Al-Farouk journal of sciences
Volume (2), Issue (3) (JUNE, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) العدد 3 يونيو 2026
ردمد: 3135-2359

أمن البيانات في الحوسبة السحابية: تحليل التهديدات واستراتيجيات الحماية الوقائية

خيرية سالم وريث[1] ايمن ضو غانم[2]
khiryawrite84s@gmail.com a.ghanim@asmarya.edu.ly
[1]قسم تقنيات الحاسوب – المعهد العالي للعلوم والتقنية – قصر اخيار – ليبيا
[2]قسم نظم المعلومات – كلية تقنية المعلومات – الجامعة الاسمرية الإسلامية – ليبيا

Data Security in Cloud Computing: Threat Analysis and Preventive Protection Strategies

Khirya Salem Warith
Department of Computer Technology – Higher Institute of Science and Technology – Qasr Akhyar – Libya
Ayman Daw Ghanim
Department of Information Systems – Faculty of Information Technology – Asmarya Islamic University, Zliten – Libya

تاريخ الاستلام: 2026/04/02 تاريخ المراجعة 2026 /05/01 تاريخ القبول:2026/05/14- تاريخ النشر: 2026 /06/03

الملخص

يهدف البحث إلى دراسة أمن البيانات في الحوسبة السحابية، وتحليل التهديدات الأمنية التي تواجه البيانات المخزنة والمستخدمة في بيئات السحابة، بالإضافة إلى استعراض الحلول والتقنيات الوقائية لضمان سلامتها. مسلطا الضوء على مشكلة تعدد التهديدات وتأثيرها على سرية ونزاهة وتوافر البيانات، مثل الوصول غير المصرح به، تسرب البيانات، الهجمات الخبيثة، استغلالAPIs ، وفقدان البيانات.

تم تحليل الدراسات السابقة، وتصنيف التهديدات وفق نموذج (CIA) السرية، النزاهة، التوافر، وتقديم جدول شامل يوضح التهديدات، ويستعرض الحلول التقنية والإدارية مثل التشفير، التحكم في الوصول، المصادقة متعددة العوامل، النسخ الاحتياطي الدوري، المراقبة المستمرة، ونماذج الأمان الحديثة كـ Zero Trust.

توصل البحث إلى أن حماية البيانات السحابية تتطلب تضافر الحلول التقنية والسياسات الأمنية والتدريب على الوعي الأمني . وأظهرت النتائج أن اعتماد أفضل الممارسات يقلل بشكل كبير من حوادث الاختراق وتسرب البيانات، ويعزز ثقة المؤسسات والمستخدمين في الخدمات السحابية. في ضوء هذه النتائج، يوصى بتطبيق الإجراءات الوقائية المتكاملة، تعزيز السياسات الوطنية، وزيادة الوعي الأمني لدى المستخدمين لضمان حماية فعالة للبيانات في البيئات السحابية.

الكلمات الدالة: السحابة، الحماية، الحلول، التهديدات.

Abstract

This study aims to investigate data security in cloud computing, analyzing the security threats facing data stored and processed in cloud environments, and reviewing preventive solutions and techniques to ensure its protection. The research problem focuses on the diversity of threats and their impact on data confidentiality, integrity, and availability, including unauthorized access, data leakage, malicious attacks, API exploitation, and data loss.

The study reviews previous research, classifies threats according to the CIA model (Confidentiality, Integrity, Availability), and presents a comprehensive table illustrating the threats, practical examples, and their relation to prior studies. It also explores technical and administrative solutions, such as encryption, access control, multi-factor authentication, regular backups, continuous monitoring, and modern security models like Zero Trust.
The findings indicate that securing cloud data requires a combination of technical measures, security policies, and user awareness training. Moreover, applying best practices significantly reduces incidents of data breaches and enhances the trust of organizations and users in cloud services. Based on these results, the study recommends implementing integrated preventive measures, strengthening national security policies, and raising user awareness to ensure effective cloud data protection.
Keywords: cloud, protection, solutions, transparent

المقدمة

تعد الحوسبة السحابية من أبرز الابتكارات التكنولوجية والركائز الأساسية لعمل المؤسسات الحديثة، لإتاحتها تخزين البيانات، تشغيل التطبيقات، ومعالجة المعلومات عبر الإنترنت بمرونة وكفاءة عالية دون ارتباط بمكان أو زمن. عبر نماذجها المتعددة كـــ (IaaS, PaaS, SaaS) ، ممكنة المؤسسات من الوصول إلى قدرات تقنية متقدمة، تقلل لتكاليفها التشغيلية وتلغي الحاجة لإدارة البنية التحتية داخلياً(1).

