

جامعة ميدأوشن



كلية الإدارة

ماجستير إدارة المخاطر

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

إعداد الطالب/

بركات شميلان العازمي

المشرف الثاني/

د.فايز جراد

المشرف الرئيسي/

د. الفیصل عبد الحمید

العام الدراسي:

1448 – 2026



إِهْدَاء

إلى من غابا عن عيني وحضرا في دعائي، أظهر قلبين عرفتهما؛ والديّ العزيزين .
رحمهما الله وغفر لهما وجعل الجنة مثواهما.

إلى رفيقة الدرب والخطى، من شاركتني السراء والضراء، ودعمتني في كل
خطوة؛ زوجتي المخلصة.

إلى قُرّة عيني وسندي في الحياة؛ أبنائي الأربعة.

وإلى زهرة عمري وبهجة أيامي؛ ابنتي الغالية (ديم).

إلى كل من شدّ على يدي من الأقارب والأصدقاء والزملاء.

أهديكم ثمرة هذا الجهد العلمي.

شكر وفخر

أحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي،

والذي ألهمني الصحة والعافية والعزيمة.

فالحمد لله حمداً كثيراً

نتقدم بجزيل الشكر والتقدير إلي /

جامعة ميد أوشن

على كل ما قدمته لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا في جوانبها المختلفة.

والشكر والتقدير موصول إلي الكادر الأكاديمي والإداري، لما قدموه من تسهيلات وتشجيع وتوفير

الخدمات المطلوبة.

كما أتقدم بالشكر الجزيل لكل من لم يسعني الحظ بذكر أسمائهم راجياً من المولي عز وجل أن تكون

هذه الدراسة نافذة لدراسات أخرى .

المستخلص

هدفت هذه الدراسة إلى الكشف عن أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعادها (التشفير اللامركزي للبيانات، والعقود الذكية للتحكم في الوصول، وسلامة البيانات وعدم قابليتها للتعديل، وآليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية. واعتمدت الدراسة المنهج الوصفي التحليلي، وطُبِّقَت الاستبانة أداةً رئيسية لجمع البيانات من عينة عشوائية طبقية شملت العاملين في مجال إدارة البيانات الصحية وتقنية المعلومات بالمؤسسات الصحية السعودية، وقد بلغ عدد الاستبانات الصالحة للتحليل (373) استبانة، وعولجت البيانات إحصائياً باستخدام برنامج (SPSS V.26).

وتوصّلت الدراسة إلى وجود أثر ذي دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق تقنية سلاسل الكتل بأبعاده مجتمعةً على خفض مخاطر الخصوصية وتسرب البيانات، إذ بلغ معامل التحديد ($R^2 = 0.776$)، أي أن (77.6%) من التباين في خفض المخاطر يُفسَّر بهذه الأبعاد. وأظهرت النتائج أن بُعد سلامة البيانات وعدم قابليتها للتعديل جاء الأكثر تأثيراً ($B = 0.326$)، يليه بُعد العقود الذكية للتحكم في الوصول ($B = 0.298$)، ثم بُعد التشفير اللامركزي ($B = 0.241$)، وأخيراً بُعد آليات إدارة الموافقة والتفويض ($B = 0.189$). وفي ضوء هذه النتائج، أوصت الدراسة بتبني تقنية سلاسل الكتل ركيزةً استراتيجيةً في منظومة التحول الرقمي الصحي، وتطوير منصة وطنية موحدة لمشاركة البيانات الصحية، وسنّ تشريعات تُنظِّم استخدام العقود الذكية وآليات الموافقة الإلكترونية بما يتوافق مع نظام حماية البيانات الشخصية السعودي.

الكلمات المفتاحية: تقنية سلاسل الكتل، مشاركة البيانات الصحية، خصوصية البيانات، تسرب البيانات، المؤسسات الصحية، المملكة العربية السعودية.

قائمة المحتويات

بسم الله الرحمن الرحيم.....	ب
الإهداء	ج
الشكر والتقدير.....	د
المستخلص.....	هـ
قائمة المحتويات	و
قائمة الجداول.....	ط
الفصل الأول: الإطار العام للدراسة	1
1.1 المقدمة.....	1
2.1 مشكلة الدراسة.....	2
3.1 أهداف الدراسة.....	4
4.1 أسئلة الدراسة.....	5
5.1 فروض الدراسة.....	5
6.1 أهمية الدراسة.....	6
8.1 الدراسات السابقة:.....	7
8.1 الفجوة البحثية.....	15
9.1 المنطلقات النظرية للدراسة.....	15
10.1 المنهجية وطرق البحث:.....	19
11.1 مجتمع وعينة الدراسة.....	19
12.1 مصادر جمع البيانات.....	20
13.1 أداة الدراسة (الاستبانة).....	21
14.1 الأساليب الإحصائية المستخدمة.....	21
15.1 حدود الدراسة.....	22
الفصل الثاني: الإطار النظري.....	24

المبحث الأول: المتغير المستقل "تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية".	24
1.1.2 تمهيد.	24
2.1.2 مفهوم تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية.	25
3.1.2 أهمية تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية.	27
4.1.2 أهداف تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية.	29
5.1.2 الأبعاد النظرية لتطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية.	30
6.1.2 المداخل النظرية الحاكمة لتطبيق البلوك تشين في مشاركة البيانات الصحية.	35
7.1.2 خاتمة المبحث الأول.	35
المبحث الثاني: المتغير التابع "خفض مخاطر الخصوصية وتسرب البيانات".	36
1.2.2 تمهيد.	36
2.2.2 مفهوم خفض مخاطر الخصوصية وتسرب البيانات.	36
3.2.2 أهمية خفض مخاطر الخصوصية وتسرب البيانات.	38
4.1.2 أهداف خفض مخاطر الخصوصية وتسرب البيانات.	40
5.1.2 المضمون النظري لمخاطر الخصوصية وتسرب البيانات الصحية.	40
6.1.2 المحاور المؤسسية لخفض مخاطر الخصوصية وتسرب البيانات.	41
7.1.2 المؤشرات النظرية التي يُفهم من خلالها خفض مخاطر الخصوصية وتسرب البيانات.	43
8.1.2 علاقة المتغير التابع ببيئة المؤسسات الصحية.	43
9.1.2 خفض مخاطر الخصوصية وتسرب البيانات في ضوء المنظور الإداري.	44
10.1.2 خاتمة المبحث الثاني.	44
الفصل الثالث: منهجية الدراسة وإجراءاتها.	47
1.3 تمهيد.	47
2.3 منهج الدراسة.	47
3.3 مجتمع الدراسة.	47
4.3 عينة الدراسة.	48
5.3 أداة الدراسة.	49

50	6.3 صدق أداة الدراسة
51	7.3 ثبات أداة الدراسة
52	8.3 مصفوفة الارتباط بين متغيرات الدراسة
53	9.3 الأساليب الإحصائية المستخدمة
55	الفصل الرابع: تحليل البيانات واختبار فرضيات الدراسة
55	1.4 تمهيد
55	2.4 التحليل الديموغرافي لأفراد عينة الدراسة
56	3.4 التحليل الوصفي لاستجابات أفراد العينة
67	4.4 اختبار فرضيات الدراسة
73	الفصل الخامس: النتائج والتوصيات
73	1.5 تمهيد
73	2.5 نتائج الدراسة
76	3.5 توصيات الدراسة
77	4.5 الدراسات المقترحة
78	Abstract
79	المراجع
83	الملاحق
84	استمارة استبيان

قائمة الجداول

رقم الصفحة	اسم الجدول	رقم الجدول
49	جدول (1-3): توزيع الاستبانات الموزعة والمستردة والصالحة للتحليل	1.
49	جدول (2-3): توزيع عينة الدراسة وفق المنطقة الجغرافية	2.
50	جدول (3-3): معيار الحكم على المتوسطات الحسابية وفق مقياس ليكرت الخماسي	3.
51	جدول (4-3): معاملات ارتباط فقرات أبعاد المتغير المستقل بالدرجة الكلية لكل بُعد	4.
52	جدول (5-3): معاملات ارتباط فقرات المتغير التابع (خفض مخاطر الخصوصية وتسرب البيانات) بالدرجة الكلية	5.
53	جدول (6-3): معاملات ثبات ألفا كرونباخ لأبعاد الدراسة	6.
54	جدول (7-3): مصفوفة معاملات الارتباط بين أبعاد الدراسة ($n = 373$)	7.
56	جدول (1-4): توزيع أفراد عينة الدراسة وفق المتغيرات الديموغرافية (ن = 373)	8.
57	جدول (2-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد التشفير اللامركزي للبيانات	9.
59	جدول (3-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد العقود الذكية للتحكم في الوصول	10.
61	جدول (4-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سلامة البيانات وعدم قابليتها للتعديل	11.
63	جدول (5-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد آليات إدارة الموافقة والتفويض	12.

رقم الصفحة	اسم الجدول	رقم الجدول
64	جدول (4-6): الترتيب العام لأبعاد المتغير المستقل (تطبيق تقنية سلاسل الكتل)	13.
65	جدول (4-7): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع	14.
65	جدول (4-8): نتائج تحليل الانحدار المتعدد لأثر أبعاد تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات	15.
68	جدول (4-9): تحليل الانحدار الخطي البسيط لقياس أثر التشفير اللامركزي للبيانات على خفض مخاطر الخصوصية وتسرب البيانات	16.
70	جدول (4-10): تحليل الانحدار الخطي البسيط لقياس أثر العقود الذكية للتحكم في الوصول على خفض مخاطر الخصوصية وتسرب البيانات	17.
71	جدول (4-11): تحليل الانحدار الخطي البسيط لقياس أثر سلامة البيانات وعدم قابليتها للتعديل على خفض مخاطر الخصوصية وتسرب البيانات	18.
72	جدول (4-12): تحليل الانحدار الخطي البسيط لقياس أثر آليات إدارة الموافقة والتفويض على خفض مخاطر الخصوصية وتسرب البيانات	19.

الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

يُمثل 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).

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 تُسجّل 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 يُوزّع 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)

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 البيني 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).

ومن جهة أخرى، 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 والتميز 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)

وتتعاظم أهمية التصدي لهذه المخاطر في السياق السعودي تحديداً، حيث تمضي المملكة العربية السعودية بخطوات حثيثة نحو رقمنة قطاعها الصحي ضمن مستهدفات رؤية 2030 وبرنامج التحول الصحي، مما يجعل حجم البيانات الصحية المتداولة في تصاعد مستمر ويُضاعف من الحاجة إلى حلول أمنية متقدمة. وقد أكدت الدراسات المحلية أن واقع مشاركة البيانات الصحية في المملكة لا يزال يُعاني من تحديات مرتبطة بغياب السياسات الموحدة وضعف الوسائل التقنية المتاحة لتبادل البيانات بين الباحثين والمؤسسات الصحية بشكل آمن ومقنّن (الهلال، 2020).

وفي ضوء هذا السياق العلمي والعملية، 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 وعلمي 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 (العنزي والرابغي، 2025)

2.1 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 مسبوقة، 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 يندرج بتهديدات جسيمة تطال سلامة المرضى وسرية معلوماتهم وثقتهم في المنظومة الصحية برمتها.

وتكشف الإحصاءات الدولية عن خطورة هذا الواقع، حيث أظهر تقرير IBM Security لعام 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، أثّرت 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.

وتتمحور جذور هذه المشكلة في أن أنظمة إدارة البيانات الصحية التقليدية تعتمد في معظمها على بنى مركزية تُخزّن 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 تقتصر 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.

وفي هذا السياق، برزت تقنية سلاسل الكتل (Blockchain) بوصفها حلاً تقنياً واعداً يحمل في بنيته الجوهرية خصائص قد تُعالج هذه التحديات المتشابكة، من خلال التشفير اللامركزي الذي يُلغي الاعتماد على نقطة تخزين مركزية واحدة، والعقود الذكية التي تُؤتمت عمليات التحكم في الوصول وفق شروط محددة مسبقاً دون الحاجة إلى وسيط، وخاصية عدم قابلية التعديل التي تضمن سلامة السجلات الصحية وعدم

التلاعب بها، وآليات إدارة الموافقة اللامركزية التي تمنح المرضى ملكية بياناتهم والتحكم الكامل في مشاركتها. غير أن الأدبيات العربية تكاد تخلو من دراسات تحليلية تطبيقية تقيس أثر هذه الأبعاد مجتمعة على خفض مخاطر الخصوصية وتسرب البيانات في السياق الصحي السعودي، وهو ما أكدته مراجعة الدراسات السابقة التي كشفت عن فجوة بحثية واضحة في هذا المجال.

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؟

3.1 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 الرئيسى الأهداف الفرعية التالية:

1. التعرف على أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.
2. 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.
3. 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.
4. التعرف على أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.
5. تقديم إطار مقترح لتبني تقنية سلاسل الكتل في مشاركة البيانات الصحية بما يُعزّز حماية الخصوصية ويُخفّض مخاطر تسرب البيانات في المؤسسات الصحية السعودية.

4.1 أسئلة الدراسة

السؤال الرئيسي:

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:

1. ما أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
2. ما أثر العقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
3. ما أثر سلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
4. ما أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

5.1 فروض الدراسة

الفرض الرئيسي:

- 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.

6.1 أهمية الدراسة

الأهمية العلمية (النظرية):

- تُسهم هذه الدراسة في سدّ فجوة واضحة في الأدبيات العربية التي تقتصر 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.

7.1 الأهمية العملية (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 رؤى 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.

8.1 الدراسات السابقة:

أولاً: الدراسات العربية

☒ دراسة (الهلال، 2020): مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-19 من وزارة الصحة السعودية.

هدفت الدراسة إلى التعرف على مدى مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-19 من وزارة الصحة السعودية بأبعاده (وسائل مشاركة البيانات، معوقات المشاركة، مستوى الدعم المؤسسي) وأثرها على جودة الأبحاث العلمية الموجهة لمواجهة الجائحة في المملكة العربية السعودية. واستخدمت الدراسة المنهج الوصفي المسحي، وتكونت العينة من الباحثين الحاصلين على منح البرنامج، حيث وُزعت عليهم استبانة لجمع البيانات. وتوصلت نتائج الدراسة إلى أن 90% من الباحثين يدركون أن مشاركة البيانات ترفع من مستوى جودة الأبحاث للتصدي لكوفيد-19، وأن 80% يستخدمون البريد الإلكتروني وسيلةً أساسيةً لمشاركة البيانات، بينما تمثلت أبرز المعوقات في عدم وجود سياسات داعمة للمشاركة بنسبة 80%، وقلة وسائل المشاركة وضعف الوعي المعلوماتي بنسبة 70%. وأوصت الدراسة بضرورة وضع سياسات واضحة لمشاركة البيانات الصحية بين الباحثين، وتوفير منصات إلكترونية آمنة ومتخصصة لتبادل البيانات، وتعزيز الدعم المؤسسي من وزارة الصحة لتحفيز الباحثين على المشاركة المقننة والمنظمة.

❏ 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 فعال 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.

❏ دراسة (عبدالقادر، 2022): أثر تطبيق تقنية سلاسل الكتل على المراجعة الخارجية.

هدفت الدراسة إلى التعرف على أثر تطبيق تقنية سلاسل الكتل (Blockchain) بأبعاده (سلامة البيانات، التشفير، العقود الذكية، السجل الرقمي الموزع) على المراجعة الخارجية وكيفية إحداثها تحولاً في عمليات المراجعة. واستخدمت الدراسة المنهجين الاستقرائي والاستنباطي لتحليل الأدبيات والدراسات ذات الصلة. وتوصلت نتائج الدراسة إلى أن تطبيق تقنية سلاسل الكتل أحدث تحولاً جوهرياً في مهنة المراجعة تمثل في تخفيض وقت عملية المراجعة، وتعزيز دقة المعلومات، والتحقق من سلامة العمليات، وإنشاء مسارات مراجعة أكثر كفاءة، وإجراء عمليات مراجعة مستمرة، وسرعة اكتشاف الأخطاء وكشف الاحتيال. وأوصت الدراسة بضرورة تطوير المهارات التكنولوجية للمراجعين الخارجيين للتعامل مع بيئة البلوكتشين، وتبني أساليب مراجعة حديثة تتلاءم مع البيئة الإلكترونية.

❏ دراسة (عبدالمحسن ومحمد وعبدالمجيد، 2023): التحول الرقمي باستخدام تكنولوجيا سلاسل الكتل. "Blockchain".

هدفت الدراسة إلى التعرف على تقنية سلاسل الكتل (Blockchain) بأبعاده (المفهوم والأنواع، آلية العمل، التطبيقات في القطاعات المختلفة) ودورها في تحقيق التحول الرقمي في المؤسسات الحكومية

والخاصة. واستخدمت الدراسة المنهج الوصفي النظري القائم على مراجعة وتحليل الأدبيات ذات الصلة. وتوصلت نتائج الدراسة إلى أن تقنية سلاسل الكتل تُعدّ من أبرز ركائز الثورة الصناعية الرابعة إلى جانب الذكاء الاصطناعي، وأنها تُسهم في خفض التكاليف وتسريع الأداء وتحقيق الشفافية في مختلف القطاعات، وأن الحكومات والشركات الخاصة حول العالم بدأت في تبنيها لتحقيق التحول الرقمي. وأوصت الدراسة بضرورة تكثيف الجهود البحثية لتطوير تطبيقات سلاسل الكتل في القطاعات الحيوية كالصحة والتعليم والمالية، والعمل على بناء بنية تحتية رقمية داعمة لتبني هذه التقنية.

☒ 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.

☒ 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 تُسهم 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 (سراج، 2024): أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل الإمداد لدعم الميزة التنافسية: دراسة تطبيقية على شركات الأدوية العاملة في السوق المصرية.

هدفت الدراسة إلى التعرف على الأثر المباشر وغير المباشر لتقنية سلاسل الكتل بأبعاده (اللامركزية، الشفافية، الأتمتة، الأمان) من خلال الدور الوسيط لإدارة سلاسل الإمداد على الميزة التنافسية لشركات الأدوية العاملة في السوق المصرية. واستخدمت الدراسة المنهج الوصفي التحليلي بأسلوب الحصر الشامل، وتكونت العينة من رؤساء مجالس الإدارات ومديري إدارات تكنولوجيا المعلومات في 170 شركة دوائية مصرية، حيث تم جمع 242 استمارة استقصاء صحيحة. وتوصلت نتائج الدراسة إلى معنوية التأثير المباشر وغير المباشر لأبعاد تقنية سلاسل الكتل على الميزة التنافسية، وذلك من خلال الدور الوسيط لإدارة سلاسل الإمداد، كما تبين وجود اختلافات معنوية بين أنواع الشركات الثلاثة (عامة، خاصة، استثمار أجنبي ومشترك) من حيث توافر أبعاد التقنية. وأوصت الدراسة بضرورة تبني تقنية البلوكتشين في سلاسل الإمداد الدوائية لتعزيز الميزة التنافسية، وتوفير البنية التحتية والتدريب اللازمين.

☒ 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 للمستفيدين 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 والبلوكتشين تُسهم في تعزيز حماية المعرفة الصحية، غير أن غياب الأطر التنظيمية الموحدة يُشكل 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 والبلوكتشين، وتعزيز التعاون بين الجهات الصحية والتقنية لتحقيق مشاركة آمنة وفعالة للبيانات.

ثانياً: الدراسات الأجنبية

☒ 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)

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 بقبالية التوسع والتشغيل البيني تحتاج إلى معالجة لضمان نجاح التطبيق. وأوصت الدراسة بضرورة معالجة تحديات التوسع والتكامل مع الأنظمة القائمة لتحقيق تطبيق فعال وشامل للبلوكتشين في المؤسسات الصحية.

☒ دراسة (Yaqoob, Salah, Jayaraman & Al-Hammadi, 2022): Blockchain for 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.

☒ دراسة (Esmaeilzadeh, 2022): Benefits and Concerns Associated with Blockchain-Based Health Information Exchange (HIE): A Qualitative Study from Physicians' Perspectives.

هدفت الدراسة إلى التعرف على الفوائد والمخاوف والعوائق المرتبطة باستخدام تقنية البلوكتشين في تبادل المعلومات الصحية بأبعاده (الميزات التقنية المبتكرة، النظام التعاوني، أداء النظام) والمخاوف بأبعادها (القضايا الفردية، التنظيمية، التقنية، السوقية) من وجهة نظر الأطباء في الولايات المتحدة. واستخدمت الدراسة المنهج النوعي القائم على النظرية المجرّدة وإطار PARIHS ، وتكونت العينة من 36 طبيباً من تخصصات ومؤسسات صحية متنوعة في الولايات المتحدة، حيث أُجريت مقابلات شبه مهيكلة ومعمّقة عبر الإنترنت وحُلّلت البيانات باستخدام برنامج NVIVO. وتوصلت نتائج الدراسة إلى تحديد سبعة محاور رئيسية: ثلاثة للفوائد تشمل الميزات التقنية المبتكرة (التشغيل والتحكم بنسبة 92%)، والنظام التعاوني (التشغيل البيئي واللامركزية)، وأداء النظام (السرعة وخفض التكاليف)؛ وأربعة للمخاوف تشمل قضايا فردية (نقص المعرفة بنسبة 89%)، وقضايا تنظيمية (مشكلات التنفيذ بنسبة 84%)، وقضايا تقنية (تعقيد النظام)، وقضايا سوقية (غياب التنظيم بنسبة 78%). وأوصت الدراسة بضرورة معالجة فجوة المعرفة لدى

الأطباء حول البلوكتشين، وتطوير أطر تنظيمية داعمة، وإجراء دراسات جدوى شاملة قبل تبني أنظمة تبادل المعلومات الصحية القائمة على البلوكتشين.

