Journal of Libyan Academy Bani Walid 2026
مجلة الأكاديمية الليبية بني وليد
e-ISSN: 3104-3860
Volume 2, Issue 1, 2026, Pages: 301-320
Website: https://journals.labjournal.ly/index.php/Jlabw/index

Identifying the Factors Influencing Improvement of Data Security in Cloud Networks" Case Study: Arabian Gulf Oil Company in Benghazi

Salwa Mohamed Ibrahim Albaraghthi [1*], Mohamed Mustafa Salem Bushaala [2] , AND Abdallah Shoaib Abdallah Alhssi [3]
[1] Department of Information system University of Benghazi - Faculty of Information Technology, Libya
[2] Department of Software development Higher Institute of Engineering Technologies – Benghazi, Libya
[3] Faculty Member at the Higher Institute of Science and Technology - Tokra, Libya.
*Email: Salwa.mohamed@uop.edu.ly

تحديد العوامل المؤثرة على تحسين أمن البيانات في الشبكات السحابية دراسة حالة : شركة الخليج العربي للنفط في بنغازي

سلوى محمد إبراهيم البرغثي [1*]، محمد مصطفى سالم[2] ، عبد الله شعيب عبد الله
[1] قسم نظم المعلومات، كلية تقنية المعلومات، جامعة بنغازي، ليبيا.
[2] قسم تطوير البرمجيات، المعهد العالي للتقنيات الهندسية - بنغازي، ليبيا.
[3] عضو هيئة تدريس في المعهد العالي للعلوم والتقنية - توكره، ليبيا.

Received: 02-12-2025	**Accepted:** 11-01-2026	**Published:** 05-02-2026

Abstract

This research aims to identify the factors influencing the improvement of data security in cloud networks, with a practical application on the Arabian Gulf Oil Company (AGOCO) in Benghazi. The study adopted the OCTAVE-S methodology for risk analysis and used a questionnaire as a tool for data collection from a sample of 81 employees.

The research focused on several key areas: protection of sensitive data, encryption and security technologies, identity and access management, data governance, risk management, and regulatory compliance.The results showed that data protection is a top priority within the company (96.6%), with clear policies for data classification in place, though they require regular updates. Encryption protocols were found to be 82.1% effective, but not sufficiently updated. Participants confirmed the effectiveness of access management (88.8%), while the implementation of multi-factor authentication was found to be limited.

In terms of data governance, employee adherence to policies was moderate (78%). As for regulatory compliance, it reached 83.1%, though there is still a need to fully align with international standards such as ISO 27001 and GDPR.

The study concluded that the company has a good institutional awareness of cybersecurity; however, there are gaps in areas such as updating policies, strengthening encryption protocols, expanding the use of multi-factor authentication, and achieving full compliance with international standards.Based on these findings, the study recommended the development of flexible risk response plans, the adoption of modern security technologies, and stricter enforcement of governance and compliance, all of which contribute to building a secure and reliable cloud environment.

Keywords: Information Security, Cloud Network, Encryption, Data Governance, Regulatory Compliance.

الملخص

يهدف هذا البحث إلى تحديد العوامل المؤثرة على تحسين أمن البيانات في الشبكات السحابية، مع تطبيق عملي على شركة الخليج العربي للنفط في بنغازي. اعتمدت الدراسة على منهجية OCTAVE-S لتحليل المخاطر، واستخدمت الاستبيان كأداة لجمع البيانات من عينة مكونة من (81) موظفًا. ركزت محاور البحث على حماية البيانات الحساسة، التشفير وتقنيات الأمان، إدارة الهوية ومراقبة الوصول، حوكمة البيانات، إدارة المخاطر، والامتثال التنظيمي.

أظهرت النتائج أن حماية البيانات تحظى بأولوية قصوى داخل الشركة (96.6%)، مع وجود سياسات واضحة لتصنيف البيانات، إلا أنها تحتاج إلى تحديث دوري. كما تبين أن بروتوكولات التشفير فعالة بنسبة (82.1%) لكنها غير محدثة بالشكل الكافي. وأكد المشاركون على فعالية إدارة الصلاحيات (88.8%)، بينما كان تطبيق المصادقة متعددة العوامل محدودًا. في جانب الحوكمة، التزم الموظفون بالسياسات بدرجة متوسطة (78%%)، أما الامتثال التنظيمي فحقق نسبة (83.1%) مع الحاجة إلى استكمال التوافق مع المعايير الدولية.(ISO 27001, GDPR)

خلصت الدراسة إلى أن الشركة تمتلك وعيًا مؤسسيًا جيدًا بالأمن السيبراني، غير أن هناك فجوات في مجالات تحديث السياسات، تعزيز بروتوكولات التشفير، تطبيق المصادقة متعددة العوامل، وتحقيق الامتثال الكامل للمعايير الدولية. وبناءً على ذلك، أوصت الدراسة بضرورة تطوير خطط استجابة مرنة لإدارة المخاطر، وتبني تقنيات أمان حديثة، وتفعيل الحوكمة والامتثال بشكل أكثر صرامة، بما يسهم في بناء بيئة سحابية آمنة وموثوقة.