تكمن مشكلة البحث في التصاعد المستمر للتهديدات الأمنية التي تستهدف البيانات ضمن بيئات الحوسبة السحابية، في ظل عدم كفاية التدابير والإجراءات الوقائية المتبعة لحمايتها، الأمر الذي يشكل خطراً مباشراً يهدد سرية المعلومات الحساسة ويقوض استمرارية الأعمال والموثوقية التشغيلية للمؤسسات.

الهدف الرئيسي: يتمثل الهدف الرئيسي لهذا البحث في إجراء دراسة لأمن البيانات في بيئات الحوسبة السحابية، مع التركيز على تحليل التهديدات الأمنية المعاصرة التي تواجهها، وتقديم استراتيجيات وحلول وقائية متطورة تضمن حماية خصوصية البيانات واستدامتها.

الأهداف الفرعية:

- تأصيل المفاهيم العلمية لأمن البيانات والخدمات السحابية المختلفة.
- تصنيف وتحليل التهديدات الأمنية وفق نموذج (CIA) لضمان السرية، النزاهة، والتوافر.
- استعراض أحدث التقنيات والتدابير الوقائية لمواجهة مخاطر الاختراق والوصول غير المصرح به.
- صياغة توصيات عملية تسهم في تعزيز مرونة الأمن السيبراني داخل المؤسسات وتفعيل نموذج المسؤولية المشتركة.

أهمية البحث: تتعزز أهمية البحث في كونه يمثل إضافة علمية وتقنية تثري المكتبة الأكاديمية بالتحليلات المفيدة حول أمن البيانات السحابية، مما يحفز الباحثين على التوسع في هذا المجال الحيوي. أما من الناحية العملية، فيوفر البحث مرجعية تقنية للمؤسسات والجهات الحكومية، مثل: هيئة أمن وسلامة المعلومات الليبية، عبر تزويدها بأساليب وسياسات فعالة لتعزيز موثوقية الخدمات السحابية. كما يسهم البحث في رفع الوعي الأمني لدى المستخدمين والموظفين، مما يقلل من المخاطر البشرية المرتبطة بالبيانات ويعزز بنية الأمن السيبراني بشكل شامل".

منهجية البحث:يعتمد البحث على المنهج الوصفي التحليلي كإطار عمل متكامل، حيث يبدأ بوصف وتأصيل مفا هيم الحوسبة السحابية وأمن البيانات، لينتقل بعدها إلى تحليل التهديدات الأمنية المعاصرة وتحديد مسبباتها الأساسية. كما

تتضمن المنهجية دراسة معمقة للآليات والتقنيات الوقائية الحديثة، بالاستناد إلى مراجعة شاملة للمراجع العلمية والدراسات السابقة ذات الصلة. ويختتم البحث بتحليل النتائج المستخلصة لصياغة توصيات عملية تساهم في تحصين بيئات البيانات السحابية وتعزيز أمنها.

حدود البحث:

- **الحدود الموضوعية** :يركز البحث حصراً على دراسة أمن البيانات في بيئات الحوسبة السحابية وتحليل تهديداتها، دون التوسع في التفاصيل البرمجية أو الجوانب التقنية المعقدة الخارجة عن نطاق التأمين.
- **الحدود الزمنية** :اعتمدت الدراسة على المراجع العلمية والبيانات التقنية الصادرة في السنوات الأخيرة، لضمان مواكبة التطورات المتسارعة في التهديدات والحلول السحابية.
- **الحدود المكانية** :يتناول البحث مفهوم الحوسبة السحابية وتطبيقاتها من منظور عام وشامل، مما يجعله قابلاً للتطبيق والاستفادة منه في مختلف البيئات المؤسسية دولياً ومحلياً.

الدراسات السابقة

تشكل الدراسات السابقة حجر الأساس لأي بحث أكاديمي، حيث تساعد الباحث على فهم الوضع الحالي للموضوع وتحديد الثغرات البحثية التي يمكن معالجتها. وفي مجال أمن البيانات في الحوسبة السحابية، ركزت الدراسات السابقة على تحليل التهديدات والمخاطر ، تقييم فاعلية تقنيات الحماية، واستكشاف أفضل الممارسات لضمان حماية البيانات المخزنة والمستخدمة في البيئات السحابية.

تدفع هذه الدراسات الباحثين نحو:

- تعزيز المعرفة العلمية حول تهديدات البيانات السحابية وأساليب الوقاية منها.
- تقديم إسهامات عملية للمؤسسات والشركات في تعزيز الأمن السيبراني عند استخدام الخدمات السحابية.
- دعم صانعي القرار في وضع سياسات وإجراءات أمنة لحماية البيانات.

