

قضايا بحثية (2)

اعداد الباحث /
سامي

اشراف /
د / سائد عدنان





التكليف -5

(القضية البحثية الخامسة)

Chapter

بيانات الرسالة

عنوان الرسالة: دور الحوسبة السحابية في تعزيز النزاهة الرقمية
وحماية البيانات في المؤسسات التقنية.

إعداد الباحث / عبد الرحمن بن علي الشهري.

المجلة العربية للحوكمة الرقمية والأمن السيبراني

تاريخ النشر: 2026 م.

- عنوان الدراسة " دور الحوسبة السحابية في تعزيز النزاهة الرقمية وحماية البيانات في المؤسسات التقنية.
- المتغير المستقل: كفاءة الحوسبة السحابية (السرعة، المرونة، التوفر).
- المتغير التابع: النزاهة الرقمية وحماية البيانات (سلامة البيانات، منع التلاعب، سرعة الاستجابة).
- الخصائص: عنوان مباشر يربط بين التقنيات السحابية ومتطلبات النزاهة والأمن السيبراني.

مقدمة الدراسة

- اعتماد التسلسل المنطقي من واقع المؤسسات التقنية المعاصرة إلى ضرورة التحول السحابي الآمن.
- إبراز تحديات "النزاهة الرقمية" (Digital Integrity) كدافع رئيسي لإجراء هذه الدراسة.

مصطلحات الدراسة

- الحوسبة السحابية: نموذج تقني يتيح الوصول لموارد الحوسبة بتفاعل محدود مع مزود الخدمة.
- النزاهة الرقمية: هي ضمان دقة، وثبات، وموثوقية البيانات الرقمية طوال دورة حياتها، وحمايتها من أي تعديل غير مصرح به.
- حماية البيانات: ممارسة تأمين البيانات من الوصول غير المصرح به أو التلف باستخدام التشفير والتحقق من الهوية.

المشكلة البحثية

➤ المشكلة: التحدي المتزايد في ضمان النزاهة الرقمية وحماية البيانات في المؤسسات التقنية عند الاعتماد على بيانات سحابية.

أسئلة الدراسة

➤ السؤال الرئيسي: ما دور الحوسبة السحابية في تعزيز النزاهة الرقمية وحماية

البيانات في المؤسسات التقنية؟

➤ الأسئلة الفرعية:

1. كيف تساهم الحوسبة السحابية في منع اللاعبين بالبيانات وضمان نزاهتها؟

2. ما هي التحديات التي تواجه المؤسسات التقنية في حماية بياناتها سحابياً؟

تمثل الهدف الرئيسي "بيان أثر الحوسبة السحابية في تعزيز النزاهة الرقمية (سلامة البيانات من التلاعب) وضمان أمن وحماية البيانات في المؤسسات التقنية.

الأهداف الفرعية:

1. قياس مستويات النزاهة: تقييم كفاءة البروتوكولات السحابية في الحفاظ على سلامة البيانات وعدم تعرضها للتغيير غير المصرح به.
2. تحليل فاعلية الحماية: تحديد مدى قدرة البنية التحتية السحابية على توفير حماية قوية للبيانات الحساسة في المؤسسات التقنية.

- الهدف الرئيسي: الكشف عن طبيعة الأثر الذي تحدثه تبني تقنيات الحوسبة السحابية على مستويات أمن البيانات وسرعة استرجاعها في الشركات التقنية الناشئة
- الأهداف الفرعية:
 - قياس مستوى الأمان: تقييم كفاءة البروتوكولات الأمنية المستخدمة في الحوسبة السحابية لحماية البيانات الحساسة للشركات الناشئة.
 - تحليل فاعلية الاسترجاع: تحديد مدى قدرة البنية التحتية السحابية على تقليص زمن استرداد البيانات في حالات الهجمات السيبرانية أو الأعطال التقنية.
 - تحديد التحديات: رصد أبرز التحديات (التقنية والإدارية) التي تواجه الشركات الناشئة عند الانتقال إلى بيئة العمل السحابية.

- الموضوعية: النزاهة الرقمية وحماية البيانات في المؤسسات التقنية.
- المكانية: المؤسسات التقنية المستهدفة.
- الزمانية: عام 2026م.

فرضيات البحث

➤ **فرضية الدراسة الرئيسية متوافقة وعلى اتساق تام مع التساؤل الرئيسي والهدف الرئيسي للدراسة توجد علاقة ذات دلالة إحصائية بين تبني الحوسبة السحابية وتعزيز النزاهة الرقمية وحماية البيانات.**

➤ **الفرضيات الفرعية:**

1. **يوجد أثر إيجابي لاستخدام الحوسبة السحابية على "سلامة البيانات" ومنع التلاعب بها.**
2. **يوجد أثر إيجابي لاستخدام الحوسبة السحابية على كفاءة "حماية البيانات" من الهجمات.**

نموذج الدراسة

بناء نموذج الدراسة على العلاقة بين المتغيرات كما يلي:

- المتغير المستقل: الحوسبة السحابية (المرونة، التوفر، التكلفة).
- المتغير التابع: النزاهة الرقمية وحماية البيانات (سلامة البيانات، الحماية، استمرارية الأعمال).

المنهجية المستخدمة في الدراسة البحثية

- **المنهج: الوصفي التحليلي.**
- **الأداة: الاستبانة الإلكترونية الموجهة للمختصين التقنيين.**
- **التحليل: استخدام برنامج (SPSS) واختبارات الانحدار (Regression Analysis) لقياس قوة الأثر**

النتائج التي توصلت اليها الدراسة البحثية

تمثلت النتائج العامة للدراسة في 3 نقاط أساسية يمكن ايجازها في الاتي:

- وجود تأثير إيجابي: إثبات وجود علاقة ذات دلالة إحصائية بين كفاءة الحوسبة السحابية (السرعة، المرونة، التوفر) وتعزيز مستويات النزاهة الرقمية وحماية البيانات.
- التفوق التقني: أن المؤسسات التقنية التي تعتمد على معايير سحابية متقدمة تمتلك قدرة أعلى على منع التلاعب بالبيانات وضمان نزاهتها مقارنة بالأنظمة التقليدية.
- سرعة الاستجابة: الحوسبة السحابية تساهم بشكل جوهري في تعزيز سرعة استعادة البيانات وضمان استمرارية العمل في حال حدوث هجمات سيبرانية.

اهم التوصيات التي توصلت اليها الدراسة

بناء على نتائج الدراسة كانت هناك 3 توصيات يمكن تلخيصها كما يلي:

1. الاستثمار في التحديث المستمر: ضرورة استمرار المؤسسات التقنية في تحديث البروتوكولات السحابية المستخدمة لضمان مواكبة أحدث معايير النزاهة الرقمية والأمن السيبراني.
2. تبني أطر النزاهة الرقمية: التوصية بوضع "إطار عمل" داخل المؤسسات التقنية يربط بين مزايا الحوسبة السحابية ومتطلبات الحوكمة الرقمية لضمان سلامة البيانات.
3. الدراسات المستقبلية: إجراء دراسات مستقبلية توسعية تقارن بين مختلف مزودي الخدمات السحابية من حيث فعاليتهم في حماية النزاهة الرقمية للمؤسسات.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You