الكلمات المفتاحية: امن المعلومات، الشبكات السحابية، التشفير، حوكمة البيانات، الامتثال التنظيمي.

المقدمة

يشهد العالم تحولاً متسارعًا نحو الرقمية، مما أدى إلى الاعتماد المتزايد على الحوسبة السحابية في مختلف القطاعات. توفر السحابة مزايا عديدة مثل خفض التكاليف، تحسين الكفاءة التشغيلية، وتعزيز الوصول إلى البيانات والتطبيقات في أي وقت ومن أي مكان. وتُعد الحوسبة السحابية نموذجًا يوفر موارد حوسبية قابلة للتكوين عند الطلب دون الحاجة إلى إدارة مباشرة للبنية التحتية، مما يتيح تقديم خدمات مثل البرمجيات كخدمة (SaaS) والمنصة كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) [3],[2],[1].

مع هذا التوسع، أصبحت أمن البيانات، الخصوصية، والامتثال التنظيمي تحديات رئيسية أمام المؤسسات. تلعب الشبكات السحابية دورًا جوهريًا في دعم بنية الحوسبة السحابية، من خلال توفير وظائف مثل التوجيه وتأمين الاتصال باستخدام تقنيات مثل الشبكات المعرفة بالبرمجيات (SDN) والشبكات الخاصة الافتراضية (VPCs)، مما يسهم في تحسين الأداء وتعزيز الأمان داخل البيئة السحابية [4].

في هذا الإطار، يهدف مشروع "حوكمة البيانات السحابية" إلى تحديد العوامل المؤثرة في تعزيز أمن البيانات والتحكم في الوصول داخل بيئة الحوسبة السحابية، مع تطبيق عملي على شركة الخليج العربي

للنفط –إحدى الشركات الوطنية الرائدة في ليبيا، والتي تبنت مؤخرًا بنية تحتية رقمية حديثة تشمل مركز بيانات متطور.
يركز البحث على دراسة آليات مثل إدارة الهوية والصلاحيات، التشفير، الجدران النارية الافتراضية، وتقنيات الامتثال، بهدف تقديم توصيات تسهم في بناء بيئة سحابية آمنة وموثوقة تدعم استدامة الأعمال الرقمية في المؤسسات.

مشكلة الدراسة:

تتعرض البيانات الحساسة لمخاطر الاختراقات أو الفقدان أو الهجمات الخبيثة نتيجة للتحديات المتزايدة التي تواجه حوكمة البيانات في الحوسبة السحابية. رغم وجود أساليب مثل التحكم في الوصول والتشفير لحماية البيانات الحساسة، إلا أنها قد لا تكون قوية بما يكفي لمواجهة التهديدات المتنوعة والمتطورة باستمرار. كما تواجه المنظمات صعوبات في مراقبة بياناتها وتنظيمها، مما يعقد الامتثال للقوانين ويعرض الخصوصية للخطر. وبالتالي، من الضروري تحديد الأساليب المناسبة لحماية البيانات في بيئة الحوسبة السحابية في كل مرحلة، بدءاً من التخزين إلى النقل[6],[7].

اهمية الدراسة:

تكمن أهمية الدراسة هو تحديد العوامل التي تساعد في تقييم فعالية تكنولوجيا إدارة الهوية في تعزيز أمن شبكات السحابة. من خلال تكنولوجيا إدارة الهوية، يمكن تقييد وصول المستخدمين إلى الخدمات السحابية المختلفة وإدارة هوياتهم والتحقق منها. يهدف هذا التقييم إلى دراسة فعالية هذه التقنية في حماية الشبكات السحابية من الهجمات السيبرانية وضمان أن الموارد متاحة فقط للمستخدمين المصرح لهم[8]. بناءً على ذلك، تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف الفرعية التي تهدف الى تحقيق الهدف الأساسي.