المشكلة التي تناولتها الدراسات السابقة

ركزت الدراسات السابقة على عدة مشاكل رئيسية تواجه أمن البيانات في الحوسبة السحابية، أهمها:

1. الوصول غير المصرح به إلى البيانات بسبب ضعف التحكم في الهوية والمصادقة.
2. تسرب البيانات أو فقدانها نتيجة أخطاء بشرية، هجمات خبيثة، أو خلل في مزود الخدمة.
3. ضعف التشفير وعدم كفاية السياسات الأمنية، مما يجعل البيانات معرضة للاختراق.
4. انخفاض الوعي الأمني لدى المستخدمين، مما يزيد من فرص وقوع حوادث أمنية.

أهداف الدراسات السابقة

هدفت الدراسات السابقة إلى:

1. تحديد مفهوم أمن البيانات في الحوسبة السحابية وفهم خصائصه الأساسية.
2. تحليل التهديدات والمخاطر الأمنية التي تواجه البيانات السحابية.
3. تقييم فعالية التقنيات الأمنية مثل التشفير والتحكم في الوصول والمصادقة متعددة العوامل.

4. اقتراح حلول واستراتيجيات لتعزيز أمن البيانات وحماية المؤسسات من المخاطر السيبرانية.

الأدوات والمنهجية المستخدمة

- استخدمت الدراسات السابقة المنهج الوصفي التحليلي، حيث تم جمع البيانات من مصادر متعددة مثل:
  - الدراسات الأكاديمية والمقالات العلمية.
  - تقارير المؤسسات والشركات المزودة للخدمات السحابية.
  - الحوادث الواقعية المتعلقة بانتهاك البيانات السحابية.
- بعض الدراسات استخدمت **الدراسات الميدانية والاستبانات** لتقييم مستوى الوعي الأمني لدى المستخدمين والعاملين في المؤسسات.

النتائج المتوصل إليها

- توصلت الدراسات إلى أن أمن البيانات في الحوسبة السحابية يعتمد على تضافر عدة عوامل :التشفير القوي، التحكم الدقيق في الوصول، المصادقة متعددة العوامل، ومراقبة الأنشطة السحابية بشكل مستمر.
- أكدت الدراسات أن ضعف الوعي الأمني والسياسات غير الفعالة يمثلان أكبر المخاطر التي تواجه حماية البيانات السحابية.
- أظهرت الدراسات أن تبني أفضل الممارسات العالمية مثل النسخ الاحتياطي الدوري، اختبارات الاختراق، وتطبيق نموذج انعدام الثقة (Zero Trust) يقلل من حوادث اختراق البيانات بشكل كبير.
- خلصت بعض الدراسات العربية إلى ضرورة تطوير سياسات أمنية وطنية موحدة ودعم المؤسسات بالتدريب والتوعية لتعزيز مستوى الأمان السيبراني في البيئات السحابية.

.1الدراسات العالمية

1. **Mell & Grance (2011)**

- قدمت هذه الدراسة التعريف الرسمي للحوسبة السحابية من خلال **المعهد الوطني للمعايير والتقنية(NIST)** ، وأكدت على أهمية حماية البيانات المخزنة والمعالجة في السحابة.
- ركزت الدراسة على **التهديدات الأمنية الأساسية** مثل الوصول غير المصرح به، وفقدان البيانات، وأهمية تطبيق أساليب التشفير المتقدمة.

2. **Subashini & Kavitha (2011)**

- أجرت الدراسة **تحليلًا لنماذج الخدمة السحابية (IaaS, PaaS, SaaS)** وحددت أبرز المخاطر المرتبطة بكل نموذج.
- أكدت الدراسة على ضرورة **اعتماد آليات التحكم في الوصول ومصادقة المستخدمين** لتقليل مخاطر الهجمات.

3. **Hashizume et al. (2013)**

- استعرضت الدراسة مجموعة من **الحوادث الواقعية لانتهاك البيانات في البيئات السحابية**، مع التركيز على الثغرات الأمنية في إعدادات مزودي الخدمات.

- أوصت الدراسة بـ **تبني سياسات أمنية صارمة وعمليات تدقيق دورية** لضمان حماية البيانات.

.2الدراسات العربية

1. **الزيات (2018)، مصر**

- ركزت الدراسة على **أمن البيانات في المؤسسات الحكومية** عند استخدام الحوسبة السحابية، وأبرزت التحديات المتعلقة **بالخصوصية والسياسات الوطنية.**
- أوصت الدراسة بتطوير **إطار تشريعي وأمني موحد** لحماية البيانات السحابية في المؤسسات العربية.

2. **المغربي (2020)، المغرب**

- تناولت الدراسة **تقنيات التشفير والتحكم في الوصول** في البيئات السحابية.
- أشارت إلى أن **ضعف الوعي الأمني لدى المستخدمين** يعد أحد العوامل الرئيسية في تسرب البيانات، ودعت إلى برامج تدريبية لتعزيز الثقافة الأمنية.