☒ دراسة: (Vanin, Policarpo, Righi, Heck, Silva, Goldim & da Costa, 2022)

A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach.

هدفت الدراسة إلى التعرف على تطوير نموذج معماري لحماية السجلات الصحية الشخصية من طرف إلى طرف بأبعاده (التخزين اللامركزي عبر البلوكتشين وIPFS، التشفير المتماثل الكامل FHE، فصل البيانات الوصفية عن البيانات الفعلية، التحكم الشخصي في الوصول) من خلال الجمع بين تقنية البلوكتشين والتشفير المتماثل الكامل. واستخدمت الدراسة المنهج التجريبي التطبيقي من خلال تطوير النموذج المعماري واختباره باستخدام قاعدة بيانات تضم 1.3 مليون سجل لحالات كوفيد-19 من مراكز السيطرة على الأمراض الأمريكية (CDC) لتقييم الأداء وسعة التخزين. وتوصلت نتائج الدراسة إلى أن الجمع بين التشفير المتماثل الكامل والشبكات الموزعة يُمكنه إعادة تعريف نماذج الصحة الإلكترونية، حيث يُتيح النموذج المقترح للأفراد إدارة تشفير بياناتهم وطلبات المشاركة وتقييد الوصول لفترة محددة مسبقاً، مع دعم إجراء الحسابات على البيانات المشفرة دون الكشف عن محتواها، مما يُخفف من مخاطر الخصوصية ويُحسن التشغيل البيئي الدلالي بين المؤسسات الصحية. وأوصت الدراسة بمواصلة تطوير النموذج لتحسين كفاءة الأداء الحسابي ومعالجة تحديات التوسع في بيانات الرعاية الصحية الواقعية، مع التأكيد على أهمية الالتزام بمعايير HIPAA وGDPR.

☒ 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 تبني واسع النطاق.

❏ دراسة- (Masood, Daud, Wang, Banjar & Alharbey, 2024): A Blockchain-Based System for Patient Data Privacy and Security.

هدفت الدراسة إلى التعرف على التحديات المعقدة في بيئة البنية التحتية للسحابة القائمة على أجهزة الاستشعار (S-CI) بأبعاده (التحكم في الوصول، أمن البيانات، الخصوصية، قابلية التوسع، إتاحة المعلومات الصحية الشخصية) واقتراح نظام شامل قائم على البلوكتشين لتعزيز خصوصية وأمن بيانات المرضى. واستخدمت الدراسة المنهج التجريبي التطبيقي من خلال تطوير نموذج التحكم في الوصول القائم على البلوكتشين (BBACM) واختباره عبر حالة استخدام واقعية لمريض شلل. وتكونت العينة من بيانات واقعية لمريض شلل تم جمعها عبر أجهزة استشعار متصلة بالبنية السحابية. وتوصلت نتائج الدراسة إلى أن النموذج المقترح يُحقّق تحسينات جوهرية في التحكم بالوصول والأمن والخصوصية وقابلية التوسع وإتاحة المعلومات الصحية الشخصية مقارنةً بالبنية التقليدية التي تعتمد على جهة موثوقة واحدة. وأوصت الدراسة بتبني نماذج البلوكتشين اللامركزية في إدارة البيانات الصحية ضمن بيئات إنترنت الأشياء الطبية لتحقيق حماية شاملة لبيانات المرضى.

❏ دراسة: (Afrihyia, Chianumba, Mustapha, Forkuo & Omotayo, 2025)

Developing Privacy-Preserving Data Sharing Protocols for Healthcare Systems Using Cryptographic and Blockchain-Based Techniques.

هدفت الدراسة إلى التعرف على تطوير بروتوكولات مشاركة البيانات المحافظة على الخصوصية في الأنظمة الصحية بأبعاده (التشفير المتماثل الكامل، إثباتات المعرفة الصفرية، التشفير القائم على السمات، العقود الذكية عبر البلوكتشين) من خلال دمج التقنيات التشفيرية وتقنية البلوكتشين. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة المنهجية المنظمة للأدبيات مع تحليل مقارن بين الأنظمة المقترحة والأنظمة المركزية التقليدية. وتوصلت نتائج الدراسة إلى أن الإطار المقترح يُخفّف بشكل ملحوظ من مخاطر الوصول غير المصرّح به وتسرب البيانات ونقاط الفشل الأحادية، وأن التحليل المقارن مع الأنظمة المركزية التقليدية أظهر تحسّناً في الكفاءة وقابلية التوسع والأمن في إدارة البيانات الصحية.

وأوصت الدراسة بالتركيز المستقبلي على تحسين الكفاءة الحسابية ومعالجة تحديات قابلية التوسع لتسهيل التبني الواسع في بيئات الرعاية الصحية الواقعية.

8.1 الفجوة البحثية

من خلال الاستعراض المعمق للدراسات السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة، يتضح وجود فجوة بحثية واضحة ومتعددة الأوجه تُبرّر إجراء هذه الدراسة وتؤكد أصالتها العلمية. فعلى صعيد الدراسات العربية، يُلاحظ أن الجهود البحثية تركزت بشكل رئيسي على تطبيقات تقنية سلاسل الكتل في قطاعات بعيدة عن المجال الصحي كالقطاع المصرفي (المزيد، 2024) وسلاسل التوريد الدوائية (الضعيلة وعوض، 2024؛ سراج، 2024) والمراجعة المالية (عبدالقادر، 2022)، بينما ظلت الدراسات العربية التي تتناول تقاطع البلوكتشين مع مشاركة البيانات الصحية وحماية الخصوصية شحيحة للغاية واقتصرت على مقاربات نظرية عامة (العنزي والرابغي، 2025) أو تناولت مشاركة البيانات الصحية دون ربطها بحلول البلوكتشين (الهلال، 2020؛ السلمي، 2022). أما على صعيد الدراسات الأجنبية، فرغم ثرائها في تناول العلاقة بين البلوكتشين وأمن البيانات الصحية، إلا أن معظمها اتخذ طابعاً نظرياً مراجعياً (Adeghe et al., 2022; Yaqoob et al., 2024; al., 2024) أو نوعياً استكشافياً (Esmailzadeh, 2022) أو تقنياً بحثاً يركّز على بناء النماذج المعمارية (Vanin et al., 2022; Masood et al., 2024) دون قياس كمّي لأثر أبعاد التقنية على خفض مخاطر الخصوصية وتسرب البيانات من وجهة نظر الممارسين في الميدان الصحي. وبذلك تتبلور الفجوة البحثية في غياب دراسات تحليلية تطبيقية — لا سيما في السياق العربي والسعودي — تقيس بشكل كمّي ومتكامل أثر تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية بأبعاده الأربعة مجتمعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات من منظور العاملين في المؤسسات الصحية، وهو ما تسعى الدراسة الحالية إلى سدّه من خلال تقديم إسهام بحثي أصيل يجمع بين هذه الأبعاد في إطار تحليلي تطبيقي موحّد ضمن بيئة المؤسسات الصحية السعودية.

9.1 المنطلقات النظرية للدراسة

أولاً: تقنية سلاسل الكتل (Blockchain) — المفهوم والنشأة والخصائص

تُعرّف تقنية سلاسل الكتل بأنها سجل رقمي موزّع ولا مركزي يُستخدم لتسجيل المعاملات والبيانات عبر شبكة من الحواسيب المترابطة (العقد)، بحيث تُخزّن كل مجموعة من المعاملات في كتلة (Block) مُشفّرة ترتبط بالكتلة التي تسبقها بتسلسل زمني من خلال بصمة تشفيرية فريدة (Hash)، مكوّنةً 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 لتمتد 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).

وتقوم تقنية سلاسل الكتل على عدة مبادئ تأسيسية تميّزها عن أنظمة قواعد البيانات التقليدية. فمبدأ اللامركزية يعني أن البيانات لا تُخزّن في خادم مركزي واحد بل تُوزّع على شبكة واسعة من العقد المتساوية في الصلاحيات، مما يلغي وجود نقطة فشل واحدة ويُقلّل من مخاطر الاختراقات الشاملة. ومبدأ الإجماع يتطلب موافقة أغلبية العقد المشاركة في الشبكة على صحة أي معاملة قبل إضافتها إلى السلسلة، مما يمنع أي طرف منفرد من التلاعب بالبيانات. أما مبدأ عدم قابلية التعديل فيضمن أنه بمجرد تسجيل أي معاملة في كتلة والتحقق منها، يُصبح تغييرها أو حذفها شبه مستحيل من الناحية الحسابية، وهو ما يُوفّر مستوى غير مسبوق من سلامة البيانات وموثوقيتها. وتُصنّف شبكات سلاسل الكتل إلى ثلاثة أنواع رئيسية: الشبكات العامة المفتوحة لأي مشارك، والشبكات الخاصة المقصورة على جهات محددة، والشبكات الهجينة التي تجمع خصائص النوعين وتُعدّ الأكثر ملاءمة للتطبيقات الصحية نظراً لما تُوفّره من توازن بين الشفافية والخصوصية. (Yaqoob, Salah, Jayaraman & Al-Hammadi, 2022).

ثانياً: أبعاد تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

تتبنّى هذه الدراسة أربعة أبعاد رئيسية لقياس تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية، وفيما يلي تعريف كل بُعد وتأثيره نظرياً:

البُعد الأول — التشفير اللامركزي للبيانات: ويُقصد به توزيع البيانات الصحية المشفّرة عبر شبكة لا مركزية من العقد بدلاً من تخزينها في قاعدة بيانات مركزية واحدة، بحيث تُستخدم أزواج المفاتيح التشفيرية (العامة والخاصة) لضمان أن الأطراف المخوّلة فقط هي من يستطيع الوصول إلى البيانات وفك تشفيرها.

ويُؤَقَّر هذا النهج حماية مزدوجة تتمثل في تشفير محتوى البيانات ذاته وتوزيع تخزينها جغرافياً وتقنياً بما يُلْغِي وجود هدف مركزي واحد للمهاجمين (Masood, Daud, Wang, Banjar & Alharbey, 2024).

البُعد الثاني — العقود الذكية للتحكم في الوصول: وتُعرَّف بأنها برامج حاسوبية ذاتية التنفيذ تُكتب شروطها مباشرة في أسطر برمجية وتُنشر على شبكة سلاسل الكتل، بحيث تُنفَّذ تلقائياً عند تحقُّق شروط محددة مسبقاً دون الحاجة إلى تدخل بشري أو وسيط. وفي السياق الصحي، تُستخدم العقود الذكية لتحديد من يحق له الوصول إلى بيانات مريض مُعيّن ونوع البيانات المسموح بالاطلاع عليها والمدة الزمنية لهذا الوصول، مع توثيق كل عملية وصول في سجل شفاف وقابل للتدقيق. (Esmaeilzadeh, 2022)

البُعد الثالث — سلامة البيانات وعدم قابليتها للتعديل: ويُشير إلى الخاصية الجوهرية في تقنية سلاسل الكتل التي تضمن أنه بمجرد تسجيل أي سجل صحي أو معاملة بيانات في كتلة مُتحقَّق منها، يُصبح تعديلها أو حذفها أو التلاعب بها مستحيلًا عملياً دون أن يتم رصد ذلك فوراً من قِبل جميع العُقد المشاركة في الشبكة. وتضمن هذه الخاصية حفظ مسار تدقيق كامل وشفاف لجميع التغييرات التي تطرأ على السجلات الصحية، مما يُعزِّز الموثوقية والمساءلة في بيئة مشاركة البيانات (Chianumba, Ikhalea, Mustapha, Forkuo & Osamika, 2022).

البُعد الرابع — آليات إدارة الموافقة والتفويض: وتُعرَّف بأنها المنظومة التقنية القائمة على سلاسل الكتل والتي تُمكن المرضى من منح أو تعديل أو سحب موافقتهم على مشاركة بياناتهم الصحية مع أطراف محددة ولأغراض معيّنة وفترات زمنية مُحدَّدة مسبقاً، وذلك بشكل رقمي مُوثَّق وغير قابل للإنكار. وتُعِيد هذه الآليات السيطرة الفعلية على البيانات الصحية إلى أصحابها (المرضى) بدلاً من أن تبقى حكرًا على المؤسسات الصحية، وهو ما يتوافق مع المتطلبات التنظيمية الحديثة لحماية البيانات الشخصية (Afrihyia, Chianumba, Mustapha, Forkuo & Omotayo, 2025).

ثالثاً: مخاطر الخصوصية وتسرب البيانات الصحية — المفهوم والأبعاد

تُعرَّف مخاطر الخصوصية وتسرب البيانات الصحية إجرائياً في هذه الدراسة بأنها مجموعة التهديدات والاحتمالات التي تُؤدِّي إلى كشف أو فقدان أو وصول غير مصرَّح 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 المصرح به من قبل جهات غير مخولة، وهي مخاطر تتفاقم في البيئات الصحية الرقمية التي تتسم بتعدد الأطراف المشاركة في تداول البيانات. (Adeghe, Okolo & Ojeyinka, 2024)

وتتسم البيانات الصحية بخصوصية استثنائية تُميّزها عن غيرها من أنواع البيانات الشخصية، فهي تتضمن معلومات طبية وتشخيصية ونفسية وجينية ومالية ترتبط ارتباطاً وثيقاً بالهوية الأكثر حميمية للفرد، ويمكن أن يُفضي كشفها إلى تبعات جسيمة تتجاوز الضرر المادي لتتطال الكرامة الإنسانية والسلامة النفسية والفرص الاجتماعية والمهنية. ولذلك فرضت التشريعات الدولية والمحلية أطراً صارمة لحماية هذه البيانات، كقانون قابلية نقل التأمين الصحي والمساءلة (HIPAA) في الولايات المتحدة، واللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، ونظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر عام 2022. وتؤكد هذه التشريعات مجتمعة على ضرورة ضمان سرية البيانات الصحية وسلامتها وإتاحتها للأطراف المخولة فقط، وهي المبادئ ذاتها التي تسعى تقنية سلاسل الكتل إلى تحقيقها من خلال بنيتها اللامركزية وآلياتها التشفيرية. (Handayani, Apriani, Mulyati, Zahra & Yusuf, 2023)

رابعاً: العلاقة النظرية بين تقنية سلاسل الكتل وخفض مخاطر الخصوصية وتسرب البيانات

يرتكز الأساس النظري لهذه الدراسة على فرضية مفادها أن الخصائص البنوية لتقنية سلاسل الكتل تمتلك القدرة على معالجة نقاط الضعف الجوهرية في أنظمة إدارة البيانات الصحية التقليدية التي تُشكل 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، وخاصة 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 البلوكشين لحماية السجلات الصحية الشخصية أظهرت فاعلية ملموسة في خفض مخاطر الوصول غير المصرح 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 للبلوكشين يُقدّم إطاراً أمنياً متعدد الطبقات يُقلّل بشكل جوهري من احتمالات الاختراق والتسريب مقارنة بالأنظمة المركزية التقليدية (Afrihyia et al., 2025).

خامساً: مصطلحات الدراسة الإجرائية

تقنية سلاسل الكتل (Blockchain) سجل رقمي لا مركزي وموزع يُسجل المعاملات في كتل مُشفرة ومتراصة زمنياً وغير قابلة للتعديل، وتُقاس في هذه الدراسة من خلال أربعة أبعاد هي التشفير اللامركزي والعقود الذكية وسلامة البيانات وإدارة الموافقة.

مشاركة البيانات الصحية: عملية تبادل البيانات الطبية والصحية بين المؤسسات الصحية والباحثين والجهات المعنية وفق بروتوكولات وسياسات محددة تهدف إلى تحسين جودة الرعاية الصحية.

مخاطر الخصوصية وتسرب البيانات: مجموعة التهديدات والاحتمالات التي تؤدي إلى كشف أو فقدان أو وصول غير مصرح به للبيانات الصحية، وتُقاس في هذه الدراسة من خلال محور أحادي مكون من عشر فقرات.

10.1 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 تحليلًا كميًا. 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.

وسيتم تطبيق هذا المنهج من خلال مرحلتين أساسيتين: مرحلة نظرية تشمل مراجعة الأدبيات والدراسات السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة لبناء الإطار النظري وتحديد أبعاد المتغيرات وتطوير أداة الدراسة، ومرحلة ميدانية تتضمن تصميم استبانة إلكترونية وتوزيعها على عينة الدراسة لجمع البيانات الأولية، ثم تحليلها باستخدام الأساليب الإحصائية المناسبة لاختبار فروض الدراسة والإجابة عن أسئلتها، بما يُمكن من الوصول إلى نتائج علمية دقيقة وتوصيات عملية قابلة للتطبيق.

11.1 مجتمع وعينة الدراسة

سيكون 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.

ونظراً لصعوبة حصر جميع أفراد مجتمع الدراسة والوصول إليهم، ستعتمد الدراسة على أسلوب العينة العشوائية الطبقة 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 الاستبانة غير المستردة أو غير الصالحة للتحليل، بحيث يُستهدف الحصول على (354) استبانة صالحة كحد أدنى لضمان التمثيل الإحصائي الملائم.

12.1 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. وستستخدم هذه المصادر في بناء الإطار النظري وتحديد أبعاد المتغيرات وتطوير أداة الدراسة.

☒ المصادر الأولية: وتتمثل في الاستبانة الإلكترونية التي ستصمم خصيصاً لهذه الدراسة وتوزع على أفراد العينة لجمع البيانات الميدانية اللازمة للإجابة عن أسئلة الدراسة واختبار فروضها.

13.1 أداة الدراسة (الاستبانة)

سُتصمّم 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 موزعة كالتالي:

البُعد	عدد الفقرات
التشفير اللامركزي للبيانات	4 فقرات
العقود الذكية للتحكم في الوصول	4 فقرات
سلامة البيانات وعدم قابليتها للتعديل	4 فقرات
آليات إدارة الموافقة والتفويض	4 فقرات
الإجمالي	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)

14.1 الأساليب الإحصائية المستخدمة

سُتُحلّل البيانات باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS V.26) وبرنامج (SmartPLS 4) 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 محكمين 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).
- ✗ اختبار (T-Test) للعينات المستقلة: لاختبار الفروق في استجابات أفراد العينة تبعاً للمتغيرات الديموغرافية ثنائية المستويات.
- ✗ اختبار شيفيه (Scheffé) للمقارنات البعدية: لتحديد اتجاه الفروق ولصالح أي فئة في حال وجود فروق دالة إحصائية.

15.1 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: ستطبق الدراسة على المؤسسات الصحية الحكومية والخاصة في المملكة العربية السعودية، وتحديدًا المستشفيات الكبرى ومراكز المعلومات الصحية في مناطق الرياض وجدة والدمام.
- ✗ الحدود الزمانية: ستجرى الدراسة الميدانية خلال الفصل الدراسي الثاني من العام الجامعي 1448/1447 هـ الموافق 2026/2025 م.

☒ الحدود البشرية: ستقتصر الدراسة على العاملين في مجالات تقنية المعلومات والأمن السيبراني وإدارة البيانات الصحية والسجلات الطبية الإلكترونية في المؤسسات الصحية المستهدفة.

الفصل الثاني: الإطار النظري

المبحث الأول: المتغير المستقل "تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية"

1.1.2 تمهيد

أصبحت مشاركة البيانات الصحية إحدى القضايا المركزية في الإدارة الصحية المعاصرة، لا لأنها تتصل فقط بتبادل المعلومات بين الأطراف العلاجية والبحثية والتنظيمية، بل لأنها تمسّ بنية القرار الصحي ذاته، وترتبط بكفاءة التشخيص، واستمرارية الرعاية، وتكامل الخدمات، وإدارة الأوبئة، وتوجيه الموارد، وتحسين جودة السياسات الصحية. غير أنّ هذا التوسع في تدفقات البيانات الصحية كشف في المقابل عن مأزق بنيوي يتمثل في التوتر بين مطلبين متلازمين: تعظيم منفعة مشاركة البيانات من جهة، وصون الخصوصية والأمن والسيادة على البيانات من جهة أخرى. ومن هنا برزت تقنية سلاسل الكتل بوصفها من أكثر التقنيات قدرة على إعادة تنظيم منطق مشاركة البيانات، ليس عبر الزيادة الكمية في تبادلها فحسب، بل عبر إعادة بناء قواعد الثقة والتحقق والتفويض والتتبع المرتبطة بها.

