.
- Afrihyia, E., Chianumba, E. C., Mustapha, A. Y., Forkuo, A. Y., & Omotayo, O. (2025). Developing privacy-preserving data sharing protocols for healthcare systems using cryptographic and blockchain-based techniques. *International Journal of Advanced Multidisciplinary Research and Studies*, 5.
- Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, 83(21), 60443–60467
- Esmailzadeh, P. (2022). Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. *BMC Medical Informatics and Decision Making*, 22(1), 80.
- Vanin, F. N. D. S., Policarpo, L. M., Righi, R. D. R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2022). A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. *Sensors*, 23(1), 14.



Thank You