3. **أبو الحسن وآخرون (2021)، ليبيا**

- ركزت الدراسة على **أمن البيانات في المؤسسات الليبية**، خاصة الجهات التي تعتمد على السحابة مثل **هيئة أمن وسلامة المعلومات.**
- أوصت الدراسة بـ **اعتماد منهجيات تقييم المخاطر الدورية** وتطبيق أفضل الممارسات العالمية في الحماية.

مؤلف/السنة	فكرة ودوافع الدراسة	المشكلة	أهداف الدراسة	الأدوات والمنهجية	النتائج المتوصل إليها
Mell & Grance (2011)	تقديم تعريف رسمي للحوسبة السحابية عبر NISTوتحليل أبعاد الأمن فيها	الحاجة لفهم التهديدات الأمنية المرتبطة بالبيانات المخزنة في السحابة	توضيح مفهوم الحوسبة السحابية وتعريف معايير الأمن الأساسية	منهج وصفي تحليلي قائم على مراجعة الأدبيات والتعريفات الرسمية	ركزت على أهمية حماية البيانات وتطبيق التشفير وأدوات التحكم في الوصول
Subashini & Kavitha (2011)	تحليل نماذج الخدمة السحابية المختلفة (IaaS, PaaS, SaaS) من منظور الأمان	التعرف على نقاط ضعف كل نموذج خدمة سحابية	تحديد المخاطر المرتبطة بكل نموذج خدمة واقتراح حلول حماية	منهج وصفي تحليلي، مراجعة الدراسات السابقة	أوصت بتطبيق آليات التحكم في الوصول والمصادقة لتقليل المخاطر
Hashizume et al. (2013)	دراسة حوادث اختراق البيانات في البيئات السحابية	الثغرات الأمنية في إعدادات مزودي الخدمات السحابية	تحليل حوادث اختراق البيانات واستعراض التوصيات الوقائية	دراسة حالات واقعية وتحليل بيانات	ضرورة اعتماد سياسات أمنية صارمة وعمل تدقيق دوري لتقليل الاختراقات
الزيات (2018، مصر)	دراسة أمن البيانات في المؤسسات الحكومية العربية	تحديات حماية البيانات والحفاظ على الخصوصية	تطوير إطار أمني لتأمين البيانات الحكومية	مراجعة أدبيات وأطر تشريعية، دراسة حالة المؤسسات الحكومية	أوصت بوضع سياسات وطنية موحدة لتعزيز حماية البيانات
المغربي (2020، المغرب)	دراسة تأثير التشفير والتحكم في الوصول على حماية البيانات	ضعف الوعي الأمني لدى المستخدمين يؤدي لتسرب البيانات	تحليل فعالية تقنيات التشفير والتحكم في الوصول	منهج وصفي، مراجعة الأدبيات، مقابلات مع المستخدمين	تعزيز التدريب والوعي الأمني يقلل من حوادث تسرب البيانات
أبو الحسن وآخرون (2021، ليبيا)	تحليل أمن البيانات في المؤسسات الليبية وخاصة الجهات الحكومية	غياب تقييم دوري للمخاطر وغياب تطبيق أفضل الممارسات	تقييم الوضع الحالي للأمن السحابي في المؤسسات الليبية	منهج وصفي تحليلي، مراجعة السياسات، دراسة حالات	أوصت بتطبيق تقييم المخاطر الدوري واعتماد أفضل الممارسات العالمية في حماية البيانات

.3خلاصة الدراسات السابقة

- تشير الدراسات السابقة إلى أن **أمن البيانات في الحوسبة السحابية** يتأثر بعدة عوامل: ضعف التشفير، التحكم المحدود في الوصول، سوء إعداد السياسات الأمنية، وضعف الوعي الأمني.
- هناك اتفاق عام على أن **التقنيات الحديثة** مثل التشفير المتقدم، المصادقة متعددة العوامل، المراقبة الذكية، وتطبيق نموذج انعدام الثقة (Zero Trust) تمثل حلولاً فعالة لتعزيز حماية البيانات.
- تبرز الحاجة إلى **دراسات محدثة** على المستوى المحلي والعربي لتقييم الوضع الحالي وتقديم توصيات قابلة للتطبيق في المؤسسات، خصوصًا في ليبيا.

التهديدات الأمنية للبيانات في بيئات الحوسبة السحابية

مع الانتشار الواسع للحوسبة السحابية واعتماد المؤسسات والشركات على خدماتها لتخزين ومعالجة البيانات، أصبحت التهديدات الأمنية أحد أبرز التحديات التي تواجه أمن البيانات السحابية. يهدف هذا الفصل إلى توضيح مفهوم الحوسبة السحابية، أنواعها، التهديدات الأمنية، وأقسامها، وربطها بما تم التوصل إليه في الدراسات السابقة.(2)

أولاً: الحوسبة السحابية وأنواعها

الحوسبة السحابية (Cloud Computing) هي نموذج لتقديم الخدمات التقنية عبر الإنترنت، يشمل التخزين والمعالجة وقواعد البيانات والتطبيقات، بحيث يمكن للمستخدم الوصول إليها حسب الحاجة دون الحاجة لإدارة البنية التحتية.