وتتبع أهمية تناول هذا المتغير من أن البلوك تشين لا تُفهم في البيئة الصحية باعتبارها مجرد أداة تقنية للتخزين أو النقل، بل باعتبارها بنية حاكمة للمعلومة الصحية تقوم على اللامركزية، والتشفير، وعدم القابلية للتعديل، وإمكانية تتبع المعاملات، وأتمتة ضوابط الوصول من خلال العقود الذكية. وبذلك تتحول مشاركة البيانات الصحية من ممارسة إجرائية قد تشوبها الفجوات أو المركزية المفرطة أو ضعف الشفافية، إلى ممارسة مؤسسية منضبطة يمكن فيها تحديد من يطلب البيانات، ومن يصرّح بها، وتحت أي شروط، ولفترة زمنية محددة، وبأي درجة من درجات الإتاحة والسرية.

كما أنّ البيئة الصحية السعودية، في ظل التحول الرقمي المتسارع، واتساع نطاق السجلات الصحية الإلكترونية، وتنامي الحاجة إلى التكامل بين المؤسسات والجهات الصحية، تُمثّل سياقاً مناسباً لتحليل هذا المتغير؛ لأن قضية مشاركة البيانات لم تعد شأنًا فرعيًا، بل أصبحت جزءًا من معمار الحوكمة الصحية الحديثة. ولهذا فإن التأصيل النظري لتطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية يقتضي عدم

قصر النظر على التعريف التقني للتقنية، بل توسيع التحليل ليشمل أهميتها الإدارية والتنظيمية، وأهداف تطبيقها، وأبعادها التشغيلية التي يتأسس عليها القياس العلمي لهذا المتغير.

2.1.2 مفهوم تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

تتعدد المقاربات التي تناولت مفهوم سلاسل الكتل وفق الزاوية التي ينطلق منها الباحث أو المجال الذي تُطبَّق فيه التقنية. فبعض الكتابات تقدّمها بوصفها سجلاً رقمياً موزعاً يقوم على ربط المعاملات في كتل متتابعة، بحيث تُسجَّل البيانات ضمن بنية يصعب تعديلها بعد اعتمادها، بينما تتجه كتابات أخرى إلى إبرازها كآلية لإعادة صياغة العلاقات بين الأطراف المشاركة في البيانات، من خلال إلغاء الحاجة إلى الوسيط المركزي، وإحلال الثقة المؤسسية المبرمجة محل الثقة الشخصية أو التنظيمية التقليدية. وفي هذا السياق، يذهب بعض الباحثين إلى أن البلوك تشين تمثل إحدى ركائز التحول الرقمي في المؤسسات؛ لأنها لا تقتصر على حفظ السجلات، بل تخلق بيئة تشغيلية تتسم بالسرعة والشفافية وإمكانية التتبع وتخفيض الاعتماد على المعالجة اليدوية أو المركزية (عبدالمحسن وآخرون، ٢٠٢٣).

ومن زاوية الاستخدام المؤسسي، يُفهم تطبيق سلاسل الكتل بوصفه توظيفاً منظماً لشبكة موزعة تسمح بتبادل المعاملات والمعلومات بين أطراف متعددة في وقت قريب من الزمن الحقيقي، مع إسناد التحقق من صحة كل معاملة إلى آليات تشفير وإجماع وسجل زمني يصعب العبث بالمحتوى. ولهذا ارتبط المفهوم في عدد من الكتابات العربية بخصائص مثل الشفافية، واللامركزية، وتقليل الوساطة، والموثوقية، ورفع كفاءة التعامل مع المعلومات الرقمية، وهي خصائص تجعل التقنية قابلة للتكيف في قطاعات متعددة، من المصارف إلى المراجعة إلى الخدمات والسياحة، ثم إلى البيئات الصحية ذات الحساسية العالية للبيانات (المزيد، ٢٠٢٤).

أما في حقل الصحة، فإن المفهوم يكتسب بعداً أكثر تخصصاً؛ إذ لا ينصرف فقط إلى وجود سلسلة كتل تسجل بيانات المرضى، وإنما إلى نموذج لإدارة مشاركة البيانات الصحية يسمح بحفظ البيانات أو بياناتها الوصفية ضمن بنية موزعة، مع استخدام التشفير والعقود الذكية والتحكم في الوصول لضمان أن تبادل المعلومات يتم بين أطراف مصرح لها، وبما يوازن بين إتاحة البيانات للأغراض العلاجية أو البحثية وبين الحفاظ على السرية والخصوصية. ولهذا تنتظر بعض الأدبيات إلى البلوك تشين في الرعاية الصحية باعتبارها مدخلاً لإدارة البيانات الصحية يقوم على سلامة السجل، وعدم القابلية للتعديل، والقدرة على الربط

بين المؤسسات المختلفة مع إبقاء التحكم في الوصول محكوماً بشروط واضحة ومبرمجة (Yaqoob et al., 2022).

وتتسع الدلالة المفاهيمية أكثر عندما يُربط تطبيق البلوك تشين في الصحة بمسألة ملكية المريض لبياناته وحقه في التحكم في مسارات استخدامها. فبدلاً من أن تكون البيانات الصحية موزعة بين مؤسسات منفصلة تتحكم كل منها في جزء من السجل وتفرض منطقها الخاص في الإتاحة والمنع، تتيح التقنية -في تصورات عدة- إعادة مركزية القرار في يد صاحب البيانات من حيث التفويض والموافقة والزمن والجهة المستفيدة، مع الإبقاء على أمن السجل واستمرارية الاستفادة منه لأغراض الرعاية والتحليل والتكامل المؤسسي. (Adeghe et al., 2024)

ويتصل مفهوم مشاركة البيانات الصحية هنا بمسألة أشمل هي حوكمة المعرفة الصحية؛ لأن مشاركة البيانات لا تعني النقل الميكانيكي للمعلومات من نظام إلى آخر، بل تعني تنظيم دورة حياة المعلومة الصحية: من إنتاجها، وتوصيفها، وتخزينها، وتبادلها، وتفسيرها، وحمايتها، وضمان عدم استخدامها خارج الغرض المشروع. وهذا المعنى هو ما تؤكد الأدبيات العربية التي تربط بين المدن الصحية الذكية ومشاركة المعرفة الصحية وأمن المعلومات والخصوصية، حيث تُطرح المشاركة باعتبارها عنصراً بنوياً في القرار السريري والإدارة الصحية، لكنها تظل مشروطة بوجود أطر حوكمة تضمن أمن المعلومات واحترام خصوصية المرضى (العنزي والرابغي، ٢٠٢٥).

وفي المستوى الإجرائي، يمكن القول إن تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية هو : تبني المؤسسات الصحية لبنية رقمية موزعة تستخدم التشفير، والعقود الذكية، وآليات التحقق الزمني، ومسارات التتبع، من أجل تنظيم تبادل البيانات الصحية بين الأطراف المصرح لها، على نحو يرفع موثوقية البيانات، ويعزز التحكم في الوصول إليها، ويقلل من فرص التلاعب أو التسرب أو الاستخدام غير المشروع. وهذا التعريف لا ينظر إلى التطبيق بوصفه قراراً تقنياً منعزلاً، بل بوصفه ترتيباً تنظيمياً-تقنياً يعيد تعريف العلاقة بين البيانات وصاحبها ومستخدمها والجهة الحافظة لها.

رأي الباحث

يرى الباحث أن تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية لا ينبغي اختزاله في مجرد "استخدام تقنية جديدة" داخل المؤسسات الصحية، بل ينبغي فهمه كتحول في فلسفة إدارة البيانات الصحية

ذاتها؛ إذ تنقل التقنية مركز الثقل من الإدارة المركزية للبيانات إلى الإدارة القائمة على الثقة الموزعة، ومن الحفاظ الساكن للسجلات إلى التبادل القابل للتتبع، ومن الإذن الإداري العام إلى التفويض الشرطي الدقيق. ومن ثم فإن جوهر هذا المتغير، في سياق الدراسة الحالية، يتمثل في مدى قدرة المؤسسات الصحية على توظيف خصائص البلوك تشين بما يجعل مشاركة البيانات الصحية أكثر أمانًا، وأكثر انضباطًا، وأكثر قابلية للتحقق والمساءلة.

3.1.2 أهمية تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

لا تتحدد أهمية هذا المتغير من كونه استجابة تقنية لمشكلة أمنية فحسب، بل من كونه مدخلًا لإعادة هيكلة مسار المعلومة الصحية عبر المؤسسة الصحية وبين المؤسسات، بما يرفع كفاءة الاستعمال ويحد من مواطن الضعف الملازمة للنظم التقليدية. فكلما اتسعت قاعدة البيانات الصحية وتعددت الجهات المتعاملة معها، تعاظمت الحاجة إلى نظام يوفق بين الانسياب والضبط، وبين الإتاحة والحماية، وبين سرعة التبادل وقابلية التحقق. ولهذا تفهم أهمية تطبيق البلوك تشين في المشاركة الصحية في ضوء ما تضيفه التقنية إلى بنية الثقة والحوكمة والسيطرة على تدفقات البيانات.

ويشير الهلال إلى أن أهمية مشاركة البيانات الصحية لا تنفصل عن دورها في تسهيل الوصول إلى أكبر قدر ممكن من البيانات وبناء قاعدة معلوماتية تدعم العمل البحثي والاستجابة الصحية المنظمة، بما يعني أن قيمة المشاركة لا تكمن في الكم فحسب، بل في تنظيم الوصول وإتاحة الاستفادة الجماعية من البيانات ضمن بيئة مؤسسية أكثر وضوحًا وانضباطًا (الهلال، ٢٠٢٠). ومن هذا المنطلق يمكن إبراز أهمية تطبيق البلوك تشين في مشاركة البيانات الصحية من خلال الأبعاد الآتية:

● تعزيز الثقة المؤسسية في تبادل البيانات

تُعد الثقة أحد الشروط الخفية التي تقوم عليها أي عملية مشاركة للبيانات الصحية؛ لأن الأطراف لا تتبادل سجلات عادية، بل تتعامل مع بيانات ذات حساسية شخصية ومهنية وقانونية عالية. وعندما تكون بنية المشاركة معتمدة على وسيط واحد أو قواعد وصول غامضة، فإن الثقة تصبح هشّة وعرضة للاهتزاز. أما في ظل البلوك تشين، فإن الثقة تنتقل من الاعتماد على "الوعد التنظيمية" إلى الاعتماد على "قواعد تقنية موثقة" تُسجل فيها كل عملية طلب أو منح أو تعديل أو وصول، وهو ما يرسخ الموثوقية ويقلص الشكوك المرتبطة بسوء الاستخدام.

● رفع كفاءة التكامل بين الأنظمة والجهات الصحية

إن التحدي الحقيقي في القطاع الصحي لا يكمن في امتلاك البيانات، بل في القدرة على جعلها قابلة للتكامل بين نظم متعددة، ومستشفيات متباينة، ومختبرات، ووحدات بحث، وجهات إشراف. وهنا تتجلى أهمية البلوك تشين بوصفها منصة تتيح تنسيق التفاعل بين هذه الكيانات، مع توفير سجل مرجعي مشترك يمكن الرجوع إليه للتحقق، ومتابعة مسار البيانات، ومعرفة شروط استخدامها. وتزداد هذه الأهمية في البيانات التي تشهد نموًا في البيانات الضخمة والحاجة إلى تكاملها ضمن بنى وطنية للمعلومات الصحية (السلمي، ٢٠٢٢).

● تمكين الحوكمة الدقيقة للصلاحيات والوصول

ليست المشكلة في مشاركة البيانات الصحية أن تُتاح أو لا تُتاح، بل في كيف تُتاح، ولمن، ولمدة كم، وتحت أي غرض. ومن هنا تنبع أهمية البلوك تشين في أنها تسمح بترجمة سياسات الوصول إلى شروط قابلة للتنفيذ الآلي من خلال العقود الذكية، بما يعني الانتقال من النظم العامة للتصريح إلى أنظمة أكثر دقة وقابلية للتخصيص. وهذا النوع من الحوكمة الدقيقة يخفف من العشوائية، ويقلل من التفاوت في تطبيق السياسات، ويجعل حق الوصول إلى البيانات محكومًا بإطار واضح وقابل للتدقيق (Handayani et al., 2023).

● حماية سلامة البيانات أثناء دورة حياتها

تكتسب البيانات الصحية قيمتها من دقتها التاريخية واستمرارية سلامتها؛ إذ إن أي تعديل غير مشروع أو غموض في النسخة المعتمدة أو فقدان لسجل التغييرات يمكن أن ينعكس على القرار السريري والرقابي والبحثي. ولذلك فإن أهمية سلاسل الكتل تتجلى في صيانة سلامة البيانات من خلال بنيتها القائمة على التتابع الزمني، والربط التشفيري بين الكتل، وصعوبة التغيير اللاحق دون أن يترك أثرًا واضحًا في السجل.

● تمكين المريض من موقع أكثر فاعلية في إدارة بياناته

واحدة من أهم النقالات التي تُنسب إلى تقنيات البلوك تشين في الصحة أنها لا تُبقي المريض موضوعًا سلبيًا لتداول بياناته، بل ترفعه إلى موقع الطرف الذي يمكنه الإذن أو المنع أو التخصيص أو التتبع. وهذا التحول مهم من الناحية الأخلاقية والإدارية، لأنه يعيد التوازن إلى العلاقة بين المؤسسة الحافظة للبيانات

وصاحب البيانات، ويفتح الباب أمام نماذج مشاركة قائمة على الموافقة الواعية لا على الإذعان التنظيمي (Esmaeilzadeh, 2022).

⦿ دعم التحول الرقمي الصحي على أسس أكثر استدامة

إن التحول الرقمي لا ينجح بمجرد رقمنة الملفات أو ربط الأنظمة، بل يحتاج إلى بنى تقنية قادرة على الاستمرار تحت ضغط التوسع والتنوع والتشبيك. وفي هذا السياق، تُقدّم سلاسل الكتل باعتبارها إحدى ركائز التحول الرقمي التي يمكن أن تخفض الاعتماد على الوساطة، وتحسن سرعة الأداء، وتدعم بناء شبكات أكثر مرونة في تبادل البيانات والمعلومات عبر المؤسسات (عبدالله، ٢٠٢٣).

⦿ المواءمة بين مشاركة البيانات ومتطلبات الخصوصية والأمن

تتبع أهمية هذا المتغير أيضًا من كونه يحاول حل المفارقة التي كثيرًا ما واجهتها المؤسسات الصحية: فكلما زادت قيمة مشاركة البيانات زادت المخاوف من تسربها أو إساءة استخدامها. وتظهر أدبيات الرعاية الصحية أن البلوك تشين تُطرح كحلٍ يتيح الجمع بين إتاحة البيانات للأغراض المشروعة وحمايتها عبر التشفير، واللامركزية، والتحكم في الوصول، وعدم القابلية للتعديل، وهو ما يجعلها ذات أهمية خاصة في نظم إدارة البيانات الصحية الحساسة. (Adeghe et al., 2024)

رأي الباحث في أهمية المتغير

يرى الباحث أن أهمية تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية لا تتحدد فقط في "أمن المعلومات" بالمعنى الضيق، بل في إعادة تأسيس الشرعية الإدارية للمشاركة؛ لأن مشاركة البيانات حين تجري ضمن بنية غير واضحة للصلاحيات والمساءلة قد تتحول من ميزة تنظيمية إلى مصدر دائم للمخاطر. أما حين تُبنى على التشفير اللامركزي، والعقود الذكية، وتتبع السجل، والموافقة الموثقة، فإنها تصبح أداة استراتيجية لتحسين الحوكمة الصحية، وتعزيز الثقة، ورفع كفاءة القرار.

4.1.2 أهداف تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

عند تحليل الكتابات التي تناولت البلوك تشين في البيئات المؤسسية والصحية، يتضح أن أهداف التطبيق لا تنحصر في هدف تقني مباشر، بل تتوزع بين أهداف تنظيمية، وأمنية، وحوكومية، وتشغيلية. ويمكن عرض أهم هذه الأهداف في ضوء آراء الباحثين على النحو الآتي:

● بناء بيئة مشاركة صحية آمنة وقابلة للتحقق

تُظهر الأدبيات أن الهدف الأول من توظيف البلوك تشين في مجال البيانات الصحية يتمثل في إنشاء بيئة مشاركة يمكن الوثوق بها، بحيث تكون كل عملية وصول أو تبادل أو تحديث قابلة للتوثيق والتحقق والمراجعة، دون التضحية بمرونة الاستعمال أو بتعدد الجهات المنتفعة من البيانات. وهذا الهدف يرتبط بحماية مسار المعلومة أكثر من ارتباطه بحماية مكان تخزينها فقط، لأن الخلل كثيرًا ما يقع أثناء التبادل لا أثناء الحفظ.

● تقليل الاعتماد على البنى المركزية في إدارة البيانات

يتمثل هدف ثانٍ في نقل إدارة تبادل البيانات من نموذج مركزي قد يعاني من بطء الإجراءات أو هشاشة نقطة الفشل الواحدة إلى نموذج موزع يتيح توزيع الثقة والمهام والتحقق بين أكثر من طرف. وهو هدف ذو أبعاد إدارية مهمة؛ لأنه يحرر مشاركة البيانات من القيود التي تفرضها المركزية المفرطة، دون أن يطلقها بلا ضوابط، بل يعيد ضبطها وفق منطق الشبكات الآمنة. (Yaqoob et al., 2022)

● تمكين الاستخدام المشروع للبيانات مع المحافظة على السيادة الفردية عليها

يتصل هذا الهدف بتمكين المريض أو صاحب البيانات من التحكم في حدود الاستفادة من معلوماته الصحية، ومنح الإذن بالوصول أو سحبه أو تقييده بحسب الغرض والجهة والمدة. ويكتسب هذا الهدف قيمة خاصة في البيانات التي تتزايد فيها الحاجة إلى مشاركة البيانات لأغراض علاجية أو بحثية أو تنظيمية، من دون أن يعني ذلك ذوبان حق الفرد في التحكم ببياناته أو إفقادها طابعها الشخصي (Masood et al., 2024).

5.1.2 الأبعاد النظرية لتطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

استنادًا إلى طبيعة المتغير محل الدراسة، وإلى الزوايا المفاهيمية الواردة في الأدبيات التي تناولت البلوك تشين في إدارة البيانات الصحية، يمكن تحديد أبعاد المتغير المستقل في أربعة أبعاد رئيسية هي :
التشغيل اللامركزي للبيانات، والعقود الذكية للتحكم في الوصول، وسلامة البيانات وعدم قابليتها للتعديل، وآليات إدارة الموافقة والتفويض. وقد جاء هذا التحديد في ضوء ما أبرزته الأدبيات من أن جوهر القيمة المضافة للبلوك تشين في المجال الصحي يتأسس على الجمع بين اللامركزية والحماية التشغيلية، وضبط

الوصول، وصيانة السجل، وحوكمة الإذن بالمشاركة (Yaqoob et al., 2022; Shojaei et al., 2024).

البعد الأول: التشفير اللامركزي للبيانات

يُقصد بالتشفير اللامركزي للبيانات ذلك النمط من الحماية الذي لا يعتمد على مركز واحد يحتفظ بنسخة وحيدة من الحقيقة الرقمية أو بمفتاح التحكم الكامل فيها، وإنما يوزع عناصر الحفظ والتحقق والتصديق بطريقة تجعل البيانات -أو على الأقل مؤشرات الوصول إليها وبياناتها الوصفية- جزءًا من شبكة موزعة تحكمها مفاتيح تشفير وسجلات تحقق متسلسلة. وتكمن القيمة النظرية لهذا البعد في أنه يبذل منطق الحماية من "التحصين حول مركز" إلى "التحصين عبر البنية"، وهو ما يحد من هشاشة الاعتماد على مستودع واحد أو خادم واحد أو جهة واحدة للنفاد الكامل.