أنواع الحوسبة السحابية نماذج الخدمة:

1. **البنية كخدمة :(IaaS)** توفير خوادم وتخزين وشبكات جاهزة للاستخدام، مع مسؤولية المستخدم عن إدارة الأنظمة والتطبيقات.
2. **المنصة كخدمة :(PaaS)** توفير بيئة تطوير وتشغيل التطبيقات دون إدارة البنية التحتية، مع تقاسم المسؤولية الأمنية بين المستخدم والمزود.
3. **البرمجيات كخدمة :(SaaS)** تطبيقات جاهزة للاستخدام عبر الإنترنت، غالبًا يكون المزود مسؤولاً عن الأمن والخصوصية.

ثانياً: تعريف التهديدات الأمنية

التهديدات الأمنية (Security Threats) هي أي عامل أو حدث محتمل أن يؤدي إلى اختراق سرية أو نزاهة أو توافر البيانات في بيئة الحوسبة السحابية، حيث يمكن أن تكون هذه التهديدات ناتجة عن **أخطاء بشرية، هجمات سيبرانية، ثغرات تقنية، أو سوء إعداد سياسات الأمان**، وتشكل خطرًا مباشرًا على المؤسسات والمستخدمين على حد سواء.

وقد أشـارت الدراسـات السـابقة، مثل (2011) Mell & Grance و(2013) Hashizume et al. ، إلى أن التهديدات السـحابية تتنوع بين **الاختراقات، تسرب البيانات، ضـعف التشـفير، وسـوء إدارة الوصـول**، وهي الأسـباب الرئيسـية لانتهاك البيانات.

ثالثاً: أنواع التهديدات الأمنية في الحوسبة السحابية

يمكن تصـنيف التهديدات الأمنية في الحوسـبة السـحابية إلى عدة أنواع رئيسـية، مرتبطة مباشـرة بما تم ذكره في الدراسـات السابقة:

1. **الوصول غير المصرح به(Unauthorized Access)**
   - يشير إلى محاولات الوصول إلى البيانات أو الموارد السحابية دون تصريح.
   - يرتبط بذلك ضعف نظم المصادقة أو استخدام كلمات مرور ضعيفة.
   - **دراسـة** (2011) Subashini & Kavitha أبرزت أن التحكم في الوصـول يمثل نقطة ضـعف رئيسـية في نماذج الخدمة المختلفة.
2. **تسرب البيانات(Data Leakage)**
   - يحدث عندما تنتقل البيانات إلى جهات غير مخوَّلة، سواء أثناء التخزين أو النقل.
   - **دراسـة** المغربي (2020) أشـار إلى أن ضـعف الوعي الأمني لدى المسـتخدمين أحد أهم أسـباب تسـرب البيانات.
3. **الهجمات الخبيثة(Malicious Attacks)**
   - تشمل هجمات الفيروسات، البرمجيات الخبيثة، وهجمات الفدية.(Ransomware)
   - **دراسـة** (2013) Hashizume et al. ركزت على تحليل حوادث اختراق البيانات التي نتجت عن هذه الهجمات.
4. **استغلال واجهات برمجة التطبيقات(API Exploitation)**
   - تعتمد الحوسـبة السـحابية على APIs بشـكل كبير، وإذا لم تكن مؤمنة بشـكل جيد، يمكن اسـتغلالها للوصول إلى البيانات.
   - **دراسة** (2011) Mell & Grance أشاروا إلى ضرورة تأمين الواجهات بشكل صارم لتجنب الهجمات.
5. **فقدان البيانات(Data Loss)**
   - يمكن أن يحدث بسبب أخطاء بشرية، أعطال تقنية، أو حوادث طبيعية.
   - **دراسة** أبو الحسن وآخرون (2021) أظهروا أن غياب النسخ الاحتياطي الدوري يمثل سببًا رئيسيًا لفقدان البيانات في المؤسسات الليبية.

رابعاً: أقسام التهديدات الأمنية في الحوسبة السحابية

يمكن تقسيم التهديدات الأمنية إلى **أقسام رئيسية مرتبطة بالسرية والنزاهة والتوافر** :(CIA Triad)

1. **تهديدات تتعلق بالسرية(Confidentiality Threats)** مثل الوصول غير المصرح به وتسرب البيانات.

2. **تهديدات تتعلق بالنزاهة(Integrity Threats)** مثل تعديل البيانات أو العبث بها من قبل جهات خبيثة أو داخلية.
3. **تهديدات تتعلق بالتوافر(Availability Threats)** مثل فقدان البيانات، الهجمات التي تعطل الخدمة، أو الأعطال الفنية.

جميع هذه الأقسام تتوافق مع نتائج الدراسات السابقة، التي أكدت أن أي اختراق لأي من هذه الجوانب يؤدي إلى تدهور الثقة في الخدمات السحابية وتأثير سلبي على المؤسسات.(3)

خامساً: العلاقة بين التهديدات الأمنية والدراسات السابقة

- توضح الدراسات السابقة أن التهديدات الأمنية في الحوسبة السحابية متعددة ومتداخلة، وتغطي كل من جوانب السرية والنزاهة والتوافر.
- هناك توافق بين جميع الدراسات على أن التهديدات الأكثر شيوعًا هي: الوصول غير المصرح به، تسرب البيانات، الهجمات الخبيثة، واستغلال.APIs
- هذه الدراسات أكدت أيضًا أن التدابير الوقائية مثل التشفير، التحكم في الوصول، والمصادقة متعددة العوامل، والمراقبة الدورية تمثل الحل الأمثل للحد من هذه التهديدات.(7)

سادساً: جدول التهديدات الأمنية للبيانات السحابية

جدول(1) يوضح انواع وأقسام التهديدات الأمنية لأمن البيانات في الحوسبة السحابية

اسم التهديد الأمني	النوع	القسم (CIA)	مثال عملي	العلاقة بالدراسات السابقة
الوصول غير المصرح به (Unauthorized Access)	هجوم سيبراني/اختراق	السرية	قيام مهاجم باختراق حساب مستخدم للوصول إلى قواعد البيانات في خدمة سحابية	Subashini & Kavitha (2011) أبرزت ضعف التحكم في الوصول كنقطة ضعف أساسية
تسرب البيانات (Data Leakage)	فقدان بيانات/انتهاك الخصوصية	السرية	تسرب بيانات العملاء المالية نتيجة إرسال بيانات غير مشفرة عبر الإنترنت	المغربي (2020) أشار إلى أن ضعف الوعي الأمني لدى المستخدمين يزيد فرص تسرب البيانات
الهجمات الخبيثة (Malicious Attacks)	برامج خبيثة/فيروسات	النزاهة	هجوم فدية (Ransomware) على خوادم سحابية أدى لتشفير البيانات	Hashizume et al. (2013) ركزت على الحوادث الواقعية لانتهاك البيانات نتيجة الهجمات الخبيثة
استغلال واجهات برمجة التطبيقات (API Exploitation)	استغلال ثغرات تقنية	السرية/النزاهة	مهاجم يستخدم ثغرة في API للوصول وتعديل بيانات المستخدمين	أكدوا Mell & Grance (2011) على ضرورة تأمين واجهات API لتجنب الاختراق

اسم التهديد الأمني	النوع	القسم (CIA)	مثال عملي	العلاقة بالدراسات السابقة
(Data Loss) فقدان البيانات	أعطال تقنية/أخطاء بشرية	التوافر	حذف بيانات بالخطأ من قبل موظف أو فقدان البيانات نتيجة عطل في الخادم	أبو الحسن وآخرون (2021) أشاروا إلى غياب النسخ الاحتياطي الدوري كسبب رئيسي لفقدان البيانات
هجمات تعطيل الخدمة (DoS/DDoS)	هجمات إلكترونية	التوافر	هجوم DDoS على خوادم سحابية مما أدى لتعطل الخدمة لعدة ساعات	Hashizume et al. (2013) أظهرت أن مثل هذه الهجمات تؤثر على توافر الخدمات السحابية
(Data Tampering) التلاعب بالبيانات	هجوم داخلي أو خارجي	النزاهة	تعديل بيانات المستخدمين في قاعدة بيانات سحابية دون تصريح	الزيات (2018) أبرزت أن غياب السياسات الأمنية الصارمة يزيد من خطر العبث بالبيانات
(Weak Encryption) ضعف التشفير	نقص تقني/إعدادات غير صحيحة	السرية	اعتراض بيانات غير مشفرة أثناء النقل بين العميل والسحابة	Mell & Grance (2011) ركزوا على أهمية التشفير القوي لحماية البيانات

الحلول والتقنيات والتدابير الأمنية لحماية البيانات في الحوسبة السحابية

بعد التعرف على التهديدات الأمنية للبيانات في الحوسبة السحابية، نستعرض أهم التقنيات الأمنية، السياسات والإجراءات الوقائية، أفضل الممارسات، والاتجاهات الحديثة في تعزيز أمن البيانات السحابية، مستندًا إلى نتائج الدراسات السابقة وتجارب المؤسسات الفعلية.(8)

أولاً: التقنيات الأمنية الأساسية لحماية البيانات السحابية

1. **التشفير** :**(Encryption)** حماية البيانات أثناء النقل والتخزين(TLS/SSL ، (AES-256.
2. **التحكم في الوصول** :**(IAM)** تحديد من يصل إلى البيانات وماذا يمكنه فعله.
3. **المصادقة متعددة العوامل** :**(MFA)** زيادة أمان الحسابات.
4. **النسخ الاحتياطي والاسترداد** :استعادة البيانات عند الفقدان أو التلف.
5. **مراقبة الأنظمة وتحليل السجلات** :**(SIEM)** كشف الأنشطة المشبوهة.