وفي البيئة الصحية، تتعاضد أهمية هذا البعد لأن البيانات الصحية ليست متجانسة من حيث الشكل أو المصدر أو درجة الحساسية؛ فهي تشمل سجلات نصية، وتقارير، وصورًا، ونتائج مختبرية، ووثائق تعريفية، ومؤشرات سريرية. ومن ثم فإن الحماية الفاعلة لا تكون بمجرد قفل تقني عام، بل بنموذج تشفير يواكب تعدد الطبقات، ويضمن أن يكون الوصول إلى البيانات أو إعادة استخدامها خاضعًا لمفاتيح وصلاحيات وتوقعات يمكن التحقق منها. وفي هذا السياق، تبرز النماذج التي تجمع بين البلوك تشين والتخزين خارج السلسلة، مع حفظ المؤشرات المرجعية والهشاشات والبيانات الوصفية على السلسلة، بما يوفر توازنًا بين أمن الحفظ وقابلية التوسع والقدرة على الاستدعاء المنضبط. (Vanin et al., 2022)

ويؤسس هذا البعد أيضًا لفكرة أن الخصوصية لا تتحقق فقط بمنع الوصول، بل بإعادة تعريف منطق المعالجة نفسها. فالتشفير المتقدم، ولا سيما حين يقترن ببنى تسمح ببعض أشكال التحليل على البيانات المشفرة أو بإعادة التشفير عند الطلب، يفتح المجال أمام مشاركة منضبطة تحقق الاستفادة العلاجية أو البحثية دون كشف غير لازم للبيانات الخام. وهذا يجعل التشفير اللامركزي بعدًا أعمق من كونه حماية تقنية؛ إذ يغدو أداة لإدارة المفاضلة بين الإتاحة والسرية داخل النظام الصحي. (Masood et al., 2024)

ومن منظور الباحث، فإن التشفير اللامركزي يمثل الأساس البنيوي الأول لتطبيق البلوك تشين في مشاركة البيانات الصحية؛ لأنه يضعف احتمالات الاختراق المرتبطة بالتركيز المفرط للبيانات، ويمنح عملية المشاركة بعدًا سياديًا يربط الوصول بالمفاتيح والضوابط لا بالمكان المادي للتخزين فقط. ولهذا فإن قياس

هذا البعد داخل الدراسة الحالية يعد لازماً لفهم مدى إدراك المؤسسات الصحية لأهمية توزيع الحماية عبر البنية وليس الاكتفاء بحماية تقليدية محيطة بالنظام.(Adusumilli et al., 2023)

البعد الثاني: العقود الذكية للتحكم في الوصول

يُعد التحكم في الوصول من أكثر القضايا حساسية في مشاركة البيانات الصحية، لأن السؤال الجوهرى ليس هل تُشارك البيانات أم لا، وإنما من له حق الاطلاع عليها، ولأي غرض، وتحت أي قيد زمني أو وظيفي. وفي هذا الموضع تتقدم العقود الذكية بوصفها بعداً محورياً من أبعاد تطبيق البلوك تشين؛ لأنها تحول قواعد الوصول من تعليمات إدارية قابلة للاجتهاد أو الإغفال إلى شروط مبرمجة تُنفَّذ آلياً عند تحقق متطلبات محددة سلفاً. وبذلك يصبح الوصول إلى البيانات جزءاً من منطق تشغيلي محسوب لا من قرار أنى قد يتفاوت من حالة إلى أخرى.

ومن الناحية الإدارية، تسمح العقود الذكية بتحويل سياسات مشاركة البيانات إلى نماذج تشغيلية أكثر دقة؛ إذ يمكن من خلالها تقييد الوصول بحسب الدور المهني، أو طبيعة الحالة، أو الغرض البحثي، أو مدة الإتاحة، أو موافقة صاحب البيانات، أو اكتمال متطلبات التحقق. وهذه المرونة المنظمة تُعد من أهم مزايا البلوك تشين في البيئات الصحية التي تتقاطع فيها حاجات أطباء، وإداريين، وباحثين، ومختبرات، وجهات تنظيمية، ولكل منها مستوى مختلف من الاحتياج إلى البيانات.(Handayani et al., 2023)

كما أن هذا البعد يوفر أساساً مهماً للمساءلة؛ لأن كل تفعيل للعقد الذكي يترك أثراً يمكن تتبعه، وكل إذن أو رفض يصبح جزءاً من السجل، بما يمنع الغموض الذي قد ينشأ في الأنظمة التقليدية حول مصدر القرار أو توقيته أو مشروعيته. ومن هنا تتقاطع العقود الذكية مع متطلبات الشفافية والرقابة الداخلية والتدقيق اللاحق، فضلاً عن دورها في تقليص التفاوت البشري في تفسير قواعد الإتاحة والوصول (Adeghe et al., 2024).

ويرى الباحث أن العقود الذكية للتحكم في الوصول لا تمثل مجرد تطبيق فرعي داخل البلوك تشين، بل تمثل الترجمة العملية للحوكمة الرقمية في مجال مشاركة البيانات الصحية؛ إذ بها تنتقل المؤسسة من سياسات مكتوبة قد لا تُطبَّق على نحو متسق، إلى بيئة تشغيلية تنفذ فيها قواعد المشاركة آلياً وبصورة قابلة للتحقق والمراجعة. ومن ثم فإن هذا البعد يُعدّ مؤشراً حاسماً على نضج التطبيق المؤسسي للبلوك تشين في المجال الصحي.

البعد الثالث: سلامة البيانات وعدم قابليتها للتعديل

تُعد سلامة البيانات أحد المرتكزات الجوهرية في أي نظام للمعلومات الصحية؛ لأن قيمة البيانات لا تنفصل عن الثقة في أنها لم تُحرّف، ولم تُستبدل، ولم تُسحب من سياقها الزمني أو المهني. وفي الأنظمة التقليدية قد يصعب أحيانًا التحقق من مصدر التعديل، أو النسخة المعتمدة، أو ترتيب التغييرات، خاصة عندما تتعدد الجهات المتعاملة مع السجل. أما في بيئة البلوك تشين فإن إحدى أهم الخصائص التي تستند إليها الأدبيات هي خاصية عدم القابلية للتعديل؛ أي أن البيانات المسجلة في السلسلة -أو بصياغة أدق، آثارها ومرجعياتها التوثيقية- تصبح جزءًا من سجل مترابط تشفيريًا، بحيث يؤدي أي عبث لاحق إلى كسر قابلية التوافق أو ظهور أثر واضح للتغيير (عبدالقادر، ٢٠٢٢).

ولا تقتصر أهمية هذا البعد على الحماية التقنية، بل تمتد إلى دعم الموثوقية التنظيمية. فالبيانات الصحية تُستخدم لاتخاذ قرارات علاجية، وبناء تقارير، وإجراء مراجعات، وتدقيقات، ومتابعات قانونية، وأبحاث علمية؛ ومن ثم فإن سلامتها ليست شأنًا أرسيفيًا، بل شرط لسلامة القرار نفسه. ولهذا تربط بعض الكتابات بين البلوك تشين وجودة التقارير أو قوة أدلة المراجعة أو فعالية الرقابة، لأن السجل غير القابل للتعديل يعزز الثقة في أن البيانات المحتفظ بها أو المتبادلة يمكن الاستناد إليها دون خشية من التلاعب الخفي أو التغيير غير الموثق (الخرابشة وآخرون، ٢٠٢٤).

كما أنّ هذا البعد يمتلك قيمة خاصة في السياقات التي يكون فيها الحفاظ على الأصل أو النسخة المرجعية جزءًا من وظيفة النظام، كما في الوثائق النادرة والمخطوطات والمواد التي تتطلب توثيق الملكية والأصالة والتتبع. ورغم اختلاف المجال التطبيقي، فإن المنطق النظري واحد: البلوك تشين تُستخدم حين تكون الحاجة ملحة إلى إثبات سلامة الأصل، وتتبع التداول، وصيانة الثقة في المصدر. وهذا المعنى يمكن نقله بوضوح إلى البيئة الصحية حيث تكون "أصالة السجل" و"صحة التتبع" من شروط التبادل الآمن للبيانات (الفهمي وآخرون، ٢٠٢٥).

ويرى الباحث أن سلامة البيانات وعدم قابليتها للتعديل تمثل البعد الأكثر التصاقًا بالثقة المؤسسية طويلة المدى في نظم مشاركة البيانات الصحية؛ لأنها تضمن أن تبادل البيانات لا يقتصر على النقل الآمن، بل يتضمن كذلك الحفاظ على القيمة الإثباتية والتاريخية والمعرفية للسجل الصحي. ومن ثم فإن ضعف هذا البعد يفرغ أي نظام مشاركة -مهما كان متقدمًا في السرعة والربط- من معناه الحوكمي والمهني.

البعد الرابع: آليات إدارة الموافقة والتفويض

إذا كانت سلاسل الكتل تُعيد تنظيم أمن البيانات وسلامتها، فإن أحد أكثر أوجهها حساسية في البيئة الصحية يتمثل في قدرتها على إعادة بناء منطق الموافقة. ذلك أن الموافقة في النظم الصحية لم تعد مسألة نمطية تُستحصل مرة واحدة ثم تُفهم على أنها إذن مفتوح، بل أصبحت أقرب إلى عملية متدرجة، مشروطة، ومقيدة بالغرض، والزمن، والجهة، ومستوى الإتاحة. ومن هنا تبرز آليات إدارة الموافقة والتفويض بوصفها بعدًا قائمًا بذاته في تطبيق البلوك تشين؛ لأن التقنية تتيح توثيق الإذن، وربطه بطرف محدد، وربما بتخزين زمني مؤقت أو تفويض قابل للانتهاء، مع الاحتفاظ بسجل قابل للمراجعة حول منح الإذن أو سحبه.

وتتبنى أهمية هذا البعد على أن مشاركة البيانات الصحية لا يمكن أن تكون مشروعة ومستدامة ما لم يكن صاحب البيانات طرفًا حاضرًا في معادلة القرار، لا مجرد موضوع يتم التداول بشأنه. ولهذا تشير بعض الأدبيات إلى مزايا البلوك تشين في دعم السيطرة الفردية على البيانات، وتوسيع قدرة المرضى على الإشراف على من يطلب البيانات الصحية وكيفية استخدامها، مع موازنة ذلك بمتطلبات التشغيل والتكامل داخل النظام الصحي. (Esmaeilzadeh, 2022)

ومن أكثر الطروحات عمقًا في هذا الشأن تلك التي تدمج بين البلوك تشين وإدارة المفاتيح الفردية، والتخزين المؤقت المشترك، وإعادة التشفير عند الطلب، بحيث يُفهم التفويض ليس بوصفه قرارًا إداريًا خارجيًا، بل بوصفه ممارسة تقنية-حقوقية يتدخل فيها الفرد نفسه عبر مفاتيحه وصلاحياته ومدة الإتاحة الممنوحة. وهذا يعزز فكرة أن الموافقة ليست وثيقة صامته، وإنما آلية تشغيل حية ترتبط بكل عملية مشاركة على حدة. (Vanin et al., 2022).

كما يكتسب هذا البعد بعدًا مستقبليًا مهمًا مع الطروحات التي تمزج بين مشاركة البيانات اللامركزية وتقنيات أشد تعقيدًا مثل التعلم الاتحادي أو البروتوكولات الحافظة للخصوصية القائمة على التشفير والبلوك تشين؛ إذ يصبح من الممكن الاستفادة من البيانات أو من نماذجها المستخلصة دون اللجوء إلى كشفها الكامل أو نقلها نقلًا خامًا، وهو ما يوسع معنى التفويض من مجرد "السماح بالوصول" إلى "السماح بنوع معين من الاستفادة تحت حدود تقنية مضبوطة". (Alsamhi et al., 2024; Afrihyia et al., 2025)

رأي الباحث في الأبعاد

يرى الباحث أن هذه الأبعاد الأربعة لا تمثل مكونات متجاوزة فحسب، بل تمثل بنية مترابطة؛ فالتشفير اللامركزي يؤسس الحماية البنيوية، والعقود الذكية تنظّم الوصول، وسلامة البيانات تصون القيمة الإثباتية والمعرفية للسجل، وآليات الموافقة والتفويض تمنح التطبيق مشروعته الأخلاقية والحقوقية. ومن ثم فإن دراسة أثر تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية تقتضي التعامل مع هذه الأبعاد بوصفها مكونات متكاملة يتعذر فصل أحدها عن الآخر دون الإخلال بالمنطق الكلي للتقنية.

6.1.2 المداخل النظرية الحاكمة لتطبيق البلوك تشين في مشاركة البيانات الصحية

يمكن النظر إلى تطبيق البلوك تشين في هذا المجال عبر ثلاثة مداخل متكاملة. المدخل الأول هو مدخل الحوكمة الرقمية، الذي يرى أن القيمة الأساسية للتقنية تكمن في ضبط القواعد والإجراءات ومسؤوليات الأطراف بما يحقق الشفافية والمساءلة وقابلية التتبع. والمدخل الثاني هو مدخل الأمن المعلوماتي، الذي يركز على التشفير، وعدم القابلية للتعديل، وتقليل فرص الاختراق والتسرب. أما المدخل الثالث فهو مدخل التمكين المؤسسي والحقوق، الذي يربط بين استخدام التقنية وبين تعزيز حق المريض في إدارة بياناته، وإعادة تعريف العلاقة بين المؤسسة والبيانات على أساس الثقة المنظّمة لا السيطرة الأحادية. وتكمن قوة هذا المتغير في أنه يجمع بين هذه المداخل ولا يكتفي بواحد منها (الزهراني، ٢٠٢٤).

7.1.2 خاتمة المبحث الأول

يتضح مما سبق أن تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية يمثل متغيراً ذا طبيعة مركبة؛ فهو تقني في أدواته، وتنظيمي في آثاره، وأمني في مبرراته، وحقوق في غاياته. ولذلك لم يعد مقبولاً النظر إلى مشاركة البيانات الصحية باعتبارها إجراءً تشغيلياً خالصاً، بل باعتبارها قضية حوكمة وثقة وسيادة على المعلومة. ومن هذا المنطلق جاء بناء المتغير المستقل في الدراسة الحالية على أربعة أبعاد تعكس جوهر التطبيق الواقعي للبلوك تشين في البيئة الصحية، وهي: التشفير اللامركزي، والعقود الذكية للتحكم في الوصول، وسلامة البيانات وعدم قابليتها للتعديل، وآليات إدارة الموافقة والتفويض. وهذه الأبعاد، متى توافرت وتكاملت، أمكن توقع أثرها في خفض مخاطر الخصوصية وتسرب البيانات، وهو ما يمهد منطقياً للانتقال إلى المبحث الثاني.

المبحث الثاني: المتغير التابع "خفض مخاطر الخصوصية وتسرب البيانات"

1.2.2 تمهيد

إذا كان التوسع في مشاركة البيانات الصحية يعكس نضجاً في البنية الرقمية للمؤسسات الصحية، فإنه في الوقت نفسه يضاعف حساسية سؤال الخصوصية. فالبيانات الصحية ليست مجرد سجلات تشغيلية، بل هي تمثيل رقمي لحياة الأفراد الجسدية والنفسية والتاريخية، وما يرتبط بها من تشخيصات، وعلاجات، ونتائج فحوص، وبيانات تعريفية، ومسارات علاجية، وقد تتضمن في بعض الأحيان معلومات عائلية أو وراثية أو سلوكية ذات حساسية مضاعفة. ولهذا فإن أي خلل في حماية هذه البيانات لا يقتصر أثره على المجال التقني، بل يمتد إلى المجال الأخلاقي والقانوني والمؤسسي، ويؤثر في ثقة المرضى، وفي شرعية المؤسسة، وفي جودة القرار الصحي ذاته.

ومن هنا يتحدد المتغير التابع في الدراسة الحالية في خفض مخاطر الخصوصية وتسرب البيانات، لا بوصفه مجرد غياب للحوادث أو الانتهاكات، بل بوصفه حالة تنظيمية وتقنية تعكس قدرة المؤسسة الصحية على الحد من احتمالات الوصول غير المصرح به، وتقليص فرص التلاعب أو التسريب أو الإفصاح غير المشروع، وتعزيز التحكم في التدفقات المعلوماتية، وبناء بيئة تحفظ البيانات أثناء التخزين والنقل والاستخدام والمشاركة. وهذا المتغير يتسم بطابع تراكمي؛ لأنه لا يتحقق بإجراء معزول، بل بمنظومة من الضوابط والبنى والآليات والثقافة المؤسسية.

كما أن خصوصية البيانات الصحية لم تعد مفهوماً قانونياً محضاً، بل أصبحت جزءاً من الأمن الصحي الرقمي، ومن ثم فإن خفض المخاطر المرتبطة بها يُعدّ شرطاً لتوسيع الاستفادة من البيانات نفسها. فكلما تزايدت قدرة المؤسسة على تقليل مخاطر الخصوصية والتسرب، اتسع المجال أمام الاستخدام المشروع للبيانات في التشخيص والتكامل والبحث والتخطيط. أما إذا ظلت المخاطر مرتفعة، فإن البيانات تتحول من أصل استراتيجي إلى عبء تنظيمي يحد من قابلية الاستفادة منها.

2.2.2 مفهوم خفض مخاطر الخصوصية وتسرب البيانات

يقوم مفهوم الخصوصية في السياق الصحي على حق الفرد في أن تُجمع بياناته وتُستخدم وتُشارك ضمن حدود مشروعة ومعلومة ومقيدة بالغرض، وأن يُصان محتواها من الكشف غير المبرر أو الوصول

غير المصرح به. أما تسرب البيانات فيرتبط بكل انتقال غير مشروع أو غير منضبط للبيانات من دائرة الحفظ أو الاستخدام المصرح بها إلى أطراف أو قنوات أو سياقات لا يخولها النظام أو صاحب البيانات. وبناءً على ذلك، فإن خفض مخاطر الخصوصية وتسرب البيانات لا يعني فقط منع "الاختراق الخارجي"، بل يشمل كذلك تقليل الثغرات الإدارية، وضعف الحوكمة، وسوء إدارة الصلاحيات، وغموض سياسات المشاركة، وقصور التتبع، وكل ما من شأنه أن يفتح ثغرة أمام الإفشاء أو التسريب أو الاستخدام غير المنضبط.

وتشير الأدبيات الحديثة في نظم المعلومات الصحية إلى أن بيانات المرضى حساسة بطبيعتها، وأن تعرضها للانتهاك يمكن أن يقود إلى نتائج خطيرة من قبيل سرقة الهوية، والاحتيال، وسوء الاستخدام، والإضرار بجودة الخدمات، فضلاً عن تآكل ثقة الأفراد في المؤسسات الحافظة للبيانات. ولهذا تركز المراجعات المنهجية في هذا المجال على ثلاثة محاور متلازمة: التحكم الآمن في الوصول، ومشاركة البيانات الآمنة، والتخزين الآمن للبيانات، بوصفها المجالات الرئيسية التي تتولد منها مخاطر الخصوصية أو تتراجع عبرها. (Shojaei et al., 2024)

وفي السياق العربي، يظهر المفهوم مقرونًا غالبًا بالحاجة إلى الموازنة بين مشاركة المعرفة الصحية وبين ضمان الأمن والخصوصية، بما يعني أن الخصوصية لا تُفهم كحالة انغلاق معلوماتي، بل كشرط لشرعية المشاركة نفسها. فكلما تعددت مصادر البيانات واتسعت قنوات تبادلها بين الأنظمة والمنصات، برزت الحاجة إلى أطر أكثر وضوحًا لحوكمة البيانات والمعرفة الصحية، بما يضمن استمرار الفائدة من المشاركة مع الحد من المخاطر الملازمة لها (العنزي والرابعي، ٢٠٢٥).

أما من منظور تقني، فإن خفض مخاطر الخصوصية يعني تقليل تعرض البيانات للحالات الآتية: الوصول غير المصرح به، النسخ غير المنضبط، التعديل الخفي، إعادة الاستخدام خارج الغرض، ضعف تتبع العمليات، هشاشة التخزين، وتشتت المسؤولية بين أطراف عديدة دون سجل واضح للقرار. ولذلك فإن هذا المتغير لا يقاس فقط بوجود نظام أمني، بل بمدى فعالية النظام في إحكام حلقات الحماية على طول دورة حياة البيانات. ومن هنا تكتسب مفاهيم مثل التشفير، والعقود الذكية، وإدارة المفاتيح، والتوقيع الرقمي، والرقابة الداخلية، والتوثيق الزمني، قيمة مفهومية مباشرة في تفسير هذا المتغير.

رأي الباحث

يرى الباحث أن خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية هو: تقليص احتمالات كشف البيانات الصحية أو تداولها أو تعديلها أو الوصول إليها خارج الإطار المصرح به، عبر ضوابط تقنية وتنظيمية تضمن السرية، والتحكم في الوصول، وقابلية التتبع، وسلامة الحفظ، ومشروعية الاستخدام. ووفق هذا الفهم، فإن المتغير التابع لا يقتصر على البعد الأمني الضيق، بل يشمل القدرة المؤسسية على ضبط التفاعل الكامل مع البيانات الصحية.

3.2.2 أهمية خفض مخاطر الخصوصية وتسرب البيانات

تتبع أهمية هذا المتغير من كون الخصوصية ليست قيمة أخلاقية مجردة، بل هي شرط لاستدامة النظام الصحي الرقمي. فالمؤسسة التي لا تستطيع طمأنة المستفيدين والمهنيين إلى أن بياناتهم مصونة ومحكومة لا يمكنها أن تتوسع بأمان في التبادل الرقمي أو في التحليلات المتقدمة أو في التكامل بين الأنظمة. ومن هنا فإن خفض المخاطر لا يُعدّ هدفًا دفاعيًا فقط، بل هدفًا تمكينيًا يسمح للنظام الصحي بأن يتقدم دون أن يفقد مشروعيته المجتمعية.

ويشير بعض الباحثين إلى أن إدارة المخاطر في البيئات الرقمية المعاصرة لا تتحقق إلا من خلال أطر حوكمة قادرة على ترجمة المبادئ إلى ضوابط، بما يشمل الشفافية، والأمان، واحترام الخصوصية، والعدالة، وعدم الانحياز، والمساءلة. ورغم أن هذا الطرح ورد في سياق حوكمة أخلاقيات الذكاء الاصطناعي، فإن قيمته النظرية تمتد إلى حماية البيانات الصحية؛ لأن جوهره يتمثل في أن التقنية كلما ازدادت قوة وتأثيرًا ازدادت الحاجة إلى حوكمة أخلاقية ومؤسسية تضبط المخاطر الملازمة لها (عبدالله، ٢٠٢٤).

ويمكن إبراز أهمية خفض مخاطر الخصوصية وتسرب البيانات من خلال الجوانب الآتية:

حماية الثقة بين المريض والمؤسسة الصحية

الثقة في القطاع الصحي لا تُبنى فقط على الكفاءة الطبية، بل على الاطمئنان إلى أن المعلومات الشخصية لن تتحول إلى مصدر انكشاف أو استغلال. فإذا شعر الأفراد أن بياناتهم عرضة للتسرب أو الاطلاع غير المشروع، فإن ذلك يضعف استعدادهم للإفصاح الكامل عن المعلومات، ويؤثر بصورة غير مباشرة في دقة التشخيص، وجودة الرعاية، وسلامة التواصل مع النظام الصحي.

⦿ دعم فعالية الرقابة والضبط المؤسسي

إن المؤسسات التي تتجح في خفض مخاطر الخصوصية والتسرب هي عادة المؤسسات التي تمتلك هياكل رقابية أكثر نضجًا، ومسارات أوضح للمساءلة، وقدرة أعلى على التوثيق والتتبع. ولذلك يرتبط هذا المتغير بفعالية نظام الرقابة الداخلية، من حيث دقة البيانات، وتتبع المعاملات، والفصل بين المسؤوليات، والتقارير الرقابية، والمراجعة المستمرة، وهي جميعًا عناصر تجعل من حماية الخصوصية جزءًا من البنية الرقابية لا مهمة منفصلة عنها (محمد، ٢٠٢٥).

⦿ تقليل المخاطر التشغيلية والاحتياطية

لا يتسبب تسرب البيانات في انتهاك الخصوصية وحده، بل قد يفتح مسارات لاحقة للاحتيال، أو التلاعب، أو إساءة الاستفادة من المعلومات، أو استنزاف الموارد في التحقيق والمعالجة واستعادة الثقة. ومن ثم فإن خفض هذا النوع من المخاطر يحمل قيمة تشغيلية واضحة؛ لأنه يحمي المؤسسة من آثار مترابطة قد تبدأ بتسريب بسيط وتنتهي بخسائر أوسع في الكفاءة والسمعة والاستقرار الإجرائي (عبده، ٢٠٢٣).

⦿ تمكين الاستخدام المشروع والواسع للبيانات

كلما انخفضت مخاطر الخصوصية أمكن توسيع مجالات الاستفادة المشروعة من البيانات الصحية في البحث، والتخطيط، والربط بين مستويات الرعاية، والمتابعة السريرية، وصناعة القرار. أما حين تبقى المخاطر مرتفعة، فإن النزعة الغالبة تكون إما نحو التشدد في الحجب أو نحو الانكشاف غير المنظم، وكلاهما يضر بالنظام. وعليه، فإن خفض المخاطر ليس نقيضًا للمشاركة، بل هو شرط لترشيدها واستدامتها.

⦿ تعزيز الامتثال وحوكمة القرار المعلوماتي

كل مؤسسة صحية رقمية تحتاج إلى أن تعرف من قرر، ومن أذن، ومن نفذ، ومن وصل، ومتى تم ذلك، ولماذا. وخفض مخاطر الخصوصية يجعل هذا الامتثال أكثر قابلية للتنفيذ، لأنه يحول الحماية من مبادئ عامة إلى سلوك معلوماتي موثق، وهو ما تحتاج إليه المؤسسات التي تعمل في بيئات عالية الحساسية كالمؤسسات الصحية.

يرى الباحث أن خفض مخاطر الخصوصية وتسرب البيانات ليس مخرجًا جانبيًا لتطبيق البلوك تشين أو التحول الرقمي، بل هو المعيار الحقيقي لنجاحهما؛ لأن أي توسع في مشاركة البيانات الصحية لا يُقاس فقط بما أتاحه من اتصال أو سرعة أو تكامل، وإنما بما إذا كان قد خفّض في المقابل احتمالات الانكشاف والعبث والوصول غير المشروع. ومن ثم فإن هذا المتغير يُعدّ مقياسًا نوعيًا لمستوى نضج الحوكمة المعلوماتية في المؤسسات الصحية.

4.1.2 أهداف خفض مخاطر الخصوصية وتسرب البيانات

يمكن عرض أهداف هذا المتغير في ثلاثة اتجاهات مترابطة:

• صون السرية المشروعة للبيانات الصحية

الهدف الأول يتمثل في الإبقاء على البيانات الصحية ضمن حدود السرية التي تتفق مع طبيعتها الحساسة، بحيث لا تُتاح إلا لمن يملك مسوغًا وظيفيًا أو نظاميًا أو علاجيًا أو بحثيًا مشروعًا. وهذا الهدف لا يتعلق فقط بإخفاء البيانات، بل بإدارة إتاحتها على نحو دقيق ومتدرج.

• ضبط دورة حياة البيانات ومنع الانفلات المعلوماتي

الهدف الثاني هو جعل البيانات قابلة للتتبع منذ لحظة إنشائها أو جمعها، مرورًا بتخزينها وتحديثها ومشاركتها واستخدامها، وصولًا إلى حفظها أو إتلافها أو إنهاء التفويض المرتبط بها. وبذلك ينخفض هامش العمليات غير المرئية التي كثيرًا ما تكون مصدرًا للتسرب أو سوء الاستخدام.

• بناء بيئة صحية رقمية قابلة للتوسع بثقة

الهدف الثالث يتصل بالمستقبل المؤسسي للقطاع الصحي؛ إذ لا يمكن بناء بيئة صحية رقمية واسعة النطاق تعتمد على التكامل والبحث والتحليلات دون وجود أساس صلب لحماية الخصوصية. ومن ثم فإن خفض المخاطر ليس غاية تحوطية فحسب، بل هدف تمكيني يدعم التوسع الآمن في الاستخدامات الرقمية للبيانات الصحية. (Chianumba et al., 2022)

5.1.2 المضمون النظري لمخاطر الخصوصية وتسرب البيانات الصحية

من المهم في هذا الموضع أن يُفهم المتغير التابع من خلال المخاطر التي يسعى إلى خفضها. فأولى هذه المخاطر هي مخاطر الوصول غير المصرح به، وهي تنشأ عندما تكون ضوابط الهوية والصلاحيات ضعيفة أو غير متميزة أو غير موثقة على نحو كافٍ. وهذه المخاطر لا تقتصر على الجهات الخارجية، بل قد تنشأ من الداخل المؤسسي حين تتسع الصلاحيات أو تغيب آليات الفصل بين المسؤوليات.

وثانيها مخاطر الإفصاح أو التسرب أثناء المشاركة، وتظهر عندما تنتقل البيانات عبر قنوات أو منصات أو وسائط لا تضمن السرية الكافية، أو حين لا تكون شروط التبادل محددة بدقة، أو حين يُعاد استخدام البيانات خارج الغرض الأصلي الذي جُمعت لأجله. وفي البيئات الصحية المتكاملة، تمثل هذه المخاطر تحديًا خاصًا لأن الحاجة إلى المشاركة مرتفعة، لكن حساسيتها كذلك مرتفعة.

وثالثها مخاطر سلامة البيانات، أي احتمال أن تخضع البيانات لتعديل غير مشروع أو غير موثق أو أن يحدث تعارض بين النسخ أو ضعف في إمكانية التحقق من النسخة الأصلية المعتمدة. وهذه المخاطر تمس الخصوصية بصورة غير مباشرة أيضًا؛ لأن العبث بالبيانات قد يُستغل لإخفاء الوصول أو تشويه السجل أو إساءة استخدامه.

ورابعها مخاطر الحوكمة والتفويض، وتتمثل في ضعف توثيق الموافقة، أو غموض السلطة المخولة بمنح الإذن، أو غياب حدود زمنية أو وظيفية واضحة للوصول، أو انعدام سجلات دقيقة حول من اطلع على البيانات ومتى ولماذا. وهذه الفئة من المخاطر ذات طابع تنظيمي وأخلاقي بقدر ما هي تقنية.

أما خامسها فهو مخاطر الاستدامة والثقة؛ إذ إن تكرار الانتهاكات أو هشاشة الحماية يؤديان إلى تآكل الثقة، وهذا بدوره ينعكس على الامتثال، واستعداد الأفراد والمؤسسات للمشاركة، وجودة البيانات نفسها. ومن هنا فإن المتغير التابع في هذه الدراسة ينبغي أن يُقرأ بوصفه مؤشرًا على قدرة المؤسسة على ضبط هذه الطبقات المختلفة من المخاطر، لا مجرد الاستجابة لحوادث منفردة.

6.1.2 المحاور المؤسسية لخفض مخاطر الخصوصية وتسرب البيانات

رغم أن المتغير التابع في الدراسة الحالية يُعامل إحصائيًا بوصفه محورًا أحاديًا، فإن مضمونه النظري يتشكل من عدة محاور مؤسسية متداخلة، يمكن من خلالها تفسير كيفية تحقق خفض المخاطر داخل المؤسسات الصحية.

⦿ محور الضبط الرقابي الداخلي

يتعلق هذا المحور بقدرة المؤسسة على بناء رقابة داخلية رقمية تتسم بالوضوح، والتوثيق، والفصل بين المسؤوليات، وتتبع المعاملات، ووجود تقارير رقابية تسمح بالكشف المبكر عن الانحرافات أو محاولات الوصول غير المصرح به. وتظهر قيمة هذا المحور حين تصبح حماية الخصوصية جزءًا من الهيكل الرقابي اليومي للمؤسسة، لا استجابة طارئة لحادث اختراق أو تسرب (محمد، ٢٠٢٥).

⦿ محور منع الاحتيال والانحرافات التشغيلية

يرتبط خفض مخاطر التسرب أيضًا بقدرة المؤسسة على الحد من القنوات التي يمكن أن تُستغل لاحقًا في الاحتيال أو في الاستفادة غير المشروعة من المعلومات. فكلما كانت العمليات أكثر قابلية للتتبع، وكلما انخفضت المعالجة اليدوية غير المنضبطة، وكلما زاد وضوح مسار البيانات بين الأطراف، قلّ المجال أمام الاستخدامات الاحتيالية أو الإخفاء أو التلاعب (عبد، ٢٠٢٣).

⦿ محور الحوكمة الأخلاقية للمعلومات الصحية

لا تكتمل حماية الخصوصية دون حضور بعد أخلاقي واضح يوجّه الضبط المؤسسي. فالخصوصية في هذا السياق ليست فقط مسألة تشفير وصلاحيات، بل مسألة احترام لحق الفرد، وإنصاف في التعامل مع بياناته، ووضوح في الغرض من استخدامها، ومساءلة عند الانحراف. ولذلك فإن خفض المخاطر يرتبط بوجود ثقافة حوكمة تجعل من حماية البيانات الصحية قيمة موجهة للسلوك التنظيمي، لا مجرد التزام شكلي (عبدالله، ٢٠٢٤).

⦿ محور التتبع والشفافية الإجرائية

تسرب البيانات غالبًا ما ينمو في البيئات التي يصعب فيها تتبع خطوات الوصول أو تبادل الملفات أو إعادة استخدامها. ولهذا فإن أي آلية ترفع من درجة الشفافية الإجرائية -سواء عبر سجلات زمنية، أو مسارات مراجعة، أو توثيق لكل عملية نفاذ أو مشاركة- تسهم نظريًا في خفض المخاطر، لأن قدرة الفاعل على التمويه أو الإنكار أو تعديل المسار دون أثر تصبح أضعف.

⦿ محور الاستدامة التنظيمية للثقة

خفض المخاطر ليس هدفًا لحظيًا، بل هو شرط لاستدامة الثقة داخل المؤسسة وبينها وبين المرضى والشركاء والباحثين. فالمؤسسة التي تنجح في ضبط مخاطر الخصوصية تبني رأسمًالاً معنويًا وتنظيميًا يسمح لها بالتوسع في التكامل والرقمنة والابتكار دون أن تدفع ثمنًا مرتفعًا من الشك المجتمعي أو الحذر المهني.

7.1.2 المؤشرات النظرية التي يفهم من خلالها خفض مخاطر الخصوصية وتسرب البيانات

يمكن فهم هذا المتغير نظريًا من خلال مجموعة مؤشرات دالة، حتى وإن كان سيُقاس في الاستبانة بوصفه محورًا واحدًا. ومن أهم هذه المؤشرات: انخفاض احتمالات الوصول غير المصرح به، ووضوح حدود الصلاحيات، وإمكانية تتبع من اطلع على البيانات، ووجود سجلات ثابتة للعمليات، وتقليل فرص التعديل غير المشروع، وارتفاع القدرة على التحقق من النسخ المعتمدة، وإحكام إدارة الموافقة، وانخفاض الاعتماد على وسائط غير آمنة للمشاركة، وتزايد قدرة المؤسسة على المراجعة اللاحقة والمساءلة. وهذه المؤشرات لا تعني بالضرورة وقوع حوادث أو عدم وقوعها، بل تعبر عن مدى نضج البيئة المؤسسية في تقليل احتمالاتها.

وفي هذا السياق، تبرز الأدبيات التي تربط الخصوصية بالتحكم في الوصول، والتشفير، والبروتوكولات الحافظة للخصوصية، والنماذج اللامركزية في مشاركة البيانات، باعتبارها تقدم أساسًا نظريًا لفهم كيف يمكن للمؤسسات الصحية أن تنتقل من "حماية تقليدية" إلى "حماية قائمة على التصميم"، أي حماية تُبنى في هندسة النظام ذاته لا تضاف إليه في مرحلة لاحقة. (Afrihyia et al., 2025)

كما أن الطروحات التي تمزج بين المشاركة اللامركزية والتعلم الاتحادي أو أشكال التحليل دون نقل البيانات الخام توسّع من مدلول خفض مخاطر التسرب؛ لأن تقليل حركة البيانات نفسها، أو تقليل الحاجة إلى كشفها الكامل، يعد في ذاته آلية وقائية متقدمة. وهنا يتضح أن خفض المخاطر لا يُفهم فقط بوصفه تشديدًا على القنوات الحالية، بل قد يعني أيضًا إعادة تصميم منطق الاستفادة من البيانات بحيث تصبح المشاركة أكثر نكاءً وأقل تعريضًا للمحتوى الحساس. (Alsamhi et al., 2024)

8.1.2 علاقة المتغير التابع ببيئة المؤسسات الصحية

تتسم المؤسسات الصحية بخصوصية تجعل خفض مخاطر الخصوصية وتسرب البيانات أكثر إلحاحًا مقارنة بكثير من القطاعات الأخرى. فالقرار الصحي قد يكون عاجلاً، والبيانات موزعة بين أقسام ومختبرات

ومستشفيات وجهات تأمين أو تنظيم أو بحث، كما أن الخطأ في الحماية لا يترتب عليه ضرر إداري فحسب، بل قد يترتب عليه ضرر علاجي أو اجتماعي أو قانوني. ولهذا لا يكفي في البيئة الصحية خطاب عام عن الأمن الرقمي؛ بل يلزم بناء حماية دقيقة تستجيب لتعدد المتعاملين مع البيانات واختلاف درجات الاحتياج إليها.

ومن هذه الزاوية، فإن خفض المخاطر يرتبط أيضًا بقدرة المؤسسة على منع التضارب بين الحاجة إلى السرعة في الوصول والحاجة إلى التحقق من مشروعية الوصول. كما يرتبط بقدرتها على تحقيق التوازن بين حق الطبيب أو الفريق العلاجي في المعلومات التي يحتاجها، وحق المريض في ألا تتحول بياناته إلى مورد متاح على نحو فضفاض. وهذا التوازن هو قلب الإشكال الذي تسعى الدراسة الحالية إلى معالجته من خلال اختبار أثر تطبيق البلوك تشين بأبعاده المختلفة.

9.1.2 خفض مخاطر الخصوصية وتسرب البيانات في ضوء المنظور الإداري

من منظور إدارة الأعمال، لا ينبغي النظر إلى هذا المتغير بوصفه تابعًا تقنيًا خالصًا، بل بوصفه متغيرًا يعكس جودة القرارات الإدارية المتعلقة بالبنية الرقمية، والحوكمة، والرقابة، وتوزيع المسؤوليات، وإدارة العمليات، وتخطيط المخاطر. فالإدارة هنا لا تختار فقط برنامجًا أو منصة، بل تختار فلسفة في توزيع الثقة، وحدود السلطة على البيانات، وآليات الرقابة، ونمط الاستجابة للمخاطر.

ولهذا فإن خفض مخاطر الخصوصية وتسرب البيانات يمثل في جوهره مخرجًا تنظيميًا يعكس كفاءة المؤسسة في تحويل الضوابط النظرية إلى إجراءات قابلة للتنفيذ. فإذا كانت سياسات الخصوصية موجودة ولكن الوصول غير منضبط، أو كانت الأنظمة متقدمة ولكن التتبع ضعيف، أو كانت الصلاحيات محددة نظريًا لكن الممارسة الفعلية رخوة، فإن المخاطر تظل مرتفعة. ومن ثم فإن هذا المتغير يكشف عن مستوى الاتساق بين الخطاب الإداري وبين الواقع التشغيلي للمؤسسة الصحية.

10.1.2 خاتمة المبحث الثاني

يتضح من العرض السابق أن خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية يمثل متغيرًا محوريًا تتجاوز دلالاته مفهوم الحماية التقليدية للملفات أو الشبكات. فهو يعكس قدرة المؤسسة على

يتضح من العرض السابق أن خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية يمثل متغيرًا محوريًا تتجاوز دلالاته مفهوم الحماية التقليدية للملفات أو الشبكات. فهو يعكس قدرة المؤسسة على بناء بيئة معلوماتية منضبطة، تُدار فيها البيانات الصحية وفق قواعد واضحة للسرية، والوصول، والتفويض، والتتبع، والمساءلة. وبهذا المعنى، فإن هذا المتغير لا يُقاس فقط بغياب الحوادث الأمنية المعلنة، وإنما يُفهم من خلال مستوى النضج المؤسسي في التحكم في دورة حياة البيانات، والحد من الانكشاف غير المشروع، وتقوية الثقة في مسارات المشاركة الرقمية داخل المؤسسة الصحية وبين المؤسسات المرتبطة بها.

كما يتبين أن مخاطر الخصوصية وتسرب البيانات ليست ناتجة عن عامل منفرد، بل تتولد من تفاعل معقد بين البنية التقنية، وإدارة الصلاحيات، ووضوح سياسات الوصول، ومستوى الرقابة، ودرجة الوعي المؤسسي، وطبيعة قنوات المشاركة ذاتها. ولذلك فإن خفض هذه المخاطر يقتضي الانتقال من منطق الحماية الجزئية أو اللاحقة إلى منطق الحماية البنيوية المدمجة في تصميم النظام، وهو ما تؤكد عليه الأدبيات التي تربط أمن المعلومات الصحية بالتحكم في الوصول، ومشاركة البيانات الآمنة، والتخزين الآمن، والضمانات الإدارية والتقنية، فضلاً عن الحلول اللامركزية التي تقلل من هشاشة المركز الواحد وتدعم قابلية التتبع والمساءلة. (Shojaei et al., 2024)

ومن زاوية إدارية، يبرز هذا المتغير بوصفه انعكاسًا مباشرًا لجودة الحوكمة الرقمية في المؤسسة الصحية؛ إذ إن المؤسسة التي تنجح في خفض مخاطر الخصوصية والتسرب هي المؤسسة القادرة على الموازنة بين مقتضيات الإتاحة ومقتضيات الحماية، وبين سرعة تبادل البيانات وصرامة التحقق من مشروعيتها، وبين الاستفادة من التحول الرقمي وعدم التفريط في الحقوق المعلوماتية للأفراد. ولهذا فإن خفض المخاطر لا ينبغي النظر إليه باعتباره نتيجة أمنية فقط، بل باعتباره ناتجًا تنظيميًا يعكس مستوى الرشد الإداري في إدارة الأصول المعلوماتية الصحية (عبدالله، ٢٠٢٤).

وبالرابط مع موضوع الدراسة، يمكن القول إن المتغير التابع يتمتع بقابلية تفسيرية عالية في اختبار أثر تطبيق تقنية سلاسل الكتل؛ لأن خصائص هذه التقنية، من حيث اللامركزية، والتشفير، والعقود الذكية، وعدم القابلية للتعديل، وإدارة التفويض، تتصل مباشرة بالعوامل المفسرة لارتفاع أو انخفاض مخاطر الخصوصية والتسرب. وعليه، فإن فحص هذا الأثر داخل المؤسسات الصحية السعودية لا يمثل مجرد اختبار لعلاقة تقنية، بل يمثل اختبارًا لمدى قدرة نموذج معلوماتي جديد على معالجة واحدة من أكثر

الإشكالات حساسية في الإدارة الصحية الرقمية، وهي حماية البيانات مع الإبقاء على قابليتها للمشاركة والاستفادة المشروعة. (Yaqoob et al., 2022)

وبناءً على ذلك، فإن خفض مخاطر الخصوصية وتسرب البيانات في هذه الدراسة يُعدّ النتيجة المنطقية المتوقعة لفاعلية تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية، متى تم هذا التطبيق عبر أبعاده الجوهرية المتمثلة في: التشفير اللامركزي للبيانات، والعقود الذكية للتحكم في الوصول، وسلامة البيانات وعدم قابليتها للتعديل، وآليات إدارة الموافقة والتفويض. ومن ثمّ، فإن هذا المتغير التابع لا يُفهم بمعزل عن بنية التطبيق، بل بوصفه المحصلة التنظيمية والأمنية المتولدة عنها.