ثانياً: الإجراءات والسياسات الوقائية

1. **تحديث الأنظمة والبرمجيات بشكل دوري** لمنع استغلال الثغرات.
2. **تطبيق سياسات كلمات مرور قوية** وتغييرها بشكل منتظم.
3. **تدريب الموظفين على الوعي الأمني** لتقليل الأخطاء البشرية.
4. **اختبارات اختراق دورية (Penetration Testing)** لتقييم قوة الدفاعات.
5. **الاتفاقيات مع مزودي الخدمة (SLA)** لتحديد مستوى الأمان والالتزام بالمعايير.

ثالثاً: أفضل الممارسات في حماية البيانات السحابية

- تطبيق **مبدأ الانقســـام والتجزئة (Data Segmentation & Isolation)** لتقليل تأثير الاختراق على النظام بالكامل.
- استخدام **تشفير متقدم مثل Homomorphic Encryption** لمعالجة البيانات دون فك التشفير.
- اعتماد **نموذج انعدام الثقة (Zero Trust Architecture)** للتحقق من جميع المستخدمين والأجهزة باستمرار.
- مراقبة الخدمات السحابية بشكل مستمر باستخدام **أنظمة كشف التسلل.(IDS/IPS)** (9)

رابعاً: جدول يوضح التقنيات والإجراءات الأمنية مع التهديدات المرتبطة

جدول (2) التقنيات والإجراءات الأمنية المرتبطة بالتهديدات في الحوسبة السحابية

التهديد الأمني	التقنية/الإجراء الوقائي	الهدف/التأثير	أمثلة عملية
الوصـــول غير المصرح به	المصـــادقة متعددة العوامل(MFA) ، التحكم في الوصول(IAM)	تعزيز الســرية ومنع الاختراق	اســتخدام رمز مؤقت + كلمة مرور للوصول إلى قاعدة بيانات سحابية
تسرب البيانات	التشفير أثناء النقل والتخزين	حمـاية البيـانـات من التجسس والاعتراض	تشـــفير بيـانـات العملاء قبـل نقلهـا للسحابة
الهجمات الخبيثة	IDS/IPS، تحديث الأنظمة، نســخ احتياطي	حماية النزاهة والتوافر	كشـــف هجوم فدية وإعادة اســـتعادة البيانات من النسخ الاحتياطي
استغلالAPIs	تأمين واجهاتAPI ، مراقبة الأنشطة	منـع الـوصـــول غيـر المصرح به	اســتخدام رموز API آمنة مع تحديد صلاحيات دقيقة
فقدان البيانات	النسخ الاحتياطي الدوري، استراتيجيات التعافي	ضمان التوافر	نســخ البيـانـات على خوادم متعـددة واستعادتها عند الحاجة
التلاعب بالبيانات	التشـفير ، مراقبة الأنشـطة، سـياسـات الصلاحيات	حماية النزاهة	تســـجيل كل تعديل على البيانـات وتحليل الأنشطة المشبوهة

خامساً: الاتجاهات الحديثة في أمن البيانات السحابية

1. **الذكاء الاصطناعي (AI) وتحليل التهديدات** :كشف الهجمات بشكل تلقائي وتوقعها قبل وقوعها.
2. **البلوك تشين لتعزيز النزاهة** :ضمان عدم التلاعب بالبيانات والتحقق من صحتها.
3. **نموذج انعدام الثقة :(Zero Trust)** لا يثق بأي مستخدم أو جهاز افتراضــي بشـكل افتراضــي، ويطلب التحقق المستمر.
4. **التشـفير القابل للاسـتيثاق :(Homomorphic Encryption)** معالجة البيانات المشـفرة دون فكها، مما يزيد الحماية.(10)

الاستنتاجات والتوصيات

بعد تحليل الدراسات السابقة والتهديدات الأمنية، والحلول الوقائية، توصلت الدراسة إلى النتائج والتوصيات التالية:

أولاً: الاستنتاجات

1. **تهديدات متعددة ومتنوعة:**
   - أكدت الدراسة أن البيانات في الحوسبة السحابية معرضة لعدة تهديدات أمنية، منها: الوصول غير المصرح به، تسرب البيانات، الهجمات الخبيثة، استغلالAPIs ، فقدان البيانات، التلاعب بالبيانات، وضعف التشفير، وهجمات تعطيل الخدمة.
   - هذه التهديدات تؤثر على **سرية، نزاهة، وتوافر البيانات**، مما يستدعي اتخاذ إجراءات شاملة لحماية المعلومات.
2. **أهمية الحلول المتكاملة:**
   - حماية البيانات السحابية تتطلب **دمج الحلول التقنية والإدارية** مثل التشفير، التحكم في الوصول، المصادقة متعددة العوامل، النسخ الاحتياطي، والمراقبة المستمرة للأنشطة.
   - الاعتماد على تقنية واحدة فقط لا يكفي، بل يجب أن تكون الإجراءات متكاملة.
3. **توافق النتائج مع الدراسات السابقة:**
   - نتائج هذه الدراسة تدعم ما توصلت إليه الدراسات السابقة، مثل أهمية التشفير، النسخ الاحتياطي، مراقبة الأنظمة، وتطبيق أفضل الممارسات في المؤسسات لضمان حماية البيانات.
4. **دور الوعي والتدريب:**
   - ضعف الوعي الأمني لدى المستخدمين والموظفين يمثل أحد أكبر المخاطر، لذا فإن التدريب والتثقيف الأمني جزء أساسي من حماية البيانات.

ثانياً: التوصيات

1. **تطبيق إجراءات وقائية متكاملة:**
   - على المؤسسات والشركات اعتماد **التشفير المتقدم، المصادقة متعددة العوامل، النسخ الاحتياطي الدوري، ومراقبة الأنشطة** لضمان حماية البيانات من جميع التهديدات.
2. **تبني أفضل الممارسات الحديثة:**
   - استخدام **نموذج Zero Trust** للتحقق المستمر من جميع المستخدمين والأجهزة.
   - توظيف **الذكاء الاصطناعي وأنظمة كشف التسلل** لرصد الهجمات ومنعها قبل حدوث الأضرار.
3. **وضع سياسات أمنية واضحة:**
   - تطوير **إجراءات وسياسات وطنية** لحماية البيانات في المؤسسات الحكومية والخاصة، مع تحديد مسؤوليات مزودي الخدمات السحابية.
   - الالتزام بالمعايير العالمية مثل NIST و ISO/IEC 27001لضمان مستوى أمان موحد.
4. **تعزيز الوعي والتدريب الأمني:**
   - تقديم برامج تدريبية مستمرة للموظفين والمستخدمين حول **مخاطر البيانات السحابية وكيفية التعامل معها**.
   - التركيز على **التثقيف ضد الهجمات الاجتماعية والهجمات الداخلية** التي غالبًا ما تكون سببًا رئيسيًا لتسرب البيانات.

5. **تقييم المخاطر دوريًا:**

إجراء **اختبارات اختراق دورية وتقييم المخاطر** لتحديد الثغرات الأمنية ومعالجتها قبل استغلالها من قبل المهاجمين.

References

1. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
2. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006
3. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5
4. الزيات، أ. (2018). دراسة أمن البيانات في المؤسسات الحكومية العربية. *مجلة الدراسات الأمنية العربية* , 12(2), 45–60.
5. محمد الطاهر المحروق. (2026). دور الإفصاح المحاسبي الإلكتروني في تحسين جودة المعلومات المحاسبية دراسة ميدانية على المصارف التجارية العاملة بمدينة الزاوية. *Al-Farooq Journal of Sciences*, *2*(1), 1373-1398.
6. المغربي، م. (2020). تحليل أثر التشفير والتحكم في الوصول على حماية البيانات في الحوسبة السحابية. *مجلة تكنولوجيا المعلومات والأمن السيبراني*. 8(1), 22–35 ,
7. أبو الحسن، ع.، وآخرون. (2021). تقييم أمن البيانات في المؤسسات الليبية: دراسة حالة للجهات الحكومية. *مجلة علوم الحاسوب والمعلوماتية*. 9(3), 50–68 ,
8. الجندلي ، متطلبات تطبيق الحوسبة السحابية في التعليم المحاسبي في ليبيا: دراسة على أعضاء هيئة التدريس بقسم المحاسبة بجامعتي صبراتة والزاوية. (2026). *مجلة الفاروق للعلوم*, 2(3), 236-330. https://doi.org/10.65405/
9. Cloud Security Alliance (CSA). (2020). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/research/security-guidance/
10. Mell, P., & Grance, T. (2011). *Security and Privacy in Cloud Computing: A Survey*. NIST Technical Report.
11. Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication 800-144*.
12. Alnnale, T. (2026). Predictive Governance in Digital Enterprises: An LSTM-Enhanced Deep Learning Framework for Economic Optimization of IT Incident Management Using Enriched Process Logs. *Al-Farooq Journal of Sciences*, *2*(3), 86-113.
13. AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). Cloud Computing Security: From Single to Multi-Clouds. *2012 45th Hawaii International Conference on System Sciences*, 5490–5499. https://doi.org/10.1109/HICSS.2012.417