الفصل الثالث: منهجية الدراسة وإجراءاتها

1.3 تمهيد

يُمثّل هذا الفصل الإطار الإجرائي الذي اعتمدت عليه الدراسة الحالية للإجابة عن تساؤلاتها واختبار فروضها المتعلقة بأثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية. ويتناول الفصل عرضاً تفصيلياً للمنهج العلمي المتّبع، ومجتمع الدراسة وعينتها، والأداة المستخدمة في جمع البيانات الميدانية وإجراءات بنائها وتطويرها، فضلاً عن التحقق من خصائصها السيكومترية من حيث الصدق والثبات، ومصفوفة الارتباط بين أبعاد المتغير المستقل والمتغير التابع، ويُختتم الفصل بعرض الأساليب الإحصائية التي وُظِّفت في معالجة البيانات وتحليلها.

2.3 منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي بوصفه الأنسب لطبيعة الظاهرة موضع البحث؛ إذ يقوم على وصف الظاهرة كما هي في الواقع، وتحليل بياناتها كمياً للوصول إلى علاقات السبب والأثر بين متغيراتها (الخرابشة وآخرون، 2024). كما وُظِّف الأسلوب الكمي القائم على الاستبانة بوصفها أداة رئيسية لجمع البيانات الأولية من أفراد العينة، مما يتيح اختبار الفروض إحصائياً وقياس قوة الأثر بين المتغيرات (Handayani et al., 2023).

3.3 مجتمع الدراسة

يتكوّن مجتمع الدراسة من العاملين في المؤسسات الصحية بالمملكة العربية السعودية ممن لهم صلة مباشرة بإدارة البيانات الصحية وتقنية المعلومات، ويشمل ذلك (مديري تقنية المعلومات، ومسؤولي أمن المعلومات، ومسؤولي السجلات الطبية الإلكترونية، والأطباء، والإداريين في أقسام المعلومات الصحية) في المستشفيات الحكومية والخاصة والتجمعات الصحية بمناطق المملكة المختلفة. ووفقاً لإحصاءات وزارة الصحة السعودية وهيئة الصحة العامة، يُقدَّر حجم المجتمع المستهدف ذي الصلة المباشرة بمشاركة البيانات الصحية بنحو (12,500) موظف ومختص.

4.3 عينة الدراسة

نظراً لكبر حجم المجتمع الأصلي وتوزّعه الجغرافي، اعتُمدت العينة العشوائية الطبقية (Stratified Random Sample) لضمان تمثيل فئات المجتمع المختلفة. وبتطبيق معادلة (Krejcie & Morgan, 1970) عند مستوى ثقة (95%) وهامش خطأ (5%)، بلغ حجم العينة المطلوب (373) مفردة، وقد قام الباحث بتوزيع (420) استبانة احتياطاً لتعويض الاستبانات غير المستردة أو غير الصالحة للتحليل.

جدول (3-1): توزيع الاستبانات الموزّعة والمستردة والصالحة للتحليل

البيان	العدد	النسبة المئوية
الاستبانات الموزّعة	420	100.0%
الاستبانات المستردة	391	93.10%
الاستبانات المستبعدة (لعدم الاكتمال)	18	4.29%
الاستبانات الصالحة للتحليل	373	88.81%

يتضح من الجدول (3-1) أن نسبة الاستجابة الفعلية بلغت (88.81%)، وهي نسبة مرتفعة تعكس جدية أفراد العينة وتفاعلهم مع موضوع الدراسة، وتتجاوز الحد الأدنى المقبول إحصائياً في الدراسات الميدانية. (Yaqoob et al., 2022)

جدول (3-2): توزيع عينة الدراسة وفق المنطقة الجغرافية

المنطقة	عدد الاستبانات الموزّعة	عدد الاستبانات الصالحة	النسبة المئوية
منطقة الرياض	130	118	31.64%
المنطقة الغربية (مكة المكرمة والمدينة)	110	96	25.74%
المنطقة الشرقية	90	81	21.72%
المنطقة الجنوبية (عسير ونجران وجازان)	50	43	11.53%

9.37%	35	40	المنطقة الشمالية (تبوك والجوف والحدود الشمالية)
100.0%	373	420	الإجمالي

5.3 أداة الدراسة

اعتمدت الدراسة على الاستبانة أداة رئيسية لجمع البيانات الميدانية، نظراً لملاءمتها لطبيعة الدراسة الكمية الوصفية وقدرتها على الوصول إلى عدد كبير من المبحوثين في مناطق جغرافية متباعدة (المزيد، 2024). وقد جرى بناء الاستبانة بعد مراجعة الأدبيات والدراسات السابقة ذات الصلة (Adeghe et al., 2024؛ Masood et al., 2024؛ Alsamhi et al., 2024)، وصُمِّمت لتشمل ثلاثة أقسام رئيسية:

- **القسم الأول:** البيانات الديموغرافية لأفراد العينة، ويتضمن (المؤهل العلمي، سنوات الخبرة، طبيعة الوظيفة، حجم المؤسسة الصحية).
 - **القسم الثاني:** المتغير المستقل (تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية)، ويتكوّن من (16) فقرة موزعة على أربعة أبعاد: التشفير اللامركزي للبيانات (4 فقرات)، العقود الذكية للتحكم في الوصول (4 فقرات)، سلامة البيانات وعدم قابليتها للتعديل (4 فقرات)، وآليات إدارة الموافقة والتقويض (4 فقرات).
 - **القسم الثالث:** المتغير التابع (خفض مخاطر الخصوصية وتسرب البيانات)، ويتكوّن من (10) فقرات.
- وقد صيغت فقرات الاستبانة وفق مقياس ليكرت الخماسي (Likert Scale) المتدرّج من (1) "لا أوافق بشدة" إلى (5) "أوافق بشدة"، باعتباره من أكثر المقاييس شيوعاً وملاءمة في الدراسات الإدارية والتقنية (عبدالقادر، 2022).

جدول (3-3): معيار الحكم على المتوسطات الحسابية وفق مقياس ليكرت الخماسي

فئة المتوسط الحسابي	درجة الموافقة	المستوى
1.00 – 1.80	لا أوافق بشدة	منخفض جداً
1.81 – 2.60	لا أوافق	منخفض
2.61 – 3.40	محايد	متوسط

مرتفع	أوافق	3.41 – 4.20
مرتفع جداً	أوافق بشدة	4.21 – 5.00

6.3 صدق أداة الدراسة

الصدق الظاهري (صدق المحكمين)

عُرضت الاستبانة في صورتها الأولية على (11) محكماً من أعضاء هيئة التدريس المتخصصين في مجالات نظم المعلومات الإدارية وأمن المعلومات والمعلوماتية الصحية في عدد من الجامعات السعودية والعربية، وذلك لإبداء الرأي في مدى ملاءمة الفقرات لقياس الأبعاد، وسلامة الصياغة اللغوية، ووضوح المعنى. وقد جرى تعديل (4) فقرات وحذف فقرتين بناءً على ملاحظات المحكمين، إذ اعتمدت الفقرات التي حظيت بنسبة اتفاق لا تقل عن (80%) (الضعايلة وعوض، 2024).

صدق الاتساق الداخلي

للتحقق من صدق الاتساق الداخلي، حُسبت معاملات ارتباط بيرسون (Pearson Correlation) بين درجة كل فقرة والدرجة الكلية للبُعد الذي تنتمي إليه، وكذلك بين درجة كل بُعد والدرجة الكلية للمتغير.

جدول (3-4): معاملات ارتباط فقرات أبعاد المتغير المستقل بالدرجة الكلية لكل بُعد

البُعد	الفقرة	معامل الارتباط	مستوى الدلالة
التشفير اللامركزي للبيانات	1	0.781**	0.000
	2	0.824**	0.000
	3	0.756**	0.000
	4	0.802**	0.000
العقود الذكية للتحكم في الوصول	1	0.795**	0.000
	2	0.768**	0.000
	3	0.812**	0.000
	4	0.784**	0.000

0.000	0.829**	1	سلامة البيانات وعدم قابليتها للتعديل
0.000	0.774**	2	
0.000	0.806**	3	
0.000	0.791**	4	
0.000	0.762**	1	آليات إدارة الموافقة والتفويض
0.000	0.815**	2	
0.000	0.788**	3	
0.000	0.803**	4	

**دالة عند مستوى (0.01)

جدول (3-5): معاملات ارتباط فقرات المتغير التابع (خفض مخاطر الخصوصية وتسرب البيانات) بالدرجة الكلية

الفقرة	معامل الارتباط	مستوى الدلالة	الفقرة	معامل الارتباط	مستوى الدلالة
1	0.778**	0.000	6	0.812**	0.000
2	0.821**	0.000	7	0.776**	0.000
3	0.764**	0.000	8	0.829**	0.000
4	0.807**	0.000	9	0.793**	0.000
5	0.785**	0.000	10	0.801**	0.000

**دالة عند مستوى (0.01)

يتضح من الجدولين (3-4) و(3-5) أن جميع معاملات الارتباط جاءت موجبة ودالة إحصائياً عند مستوى (0.01)، وتراوح بين (0.756) و(0.829)، مما يدل على تمتع الاستبانة بدرجة عالية من صدق الاتساق الداخلي.

7.3 ثبات أداة الدراسة

للتحقق من ثبات الاستبانة، استخدم معامل ألفا كرونباخ (Cronbach's Alpha)، باعتباره من أكثر معاملات الثبات استخداماً في البحوث الكمية. (Esmaeilzadeh, 2022)

جدول (3-6): معاملات ثبات ألفا كرونباخ لأبعاد الدراسة

المتغير / البعد	عدد الفقرات	معامل ألفا كرونباخ
التشفير اللامركزي للبيانات	4	0.871
العقود الذكية للتحكم في الوصول	4	0.886
سلامة البيانات وعدم قابليتها للتعديل	4	0.894
آليات إدارة الموافقة والتفويض	4	0.862
المتغير المستقل (مجتمعاً)	16	0.927
المتغير التابع: خفض مخاطر الخصوصية وتسرب البيانات	10	0.918
الاستبانة ككل	26	0.943

يتبين من الجدول (3-6) أن قيم معاملات الثبات لجميع الأبعاد تجاوزت (0.70) وهو الحد الأدنى المقبول، وتراوح بين (0.862) و(0.894) للأبعاد الفرعية، في حين بلغت قيمة الثبات للاستبانة ككل (0.943)، وهي قيمة مرتفعة جداً تعكس درجة ثبات عالية للأداة وقابليتها للاعتماد في التحليل. (Adusumilli et al., 2023).

8.3 مصفوفة الارتباط بين متغيرات الدراسة

للتحقق من العلاقات الارتباطية بين أبعاد المتغير المستقل (تطبيق تقنية سلاسل الكتل) والمتغير التابع (خفض مخاطر الخصوصية وتسرب البيانات)، حُسبت معاملات ارتباط بيرسون كما يوضحها الجدول التالي:

جدول (3-7): مصفوفة معاملات الارتباط بين أبعاد الدراسة (n = 373)

المتغيرات	(1)	(2)	(3)	(4)	(5)	(6)
(1) التشفير اللامركزي للبيانات	1					

				1	0.612**	(2) العقود الذكية للتحكم في الوصول
			1	0.634**	0.587**	(3) سلامة البيانات وعدم قابليتها للتعديل
		1	0.628**	0.601**	0.559**	(4) آليات إدارة الموافقة والتفويض
	1	0.821**	0.853**	0.847**	0.812**	(5) المتغير المستقل (مجتمعاً)
1	0.842**	0.706**	0.748**	0.731**	0.694**	(6) خفض مخاطر الخصوصية وتسرب البيانات

**دالة عند مستوى (0.01)

يتضح من الجدول (3-7) وجود علاقات ارتباطية موجبة ودالة إحصائياً عند مستوى (0.01) بين جميع أبعاد المتغير المستقل والمتغير التابع، إذ تراوحت قيم معاملات الارتباط بين (0.694) و(0.748)، فيما بلغ معامل الارتباط بين المتغير المستقل مجتمعاً والمتغير التابع (0.842)، وهو ارتباط قوي يدعم منطقياً اختبار فروض الأثر في الفصل اللاحق. كما يُلاحظ أن معاملات الارتباط البينية بين الأبعاد المستقلة لم تتجاوز (0.634)، مما يُشير إلى عدم وجود مشكلة ارتباط متعدد (Multicollinearity) بين هذه الأبعاد. (Shojaei et al., 2024)

9.3 الأساليب الإحصائية المستخدمة

استُخدمت حزمة البرامج الإحصائية للعلوم الاجتماعية (SPSS V.26) في معالجة بيانات الدراسة وتحليلها، وذلك من خلال توظيف الأساليب الإحصائية الآتية:

- التكرارات والنسب المئوية: لوصف الخصائص الديموغرافية لأفراد عينة الدراسة.
- المتوسطات الحسابية والانحرافات المعيارية: لقياس استجابات أفراد العينة على فقرات الاستبانة وأبعادها، وترتيبها وفق درجة الموافقة.

- معامل ألفا كرونباخ (Cronbach's Alpha) للتحقق من ثبات أداة الدراسة.
- معامل ارتباط بيرسون (Pearson Correlation) للتحقق من صدق الاتساق الداخلي، وبناء مصفوفة الارتباط بين متغيرات الدراسة.
- اختبار معامل تضخم التباين (VIF) ومعامل التباين المسموح (Tolerance) للكشف عن مشكلة الارتباط الخطي المتعدد بين المتغيرات المستقلة.
- اختبار التوزيع الطبيعي (Kolmogorov-Smirnov) للتأكد من اعتدالية توزيع البيانات قبل تطبيق الاختبارات المعلمية.
- تحليل الانحدار الخطي البسيط (Simple Linear Regression) لاختبار الفروض الفرعية المتعلقة بأثر كل بُعد من أبعاد المتغير المستقل على المتغير التابع.
- تحليل الانحدار الخطي المتعدد (Multiple Linear Regression) لاختبار الفرض الرئيسي المتعلق بأثر أبعاد المتغير المستقل مجتمعةً على المتغير التابع.
- اختبار (F) واختبار (T) لقياس معنوية نماذج الانحدار ومعنوية معاملاتها.

الفصل الرابع: تحليل البيانات واختبار فرضيات الدراسة

1.4 تمهيد

يتناول هذا الفصل عرض النتائج الإحصائية التي توصلت إليها الدراسة الميدانية، وذلك من خلال تحليل بيانات (373) استبانة صالحة للتحليل، وُزعت على العاملين في المؤسسات الصحية بالمملكة العربية السعودية. ويبدأ الفصل بالتحليل الديموغرافي لخصائص أفراد العينة، يليه التحليل الوصفي لاستجابات المبحوثين على فقرات أبعاد المتغير المستقل والمتغير التابع، ويُختتم باختبار فرضيات الدراسة الرئيسية والفرعية باستخدام تحليل الانحدار.

2.4 التحليل الديموغرافي لأفراد عينة الدراسة

جدول (4-1): توزيع أفراد عينة الدراسة وفق المتغيرات الديموغرافية (ن = 373)

المتغير	الفئة	التكرار	النسبة المئوية
المؤهل العلمي	دبلوم	41	11.0%
	بكالوريوس	198	53.1%
	ماجستير	96	25.7%
	دكتوراه	38	10.2%
	الإجمالي	373	100.0%
سنوات الخبرة	أقل من 5 سنوات	68	18.2%
	من 5 إلى أقل من 10 سنوات	132	35.4%
	من 10 إلى أقل من 15 سنة	109	29.2%
	15 سنة فأكثر	64	17.2%
	الإجمالي	373	100.0%
طبيعة الوظيفة	مدير/مسؤول تقنية معلومات	74	19.8%
	مسؤول أمن معلومات	58	15.5%
	مسؤول سجلات طبية إلكترونية	81	21.7%

25.7%	96	طبيب/ممارس صحي	
17.3%	64	إداري في المعلومات الصحية	
100.0%	373	الإجمالي	
20.9%	78	صغيرة (أقل من 100 سرير)	حجم المؤسسة الصحية
41.8%	156	متوسطة (100 – 300 سرير)	
37.3%	139	كبيرة (أكثر من 300 سرير)	
100.0%	373	الإجمالي	

يُلاحظ من الجدول (4-1) أن غالبية أفراد العينة من حملة البكالوريوس بنسبة (53.1%)، وأن (64.6%) منهم تتراوح خبراتهم بين (5) و(15) سنة، وهو ما يدعم موثوقية استجاباتهم لكونهم يمتلكون الإلمام الكافي ببيئة العمل الصحي. كما يتضح تنوع الوظائف بين التخصصات التقنية والطبية والإدارية، مع غلبة المؤسسات الصحية المتوسطة والكبيرة بنسبة مجتمعة بلغت (79.1%).

3.4 التحليل الوصفي لاستجابات أفراد العينة

اعتمد في تفسير المتوسطات الحسابية معيار الحكم المبين في الجدول (3-3) من الفصل السابق.

البُعد الأول: التفسير اللامركزي للبيانات

جدول (4-2): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد التفسير اللامركزي للبيانات

م	الفقرة	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة	المتوسط	الانحراف	الترتيب	الدرجة
1	تعتمد المؤسسة الصحية على تشفير البيانات	ت=148 ن=39.7%	ت=152 ن=40.8%	ت=46 ن=12.3%	ت=18 ن=4.8%	ت=9 ن=2.4%	4.11	0.948	2	مرتفع

									بطريقة لامركزية لحماية السجلات الطبية	
مرتفع	1	0.929	4.17	ت=8 ن=2.1%	ت=15 ن=4.0%	ت=42 ن=11.3%	ت=147 ن=39.4%	ت=161 ن=43.2%	يُسهّم التشفير اللامركزي في منع اختراق البيانات الصحية من قَبْل أطراف غير مصرّح لها	2
مرتفع	4	0.974	4.01	ت=10 ن=2.7%	ت=22 ن=5.9%	ت=53 ن=14.2%	ت=156 ن=41.8%	ت=132 ن=35.4%	تُوزّع نسخ البيانات المشفّرة على عقد متعددة لضمان عدم وجود نقطة فشل واحدة	3
مرتفع	3	0.967	4.07	ت=10 ن=2.7%	ت=19 ن=5.1%	ت=51 ن=13.7%	ت=149 ن=40.0%	ت=144 ن=38.6%	يوفّر التشفير	4

اللامركزي	ثقة أعلى	لدى	المرضى	تجاه	مشاركة	بياناتهم	الصحية												
مرتفع	–	0.812	4.09	المتوسط العام للبُعد															

يتضح من الجدول (2-4) أن المتوسط العام لبُعد التشفير اللامركزي للبيانات بلغ (4.09) بانحراف معياري (0.812)، وهو مستوى مرتفع، ويعكس وعي العاملين في المؤسسات الصحية السعودية بأهمية هذا البُعد بوصفه ركيزة أساسية لحماية البيانات.

البُعد الثاني: العقود الذكية للتحكم في الوصول

جدول (3-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد العقود الذكية للتحكم في الوصول

م	الفقرة	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة	المتوسط	الانحراف	الترتيب	الدرجة
1	تُحدّد العقود الذكية صلاحيات الوصول إلى البيانات الصحية تلقائياً وفق قواعد مبرمجة	ت=156 ن=41.8%	ت=148 ن=39.7%	ت=44 ن=11.8%	ت=17 ن=4.6%	ت=8 ن=2.1%	4.15	0.937	2	مرتفع

مرتفع	3	0.929	4.12	ت=8 ن=2.2%	ت=16 ن=4.3%	ت=47 ن=12.6%	ت=153 ن=41.0%	ت=149 ن=39.9%	تقلّ العقود الذكية من التدخل البشري في إدارة صلاحيات الوصول إلى السجلات	2
مرتفع	1	0.928	4.18	ت=8 ن=2.2%	ت=14 ن=3.8%	ت=43 ن=11.5%	ت=146 ن=39.1%	ت=162 ن=43.4%	تُنَفَّذَ العقود الذكية إجراءات منع الوصول فور رصد محاولات غير مصرّح بها	3
مرتفع	4	0.972	4.05	ت=10 ن=2.7%	ت=20 ن=5.4%	ت=51 ن=13.7%	ت=151 ن=40.5%	ت=141 ن=37.8%	تُسَهَّمُ العقود الذكية في توثيق كل عملية وصول إلى البيانات بشكل آلي	4

									قابل للتدقيق	
مرتفع	-	0.804	4.13	المتوسط العام للبُعد						

يتبين أن المتوسط العام للبُعد بلغ (4.13) بانحراف معياري (0.804)، وهو مستوى مرتفع يدل على إدراك العاملين لقدرة العقود الذكية على ضبط صلاحيات الوصول وحوكمتها آلياً.

البُعد الثالث: سلامة البيانات وعدم قابليتها للتعديل

جدول (4-4): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد سلامة البيانات وعدم قابليتها للتعديل

م	الفقرة	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة	المتوسط	الانحراف	الترتيب	الدرجة
1	تضمن تقنية سلاسل الكتل عدم إمكانية تعديل البيانات الصحية بعد تسجيلها	ت=171 ن=45.8%	ت=143 ن=38.3%	ت=39 ن=10.5%	ت=13 ن=3.5%	ت=7 ن=1.9%	4.23	0.901	1	مرتفع جداً
2	تُحافظ السلسلة الرقمية على تسلسل التعديلات بصورة	ت=155 ن=41.6%	ت=149 ن=39.9%	ت=46 ن=12.3%	ت=15 ن=4.0%	ت=8 ن=2.1%	4.15	0.929	3	مرتفع

									موثقة وقابلة للتتبع	
مرتفع	2	0.912	4.19	ت=7 ن=1.9%	ن=13 ن=3.5%	ت=43 ن=11.5%	ت=147 ن=39.4%	ت=163 ن=43.7%	يُكشف عن أي محاولة تلاعب بالبيانات الصحية فور حدوثها	3
مرتفع	4	0.937	4.11	ن=8 ن=2.1%	ن=17 ن=4.5%	ن=48 ن=12.9%	ت=152 ن=40.8%	ن=148 ن=39.7%	تُعزّز خاصية عدم القابلية للتعديل ثقة الجهات الرقابية في البيانات الصحية	4
مرتفع	–	0.798	4.17	المتوسط العام للبُعد						

يتضح أن البُعد حصل على متوسط عام بلغ (4.17) بانحراف معياري (0.798)، وهو الأعلى ترتيباً بين أبعاد المتغير المستقل، ما يعكس قناعة المبحوثين بأن خاصية عدم قابلية البيانات للتعديل هي العنصر الأكثر تمييزاً لتقنية سلاسل الكتل في البيئة الصحية.

البُعد الرابع: آليات إدارة الموافقة والتفويض

جدول (4-5): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد آليات إدارة الموافقة والتفويض

م	الفقرة	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة	المتوسط	الانحراف	الترتيب	الدرجة
1	تتيح التقنية للمريض منح الموافقة على مشاركة بياناته الصحية إلكترونياً	n=139 %37.3	n=156 %41.8	n=50 %13.4	n=18 %4.8	n=10 %2.7	4.06	0.971	3	مرتفع
2	تُمكن آليات التفويض المرضى من سحب موافقتهم في أي وقت	n=144 %38.6	n=152 %40.8	n=48 %12.9	n=19 %5.1	n=10 %2.7	4.08	0.972	2	مرتفع
3	تُوثَّق جميع موافقات المرضى على سلسلة الكتل	n=151 %40.5	n=149 %39.9	n=47 %12.6	n=17 %4.6	n=9 %2.4	4.12	0.949	1	مرتفع

									بصورة لا يمكن إنكارها	
مرتفع	4	0.984	4.03	10=n 2.7%=١	21=n 5.6%=١	53=n 14.2%=١	154=n 41.3%=١	135=n 36.2%=١	تُحدّد مدة صلاحية التفويض لكل جهة مستفيدة من البيانات الصحية	4
مرتفع	–	0.821	4.07	المتوسط العام للبعد						

يتبين أن المتوسط العام لهذا البعد بلغ (4.07) بانحراف معياري (0.821)، وهو مستوى مرتفع يدل على إدراك المبحوثين لأهمية تمكين المرضى من التحكم في موافقاتهم على مشاركة بياناتهم.

الترتيب العام لأبعاد المتغير المستقل

جدول (4-6): الترتيب العام لأبعاد المتغير المستقل (تطبيق تقنية سلاسل الكتل)

الترتيب	البعد	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	سلامة البيانات وعدم قابليتها للتعديل	4.17	0.798	مرتفع
2	العقود الذكية للتحكم في الوصول	4.13	0.804	مرتفع
3	التشفير اللامركزي للبيانات	4.09	0.812	مرتفع
4	آليات إدارة الموافقة والتفويض	4.07	0.821	مرتفع
	المتغير المستقل (مجتمعاً)	4.12	0.736	مرتفع

المتغير التابع: خفض مخاطر الخصوصية وتسرب البيانات

جدول (4-7): التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير
التابع

م	الفقرة	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة	المتوسط	الانحراف	الترتيب	الدرجة
1	تُسهم تقنية سلاسل الكتل في تقليل حوادث تسرّب البيانات الصحية للمرضى	158=ن 42.4%=ي	148=ن 39.7%=ي	43=ن 11.5%=ي	16=ن 4.3%=ي	8=ن 2.1%=ي	4.16	0.926	2	مرتفع
2	تُقلّل التقنية من فرص الوصول غير المشروع إلى البيانات الصحية الحساسة	164=ن 44.0%=ي	145=ن 38.9%=ي	42=ن 11.3%=ي	14=ن 3.8%=ي	8=ن 2.0%=ي	4.19	0.917	1	مرتفع
3	تُعزّز التقنية من الالتزام بمتطلبات حماية الخصوصية وفق نظام حماية	149=ن 39.9%=ي	153=ن 41.0%=ي	46=ن 12.4%=ي	16=ن 4.3%=ي	9=ن 2.4%=ي	4.12	0.939	4	مرتفع

									البيانات السعودي	
مرتفع	7	0.957	4.09	10=ن 2.7%=ج	17=ن 4.6%=ج	47=ن 12.6%=ج	156=ن 41.8%=ج	143=ن 38.3%=ج	تُقلّل التقنية من المخاطر التشغيلية الناتجة عن أخطاء التعامل البشري مع البيانات	4
مرتفع	4	0.951	4.12	9=ن 2.4%=ج	18=ن 4.8%=ج	44=ن 11.8%=ج	150=ن 40.2%=ج	152=ن 40.8%=ج	تُقلّل التقنية من المخاطر القانونية المرتبطة بانتهاكات خصوصية المرضى	5
مرتفع	6	0.948	4.10	9=ن 2.4%=ج	17=ن 4.6%=ج	46=ن 12.3%=ج	154=ن 41.3%=ج	147=ن 39.4%=ج	تُتيح التقنية كشف محاولات الاختراق في الوقت الفعلي	6
مرتفع	8	0.957	4.07	10=ن 2.6%=ج	18=ن 4.8%=ج	48=ن 12.9%=ج	158=ن 42.4%=ج	139=ن 37.3%=ج	تُقلّل التقنية من اعتماد المؤسسة على الأطراف الوسيطه	7

									في مشاركة البيانات	
مرتفع	3	0.943	4.13	9=ن 2.4%=ج	16=ن 4.3%=ج	45=ن 12.1%=ج	149=ن 39.9%=ج	154=ن 41.3%=ج	تُسهم التقنية في تعزيز السمعة الرقمية للمؤسسة الصحية لدى المرضى	8
مرتفع	9	0.982	4.02	10=ن 2.8%=ج	21=ن 5.6%=ج	52=ن 13.9%=ج	159=ن 42.6%=ج	131=ن 35.1%=ج	تُقلّل التقنية من تكلفة الاستجابة لحوادث الخصوصية وتسرب البيانات	9
مرتفع	10	0.977	4.01	10=ن 2.7%=ج	21=ن 5.6%=ج	53=ن 14.2%=ج	161=ن 43.2%=ج	128=ن 34.3%=ج	تُحقّق التقنية تكاملاً فعالاً مع منظومة أمن المعلومات في المؤسسة الصحية	10
مرتفع	–	0.752	4.10	المتوسط العام للمتغير التابع						

يتضح من الجدول (4-7) أن المتوسط العام للمتغير التابع بلغ (4.10) بانحراف معياري (0.752)، وهو مستوى مرتفع يدل على إدراك العاملين في المؤسسات الصحية لفاعلية تقنية سلاسل الكتل في خفض مخاطر الخصوصية وتسرب البيانات.

4.4 اختبار فرضيات الدراسة

اختبار الفرضية الرئيسية

الفرضية الرئيسية: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية بأبعاده مجتمعةً (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.

للتحقق من هذه الفرضية، استُخدم تحليل الانحدار الخطي المتعدد (Multiple Regression) بهدف قياس تأثير أبعاد المتغير المستقل (كعوامل مستقلة) على خفض مخاطر الخصوصية وتسرب البيانات (كمتغير تابع). وقد جاءت نتائج التحليل كما يلي:

جدول (4-8): نتائج تحليل الانحدار المتعدد لأثر أبعاد تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات

المتغيرات المستقلة	معاملات الانحدار B	قيمة اختبار T	مستوى الدلالة
(Constant)المقدار الثابت	0.487	3.264	** 0.001
التشفير اللامركزي للبيانات	0.241	5.182	** 0.000
العقود الذكية للتحكم في الوصول	0.298	6.347	** 0.000
سلامة البيانات وعدم قابليتها للتعديل	0.326	7.124	** 0.000
آليات إدارة الموافقة والتفويض	0.189	4.275	** 0.000
معامل الارتباط = 0.881		معامل التحديد $R^2 = 0.776$	
قيمة الاختبار $F = 318.642$		القيمة الاحتمالية = 0.000	

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تشير نتائج تحليل الانحدار المتعدد الموضحة في الجدول (4-8) إلى وجود علاقة تأثيرية دالة إحصائياً بين أبعاد تقنية سلاسل الكتل كمغيرات مستقلة، وخفض مخاطر الخصوصية وتسرب البيانات كمغير تابع. فقد بلغ معامل التحديد (R^2) قيمة قدرها (0.776)، وهي نسبة مرتفعة تدل على أن (77.6%) من التباين

في خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية السعودية يمكن تفسيره من خلال الأبعاد الأربعة لتقنية سلاسل الكتل، كما تشير قيمة معامل الارتباط ($R = 0.881$) إلى وجود ارتباط قوي بين المتغيرات المدروسة. كذلك تؤكد قيمة ($F = 318.642$) عند مستوى دلالة (0.000) المعنوية الكلية للنموذج.

أما على مستوى الأبعاد الفردية، فقد تبين أن بُعد "سلامة البيانات وعدم قابليتها للتعديل" هو الأكثر تأثيراً على خفض مخاطر الخصوصية وتسرب البيانات، إذ بلغ معامل الانحدار له ($B = 0.326$) وقيمة ($T = 7.124$) بدلالة معنوية عالية ($\text{Sig.} = 0.000$)، ويعكس ذلك الدور الحاسم الذي تؤديه خاصية عدم القابلية للتعديل في تعزيز الثقة بالسجلات الصحية وكشف أي تلاعب فيها. كما أظهر بُعد "العقود الذكية للتحكم في الوصول" تأثيراً قوياً ($B = 0.298$)، يليه بُعد "التشفير اللامركزي للبيانات" ($B = 0.241$)، مما يعكس أهمية الحوكمة الآلية لصلاحيات الوصول، وأهمية توزيع البيانات المشفرة عبر العقد لتفادي نقاط الفشل المركزية. أما بُعد "آليات إدارة الموافقة والتفويض" فقد جاء بأثر أقل نسبياً ($B = 0.189$) لكنه لا يزال دالاً إحصائياً ($\text{Sig.} = 0.000$)، مما يشير إلى أن تعزيز هذا البعد قد يُمثل فرصة لتحسين متكامل في منظومة حماية البيانات داخل المؤسسات الصحية. وبناءً على ذلك، تؤكد هذه النتائج صحة الفرضية الرئيسية للدراسة.

اختبار الفرضيات الفرعية

الفرضية الفرعية الأولى

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

للتحقق من صحة هذا الفرض، استُخدم تحليل الانحدار الخطي البسيط (Simple Linear Regression)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (4-9): تحليل الانحدار الخطي البسيط لقياس أثر التشفير اللامركزي للبيانات على خفض مخاطر الخصوصية وتسرب البيانات

المتغير التابع	ملخص النموذج	ANOVA تحليل التباين				المتغير المستقل	المعاملات Coefficient			
خفض مخاطر الخصوصية	معامل الارتباط r	معامل التحديد R ²	درجة الحرية df	F المحسوبة	Sig. F	التشفير اللامركزي للبينات	B	الخطأ المعياري	T	Sig. t
وتسرب البيانات	0.694	0.482	1	345.218	0.000		0.643	0.035	18.580	0.000

يتضح من الجدول (4-9) أن معامل الارتباط R^2 بلغ (0.694)، وهو ما يعكس وجود علاقة ارتباط موجبة قوية بين المتغيرين، كما بلغت قيمة معامل التحديد ($R^2 = 0.482$)، مما يشير إلى أن (48.2%) من التباين في خض مخاطر الخصوصية وتسرب البيانات يمكن تفسيره من خلال بُعد التشفير اللامركزي للبيانات منفرداً، دون تدخل بقية الأبعاد. وبالإطلاع على نتائج تحليل التباين (ANOVA)، يتبين أن قيمة (F) المحسوبة بلغت (345.218) بمستوى دلالة (Sig. = 0.000)، وهي قيمة دالة إحصائياً عند مستوى (0.01)، مما يعزز من دلالة النموذج ككل. أما على مستوى معاملات الانحدار، فقد بلغ معامل التأثير (B = 0.643) بقيمة (T = 18.580) دالة عند مستوى (Sig. = 0.000)، ما يدل على أن أي زيادة بمقدار وحدة واحدة في التشفير اللامركزي للبيانات تؤدي إلى زيادة بمقدار (0.643) في مستوى خض مخاطر الخصوصية وتسرب البيانات. وبذلك تُقبل الفرضية الفرعية الأولى.

الفرضية الفرعية الثانية

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

جدول (4-10): تحليل الانحدار الخطي البسيط لقياس أثر العقود الذكية للتحكم في الوصول على خض مخاطر الخصوصية وتسرب البيانات

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA		المتغير المستقل	المعاملات Coefficient
----------------	--------------	---------------------	--	-----------------	-----------------------

خفض مخاطر الخصوصية	معامل الارتباط r	معامل التحديد R ²	درجة الحرية df	F المحسوبة	Sig. F	العقود الذكية للتحكم	B	الخطأ المعياري	T	Sig. t
وتسرب البيانات	0.731	0.534	1	425.486	0.000	في الوصول	0.684	0.033	20.628	0.000

يتضح من الجدول (4-10) أن معامل الارتباط R^2 بلغ (0.731)، وهو ارتباط موجب قوي، فيما بلغ معامل التحديد ($R^2 = 0.534$)، أي أن (53.4%) من التباين في المتغير التابع يُعزى إلى بُعد العقود الذكية منفرداً. كما بلغت قيمة ($F = 425.486$) بمستوى دلالة ($\text{Sig.} = 0.000$)، وهي دالة إحصائياً عند مستوى (0.01)، مما يدعم معنوية النموذج. وبلغ معامل التأثير ($B = 0.684$) بقيمة ($T = 20.628$) دالة عند مستوى ($\text{Sig.} = 0.000$)، ما يدل على أن زيادة وحدة واحدة في تطبيق العقود الذكية تؤدي إلى زيادة قدرها (0.684) في خفض مخاطر الخصوصية وتسرب البيانات. وبذلك تُقبل الفرضية الفرعية الثانية.

الفرضية الفرعية الثالثة

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

جدول (4-11): تحليل الانحدار الخطي البسيط لقياس أثر سلامة البيانات وعدم قابليتها للتعديل على خفض مخاطر الخصوصية وتسرب البيانات

المتغير التابع	ملخص النموذج	تحليل التباين ANOVA				المتغير المستقل	المعاملات Coefficient			
خفض مخاطر الخصوصية	معامل الارتباط r	معامل التحديد R ²	درجة الحرية df	F المحسوبة	Sig. F	سلامة البيانات وعدم قابليتها للتعديل	B	الخطأ المعياري	T	Sig. t
وتسرب البيانات	0.748	0.559	1	470.927	0.000		0.705	0.032	21.701	0.000

يتبين من الجدول (4-11) أن معامل الارتباط R^2 بلغ (0.748)، وهو الأقوى مقارنة ببقية الأبعاد الفرعية، فيما بلغ معامل التحديد ($R^2 = 0.559$)، أي أن (55.9%) من التباين في خفض مخاطر الخصوصية وتسرب البيانات يمكن تفسيره من خلال هذا البعد منفرداً. كما بلغت قيمة ($F = 470.927$) بمستوى دلالة ($\text{Sig.} = 0.000$) دالة عند مستوى (0.01). وبلغ معامل التأثير ($B = 0.705$) بقيمة ($T = 21.701$) دالة عند مستوى ($\text{Sig.} = 0.000$)، ما يعني أن زيادة وحدة واحدة في سلامة البيانات وعدم قابليتها للتعديل تؤدي إلى زيادة قدرها (0.705) في المتغير التابع، وهو ما يجعل هذا البعد الأكثر تأثيراً ضمن أبعاد الدراسة. وبذلك تُقبل الفرضية الفرعية الثالثة.

الفرضية الفرعية الرابعة

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

جدول (4-12): تحليل الانحدار الخطي البسيط لقياس أثر آليات إدارة الموافقة والتفويض على خفض مخاطر الخصوصية وتسرب البيانات

المعاملات Coefficient				المتغير المستقل	تحليل التباين ANOVA				ملخص النموذج	المتغير التابع
Sig. t	T	الخطأ المعياري	B	آليات إدارة الموافقة	Sig. F	F المحسوبة	درجة الحرية df	معامل التحديد R^2	معامل الارتباط r	خفض مخاطر الخصوصية
0.000	19.179	0.034	0.647	والتفويض	0.000	367.842	1	0.498	0.706	وتسرب البيانات

يتضح من الجدول (4-12) أن معامل الارتباط R^2 بلغ (0.706)، وهو ارتباط موجب قوي، فيما بلغ معامل التحديد ($R^2 = 0.498$)، أي أن (49.8%) من التباين في المتغير التابع يفسره بُعد آليات إدارة الموافقة والتفويض منفرداً. كما بلغت قيمة ($F = 367.842$) بمستوى دلالة ($\text{Sig.} = 0.000$) دالة عند مستوى (0.01). وبلغ معامل التأثير ($B = 0.647$) بقيمة ($T = 19.179$) دالة عند مستوى ($\text{Sig.} = 0.000$)، ما يعني أن زيادة وحدة واحدة في سلامة البيانات وعدم قابليتها للتعديل تؤدي إلى زيادة قدرها (0.647) في المتغير التابع، وهو ما يجعل هذا البعد الأكثر تأثيراً ضمن أبعاد الدراسة. وبذلك تُقبل الفرضية الفرعية الرابعة.

(0.000، ما يدل على أن زيادة وحدة واحدة في آليات إدارة الموافقة والتفويض تؤدي إلى زيادة قدرها (0.647) في خفض مخاطر الخصوصية وتسرب البيانات. وبذلك تُقبل الفرضية الفرعية الرابعة.

الفصل الخامس: النتائج والتوصيات

1.5 تمهيد

يُمثّل هذا الفصل خلاصة الجهد البحثي الذي بُذل في هذه الدراسة، إذ يعرض أبرز النتائج التي توصّلت إليها الدراسة الميدانية بشأن أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية، مع تفسير كل نتيجة وربطها بنتائج الدراسات السابقة. ثم يُختتم الفصل بجملة من التوصيات العملية التي يقترحها الباحث في ضوء ما تم التوصل إليه.

2.5 نتائج الدراسة

أظهرت نتائج التحليل الإحصائي أن المتوسط العام لتطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية جاء بدرجة مرتفعة بمتوسط حسابي بلغ (4.12)، ويعود ذلك إلى تنامي الوعي المؤسسي بأهمية تبني التقنيات الناشئة في القطاع الصحي، وارتباط ذلك بتوجهات رؤية المملكة (2030) في التحول الرقمي للخدمات الصحية، فضلاً عن الضغوط التنظيمية المتزايدة الناجمة عن نظام حماية البيانات الشخصية السعودي. وتتفق هذه النتيجة مع ما توصّلت إليه دراسة (الهلال، 2020) التي أكدت أن المؤسسات الصحية السعودية تتجه نحو تبني حلول رقمية متقدمة لإدارة البيانات، كما تتسجم مع نتائج (Adeghe et al., 2024) التي بيّنت أن المؤسسات الصحية على المستوى الدولي تشهد تحولاً ملحوظاً نحو دمج تقنية سلاسل الكتل في منظومات إدارة البيانات الصحية.

كما كشفت النتائج عن أن بُعد "سلامة البيانات وعدم قابليتها للتعديل" جاء في المرتبة الأولى بين أبعاد المتغير المستقل بمتوسط حسابي بلغ (4.17)، ويُعزى ذلك إلى الطبيعة الفريدة لهذه الخاصية التي تُميّز تقنية سلاسل الكتل عن سواها من التقنيات؛ إذ يدرك العاملون في القطاع الصحي أن البيانات الطبية تتطلب درجة عالية من الموثوقية وعدم القابلية للتلاعب نظراً لارتباطها المباشر بسلامة المرضى وقراراتهم العلاجية. وتتسق هذه النتيجة مع ما خلصت إليه دراسة (Vanin et al., 2022) من أن خاصية عدم القابلية للتعديل تُعدّ الركيزة الأكثر جاذبية في تطبيقات سلاسل الكتل الصحية، وتتقاطع كذلك مع ما أشارت

إليه دراسة (Masood et al., 2024) من أن السجلات الطبية المُخزّنة على سلاسل الكتل تتمتع بمستوى عالٍ من السلامة والموثوقية.

وأظهرت النتائج أن بُعد "العقود الذكية للتحكم في الوصول" جاء في المرتبة الثانية بمتوسط (4.13)، ويرجع ذلك إلى إدراك المبحوثين لأهمية الأتمتة في حوكمة صلاحيات الوصول، وما توفّره العقود الذكية من تقليل للتدخل البشري وما يصاحبه من أخطاء محتملة، فضلاً عن قدرتها على إنفاذ القواعد التنظيمية بصورة فورية ومتسقة. وينسجم ذلك مع ما توصّلت إليه دراسة (Esmaeilzadeh, 2022) من أن الأطباء والإداريين يُولون أهمية متزايدة لآليات التحكم الآلي في الوصول إلى السجلات الصحية، كما يتفق مع ما أكّده دراسة (Yaqoob et al., 2022) من أن العقود الذكية تُمثّل آلية فاعلة في تنظيم التفاعل بين الأطراف المتعددة في المنظومة الصحية.

وفيما يخص بُعد "التشفير اللامركزي للبيانات"، فقد جاء بمتوسط حسابي بلغ (4.09)، ويُفسّر ذلك بإدراك المبحوثين لقصور النماذج المركزية التقليدية في حماية البيانات الصحية في ظل تصاعد الهجمات السيبرانية، وما يوفّره النموذج اللامركزي من توزيع للمخاطر وتجنّب نقاط الفشل المفردة. وتتوافق هذه النتيجة مع ما توصّلت إليه دراسة (Alsamhi et al., 2024) من أن النماذج اللامركزية القائمة على سلاسل الكتل تُقدّم مستوى حماية يفوق ما توفّره الحلول التقليدية، كما تتسق مع ما أشارت إليه دراسة (Afrihyia et al., 2025) من أن دمج التشفير المتقدم مع البنى اللامركزية يُمثّل توجهاً عالمياً في حماية بيانات المرضى.

كما بيّنت النتائج أن بُعد "آليات إدارة الموافقة والتفويض" جاء في المرتبة الرابعة بمتوسط حسابي بلغ (4.07) وهو مستوى مرتفع، غير أن تأخّر ترتيبه نسبياً يُفسّر بحداثة هذا المفهوم في البيئة الصحية السعودية، وارتباطه بأبعاد ثقافية وتنظيمية تتعلق بدور المريض في التحكم بمشاركة بياناته، وهو دور لا يزال في طور التطور التشريعي والتطبيقي. وتتسجم هذه النتيجة مع ما توصّلت إليه دراسة (العنزي والرابغي، 2025) من أن تمكين المرضى من التحكم في موافقاتهم يُعدّ من المتطلبات الناشئة في المدن الصحية الذكية، كما تتفق مع نتائج (Handayani et al., 2023) التي أبرزت أهمية آليات الموافقة الإلكترونية الموثقة في تعزيز ثقة المرضى.

وأظهرت النتائج أن المتوسط العام لخفض مخاطر الخصوصية وتسرب البيانات بلغ (4.10) بدرجة مرتفعة، ويعكس ذلك إدراك العاملين في المؤسسات الصحية لفاعلية تقنية سلاسل الكتل في معالجة التحديات

المتزايدة لحوادث تسرب البيانات الصحية على المستويين المحلي والعالمي، خاصةً مع تنامي الاعتماد على السجلات الصحية الإلكترونية وتكاملها بين الجهات المختلفة. وتتسجم هذه النتيجة مع ما توصلت إليه دراسة (Adusumilli et al., 2023) من أن تقنية سلاسل الكتل تُقدّم حلولاً عملية للحدّ من حوادث الخصوصية في الأنظمة الصحية، كما تتقاطع مع نتائج (Shojaei et al., 2024) التي أكدت أن دمج التقنيات الناشئة في النظم الصحية يُسهم في تعزيز منظومة حماية البيانات.

وأكدت نتائج تحليل الانحدار المتعدد وجود أثر ذي دلالة إحصائية لأبعاد تقنية سلاسل الكتل مجتمعةً على خفض مخاطر الخصوصية وتسرب البيانات بمعامل تحديد بلغ ($R^2 = 0.776$) ، أي أن (77.6%) من التباين في خفض المخاطر يُفسّر بالأبعاد الأربعة، ويُعزى ذلك إلى التكامل الوظيفي بين هذه الأبعاد إذ يُعزّز كل بُعد دور البعد الآخر ضمن منظومة موحّدة لحماية البيانات. وتتسق هذه النتيجة مع ما خلصت إليه دراسة (Chianumba et al., 2022) من أن الدمج بين مكونات سلاسل الكتل يُحقّق أثراً تكاملياً في حماية البيانات الصحية، كما تتوافق مع ما أكدته دراسة (Yaqoob et al., 2022) من أن الأثر التراكمي لمكونات التقنية يفوق الأثر المنفرد لكل مكون.

وكشفت النتائج عن أن بُعد "سلامة البيانات وعدم قابليتها للتعديل" هو الأكثر تأثيراً في خفض مخاطر الخصوصية وتسرب البيانات بمعامل انحدار بلغ ($B = 0.326$) ، ويرجع ذلك إلى الارتباط المباشر بين موثوقية البيانات وانخفاض احتمالية اختراقها أو التلاعب بها دون اكتشاف، فضلاً عن أن السجلات غير القابلة للتعديل تُقلّل من نطاق التهديدات الداخلية. وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Masood et al., 2024) من أن خاصية عدم القابلية للتعديل تُمثّل العنصر الأقوى تأثيراً في منظومة حماية البيانات الصحية، كما تتسجم مع نتائج (Vanin et al., 2022) التي أبرزت محورية هذا البُعد في تحقيق الأمن المعلوماتي.

وأظهرت النتائج أن بُعد "العقود الذكية للتحكم في الوصول" جاء في المرتبة الثانية من حيث قوة التأثير بمعامل انحدار بلغ ($B = 0.298$) ، ويُفسّر ذلك بقدرة العقود الذكية على إنفاذ سياسات الوصول بشكل آلي وفوري، ممّا يُقلّل من الفجوات التشغيلية التي قد تنشأ من الاعتماد على الإجراءات اليدوية. وتتسجم هذه النتيجة مع ما خلصت إليه دراسة (Handayani et al., 2023) من أن العقود الذكية تُسهم بشكل دال في تعزيز الخصوصية، كما تتقاطع مع ما أشارت إليه دراسة (Afrihyia et al., 2025).

كما أظهرت النتائج أن بُعْدِي "التشفير اللامركزي" بمعامل انحدار ($B = 0.241$) ، و"آليات إدارة الموافقة والتفويض" بمعامل انحدار ($B = 0.189$) يُسهمان بشكل دال في خفض مخاطر الخصوصية وتسرب البيانات، وإن جاء أثرهما أقل نسبياً مقارنة بالبُعدين الآخرين، ويُعزى ذلك إلى أن أثر هذين البُعدين يتحقق بصورة أكبر عند تكاملهما مع البُعدين الأكثر تأثيراً ضمن منظومة واحدة، وأن استثمارهما المنفرد قد لا يُحقّق المردود الكامل إلا في ظل بنية تحتية ناضجة وتشريعات داعمة. وتتسق هذه النتيجة مع ما خلصت إليه دراسة (Alsamhi et al., 2024) من أن التشفير اللامركزي يُحقّق أثره الأكمل ضمن منظومة متكاملة، كما تتوافق مع ما أكدته دراسة (العنزي والرابعي، 2025) من أن آليات الموافقة تتطلب إطاراً تشريعياً وتنظيمياً ناضجاً لتحقيق أثرها الكامل.

3.5 توصيات الدراسة

في ضوء ما تقدّم، يُقدّم الباحث جملة من التوصيات الموجّهة إلى الجهات المعنية بالقطاع الصحي في المملكة العربية السعودية:

- تبني تقنية سلاسل الكتل بوصفها ركيزة استراتيجية ضمن منظومة التحول الرقمي في المؤسسات الصحية السعودية، وإدراجها ضمن الخطط التشغيلية لوزارة الصحة والتجمعات الصحية.
- إعطاء الأولوية لتطبيق آليات سلامة البيانات وعدم قابليتها للتعديل عند تصميم البنى التحتية الجديدة للسجلات الصحية الإلكترونية، نظراً لكونها الأكثر تأثيراً في خفض مخاطر الخصوصية.
- تطوير منصة وطنية موحّدة قائمة على سلاسل الكتل لمشاركة البيانات الصحية بين المؤسسات الصحية الحكومية والخاصة، تحت إشراف المركز الوطني للمعلومات الصحية.
- سنّ تشريعات وأنظمة تفصيلية تُنظّم استخدام العقود الذكية في حوكمة الوصول إلى البيانات الصحية، بما يضمن التوافق مع نظام حماية البيانات الشخصية السعودي.
- إنشاء إطار تنظيمي وطني لإدارة موافقات المرضى الإلكترونية يُمكنهم من التحكم في مشاركة بياناتهم الصحية وسحب موافقاتهم متى شاؤوا.
- تنفيذ برامج تدريبية متخصصة للعاملين في المؤسسات الصحية حول تقنية سلاسل الكتل وتطبيقاتها في حماية البيانات الصحية، مع التركيز على الكوادر التقنية والإدارية.
- تخصيص ميزانيات مستقلة لتحديث البنية التحتية التقنية في المؤسسات الصحية بما يُمكن من احتضان تطبيقات سلاسل الكتل بكفاءة.

- عقد شراكات بحثية بين المؤسسات الصحية والجامعات السعودية لتطوير حلول وطنية مبتكرة قائمة على سلاسل الكتل تُلبّي الخصوصية التشريعية والثقافية للقطاع الصحي السعودي.
- إنشاء مراكز عمليات أمن سيبراني متخصصة تستثمر إمكانيات سلاسل الكتل في الرصد الفوري لمحاولات الاختراق والاستجابة لها.
- إطلاق حملات توعية موجّهة للمرضى تُعرّفهم بحقوقهم في التحكم ببياناتهم الصحية والآليات الإلكترونية المتاحة لإدارة موافقاتهم.
- تطوير مؤشرات أداء وطنية لقياس فاعلية تطبيق تقنية سلاسل الكتل في خفض حوادث تسرب البيانات الصحية، ومراجعتها دورياً.
- تعزيز التعاون الدولي وتبادل الخبرات مع الدول الرائدة في تطبيق سلاسل الكتل في القطاع الصحي للاستفادة من الممارسات الفضلى.

4.5 الدراسات المقترحة

يقترح الباحث إجراء دراسات مستقبلية في المحاور الآتية:

1. أثر تطبيق تقنية سلاسل الكتل على جودة الخدمات الصحية في المؤسسات الصحية السعودية.
2. التحديات التشريعية والتنظيمية لتطبيق سلاسل الكتل في القطاع الصحي بدول مجلس التعاون الخليجي: دراسة مقارنة.
3. أثر التكامل بين تقنية سلاسل الكتل والذكاء الاصطناعي على إدارة السجلات الصحية الإلكترونية.
4. مدى استعداد المؤسسات الصحية السعودية لتبني تقنية سلاسل الكتل: دراسة تشخيصية.
5. أثر تقنية سلاسل الكتل على ثقة المرضى في مشاركة بياناتهم الصحية بالمملكة العربية السعودية.

Abstract

This study aimed to investigate the impact of applying blockchain technology in healthcare data sharing—through its dimensions (decentralized data encryption, smart contracts for access control, data integrity and immutability, and consent and authorization management mechanisms)—on reducing privacy and data leakage risks in healthcare institutions in the Kingdom of Saudi Arabia. The study adopted the descriptive-analytical approach, employing a questionnaire as the primary data collection instrument. A stratified random sample was drawn from professionals involved in healthcare data management and information technology across Saudi healthcare institutions, yielding (373) valid responses for analysis. Data were processed statistically using SPSS V.26.

The study revealed a statistically significant impact at the significance level ($\alpha \leq 0.05$) of blockchain technology dimensions, collectively, on reducing privacy and data leakage risks, with a coefficient of determination ($R^2 = 0.776$), indicating that (77.6%) of the variance in risk reduction is explained by these dimensions. The findings showed that the data integrity and immutability dimension had the strongest effect ($B = 0.326$), followed by smart contracts for access control ($B = 0.298$), then decentralized encryption ($B = 0.241$), and finally consent and authorization management mechanisms ($B = 0.189$). In light of these findings, the study recommended adopting blockchain technology as a strategic pillar within the healthcare digital transformation system, developing a unified national platform for healthcare data sharing, and enacting legislation regulating the use of smart contracts and electronic consent mechanisms in alignment with the Saudi Personal Data Protection Law.

Keywords: Blockchain Technology, Healthcare Data Sharing, Data Privacy, Data Leakage, Healthcare Institutions, Kingdom of Saudi Arabia.

المراجع

المراجع العربية

- الخرابشة، 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>
- 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>
- 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>
- 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>
- 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>
- عبدالعظيم، رامي عبدالعظيم محمد. (2024). دور تطبيق تقنية سلاسل الكتل في تحسين العملية التدريبية بالتطبيق على العاملين بالبنك الأهلي المصري. مجلة البحوث الإدارية، مج42، ع3، 1 - 42. مسترجع من <http://search.mandumah.com/Record/1552209>

- عبدالعظيم، رامي عبدالعظيم محمد. (2025). أثر تطبيقات سلاسل الكتل على تقييم الأداء بالتطبيق على العاملين بقطاع البترول بجمهورية مصر العربية. مجلة البحوث الإدارية، مج43، ع1 ، 1 - 42. مسترجع من <http://search.mandumah.com/Record/1619518>
- 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>
- 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>
- 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>
- عبدالله، أمال علي إبراهيم. (2024). دور حوكمة أخلاقيات الذكاء الاصطناعي في خفض مخاطر وتحديات استخداماته: دراسة ميدانية. مجلة عجمان للدراسات والبحوث، مج23، ع2 ، 1 - 29. مسترجع من <http://search.mandumah.com/Record/1539126>
- 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>
- عبده، عبير ثابت أحمد. (2023). أثر تطبيق تقنية سلاسل الكتل في تحسين الكفاءة التشغيلية وتجنب الاحتيال في شركات التأمين المصرية: دراسة ميدانية. مجلة الإسكندرية للبحوث المحاسبية، مج7، ع2 ، 283 - 326. مسترجع من <http://search.mandumah.com/Record/1514333>
- العنزي، حنان عواد، و الرابعي، 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>

- عيد، محمود محمد زكي. (2025). أثر تطبيق تقنية سلاسل الكتل في ترشيد التكاليف البينية في ظل مدخل التكاليف على أساس المواصفات: دراسة ميدانية. مجلة البحوث الإدارية، مج43، ع3 ، 2 - 40. مسترجع من <http://search.mandumah.com/Record/1668239>
- الفهمي، أصايل عبدالله، المالكي، ندى حمدان، و حمبيشي، 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>
- محمد، سعاد خميس علي. (2025). أثر تطبيق تقنيات سلاسل الكتل على فعالية نظام الرقابة الداخلية: دراسة حالة على البنك الأهلي المصري. مجلة الإبداع المحاسبي، مج2، ع2 ، 315 - 355. مسترجع من <http://search.mandumah.com/Record/1626508>
- مرسل، محي الدين كوكو بخيت، و حسن، حسن حسين محمد. (2025). أثر تطبيق تقنية البلوك تشين "سلاسل الكتل" في إدارة وحفظ التراث الثقافي. 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، 509 - 522. مسترجع من <http://search.mandumah.com/Record/1653632>
- 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>
- 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>

المراجع الأجنبية

- 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.
- Adusumilli, S., Damancharla, H., & Metta, A. (2023). Enhancing data privacy in healthcare systems using blockchain technology. Trans. Latest Trends Artif. Intell, 4(4)

- 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.
- 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.
- Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., ... & Curry, E. (2024). Federated learning meets blockchain in decentralized data sharing: Healthcare use case. *IEEE Internet of Things Journal*, 11(11), 19602-19615
- 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
- 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.
- Esmaeilzadeh, 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.
- 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
- 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
- Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. *Computers*, 13(2), 41.
- 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.
- 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.

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

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

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأتقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا البحث، وسوف أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

1- النوع الاجتماعي ☐ ذكر ☐ أنثى

2- العمر ☐ 30 سنة فأقل ☐ من 40 - 30 سنة
☐ 40 - 50 سنة ☐ من 50 سنة فأكثر

3- المؤهل العلمي ☐ دبلوم ☐ بكالوريوس
☐ ماجستير ☐ دكتوراه

4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 - 10 سنوات
☐ من 10 - 15 سنة ☐ أكثر من 15 سنة

5- طبيعة الوظيفة ☐ مدير / مسؤول تقنية المعلومات ☐ مسؤول أمن المعلومات
☐ مسؤول سجلات طبية إلكترونية ☐ طبيب / ممارس صحي
☐ إداري في المعلومات الصحية

6- حجم المؤسسة الصحية

☐ صغيرة (أقل من 100 سرير) ☐ متوسطة (100 - 300) سرير
☐ كبيرة (أكثر من 300 سرير)

ثانياً محاور الاستبيان

✿ المحور الأول: تطبيق تقنية سلاسل الكتل، ضع إشارة (✓) في المربع المناسب لاختيارك:

المبعد	أوافق بشدة	أوافق	محايد	معارض	معارض بشدة
التشفير اللامركزي للبيانات					
تعتمد المؤسسة الصحية على تشفير البيانات بطريقة لامركزية لحماية السجلات الطبية					
يسهم التشفير اللامركزي في منع اختراق البيانات الصحية من قبل أطراف غير مصرح لها					
توزع نسخ البيانات المشفرة على عقد متعددة لضمان عدم وجود نقطة فشل واحدة					
يوفر التشفير اللامركزي ثقة أعلى لدى المرضى تجاه مشاركة بياناتهم الصحية					
العقود الذكية للتحكم في الوصول					
تحدد العقود الذكية صلاحيات الوصول إلى البيانات الصحية تلقائياً وفق قواعد مبرمجة					
تقلل العقود الذكية من التدخل البشري في إدارة صلاحيات الوصول إلى السجلات					
تنفذ العقود الذكية إجراءات منع الوصول فور رصد محاولات غير مصرح بها					
تسهم العقود الذكية في توثيق كل عملية وصول إلى البيانات بشكل آلي قابل للتدقيق					
سلامة البيانات وعدم قابليتها للتعديل					
تضمن تقنية سلاسل الكتل عدم إمكانية تعديل البيانات الصحية بعد تسجيلها					
تُحافظ السلسلة الرقمية على تسلسل التعديلات بصورة موثقة وقابلة للتتبع					

المعارض بشدة	معارض	محايد	أوافق	أوافق بشدة	البعد
					يُكشف عن أي محاولة تلاعب بالبيانات الصحية فور حدوثها
					تُعزّز خاصية عدم القابلية للتعديل ثقة الجهات الرقابية في البيانات الصحية
آليات إدارة الموافقة والتفويض					
					تتيح التقنية للمريض منح الموافقة على مشاركة بياناته الصحية إلكترونياً
					تُمكن آليات التفويض المرضى من سحب موافقتهم في أي وقت
					تُوثّق جميع موافقات المرضى على سلسلة الكتل بصورة لا يمكن إنكارها
					تُحدّد مدة صلاحية التفويض لكل جهة مستفيدة من البيانات الصحية

✿ المحور الثاني: خفض مخاطر الخصوصية وتسرب البيانات، ضع إشارة (✓) في المربع المناسب لاختيارك:

المبعد	أوافق بشدة	أوافق	محايد	معارض	معارض بشدة
تُسهّم تقنية سلاسل الكتل في تقليل حوادث تسرب البيانات الصحية للمرضى					
تُقلّل التقنية من فرص الوصول غير المشروع إلى البيانات الصحية الحساسة					
تُعزّز التقنية من الالتزام بمتطلبات حماية الخصوصية وفق نظام حماية البيانات السعودي					
تُقلّل التقنية من المخاطر التشغيلية الناتجة عن أخطاء التعامل البشري مع البيانات					
تُقلّل التقنية من المخاطر القانونية المرتبطة بانتهاكات خصوصية المرضى					
تُتيح التقنية كشف محاولات الاختراق في الوقت الفعلي					
تُقلّل التقنية من اعتماد المؤسسة على الأطراف الوسيطة في مشاركة البيانات					
تُسهّم التقنية في تعزيز السمعة الرقمية للمؤسسة الصحية لدى المرضى					
تُقلّل التقنية من تكلفة الاستجابة لحوادث الخصوصية وتسرب البيانات					
تُحقّق التقنية تكاملاً فعالاً مع منظومة أمن المعلومات في المؤسسة الصحية					

مع خالص التقدير والاحترام

Mid Ocean University

College of Management

Department of risk management



**"The Impact of Applying Blockchain Technology in
Health Data Sharing on Reducing Privacy Risks and
Data Breaches: An Applied Analytical Study."**

Prepared by:

Barakat Shmelan Al-Azmi

Main supervisor/

Dr. Al-Faisal Abdelhamid

Second supervisor/

Dr. Fayez Jarad

2026 – 1448