اهداف الدراسة:

تحليل الوضع الحالي لأمن البيانات في بيئة الشبكات السحابية المستخدمة داخل شركة الخليج العربي للنفط.
بهدف فهم الممارسات الحالية ونقاط الضعف المحتملة.
تحديد أبرز التهديدات والمخاطر الأمنية التي تواجه بيانات الشركة المخزنة في الشبكة السحابية.مثل: الهجمات السيبرانية، فقدان البيانات، الوصول غير المصرح به، إلخ.
تحديد العوامل التقنية والتنظيمية المؤثرة على تعزيز أمن البيانات السحابية.مثل: التشفير، إدارة الهوية والصلاحيات، السياسات الأمنية، التدريب، وغيرها.
قياس وعي الموظفين والمستخدمين داخل الشركة بأهمية أمن البيانات في بيئة الحوسبة السحابية.
من خلال استبيانات أو مقابلات لمعرفة مستوى الفهم والتفاعل مع الإجراءات الأمنية.
تقييم فعالية السياسات والإجراءات الأمنية المتبعة حالياً في الشركة.ومقارنتها بالممارسات الموصى بها عالمياً في مجال أمن السحابة.

حدود الدراسة:

الحدود الموضوعية : تتمثل الحدود الموضوعية لهذه الدراسة في التركيز على أمن البيانات داخل بيئة الشبكات السحابية، حيث تسعى الدراسة إلى تحديد وتحليل العوامل (التقنية، التنظيمية، والبشرية) التي تؤثر على مستوى الأمان في استخدام الحوسبة السحابية، دون التوسع في بقية الجوانب المتعلقة بتقنيات الحوسبة السحابية مثل الأداء أو الكفاءة التشغيلية أو التكلفة.

الحدود المكانية : شركة الخليج العربي للنفط الكائنة في مدينة بنغازي – ليبيا، وتُعتمد هذه الشركة كدراسة حالة بهدف فحص مدى تطبيق معايير أمن البيانات في بيئة العمل السحابية الخاصة بها، دون تعميم النتائج على جميع الشركات النفطية أو المؤسسات الأخرى.
الحدود الزمانية :تغطي الدراسة الفترة الزمنية من يناير 2025 إلى يونيو 2025، وهي الفترة التي تم خلالها جمع البيانات وتحليلها وتفسير النتائج. كما أن الدراسة تستند إلى الوضع الراهن لأمن البيانات وتقنيات الحوسبة السحابية خلال هذه المدة، وبالتالي فإن أي تطورات لاحقة في المجال قد تكون خارج نطاق الدراسة.

الإطار النظري للدراسة

أولًا :مفهوم الحوسبة السحابية : الحوسبة السحابية (Cloud Computing) تُعد من أبرز التحولات التقنية التي غيرت طريقة تقديم الخدمات الرقمية. وهي تعني توفير موارد الحوسبة (مثل الخوادم، التخزين، قواعد البيانات، الشبكات، البرمجيات) عبر الإنترنت ("السحابة") بشكل عند الطلب، دون الحاجة إلى امتلاك بنية تحتية مادية.

خصائص الحوسبة السحابية:

1. الوصول عند الطلب.
2. قابلية التوسع.
3. المرونة.
4. مشاركة الموارد.
5. الدفع حسب الاستخدام.

ثانيًا :أمن البيانات في بيئة الحوسبة السحابية : يُعد أمن البيانات أحد أهم التحديات في تبني الحوسبة السحابية، نظرًا لاعتماد المؤسسات على مزودي الخدمة في إدارة وتخزين ومعالجة البيانات.

مجالات أمن البيانات السحابية:

1. الخصوصية :حماية البيانات من الوصول غير المصرح به.
2. السلامة :(Integrity) ضمان عدم تعديل البيانات أو تلفها.
3. التوافر :(Availability) ضمان الوصول إلى البيانات في الوقت المناسب.
4. إدارة الهوية والتحكم في الوصول.
5. التشفير :أثناء النقل والتخزين.
6. النسخ الاحتياطي واسترجاع البيانات.

ثالثًا :العوامل المؤثرة على أمن البيانات في السحابة

العوامل التقنية:

1. قوة أنظمة التشفير.
2. بروتوكولات الأمان.
3. نظام المراقبة والكشف عن التهديدات.
4. مستوى حماية مراكز البيانات.

العوامل الإدارية والتنظيمية:

السياسات الأمنية المعتمدة داخل الشركة.
التوافق مع المعايير الدولية (ISO/IEC 27001 ،NIST).
وضوح العقود مع مزودي الخدمة (SLA – اتفاقية مستوى الخدمة).

العوامل البشرية:

1. وعي الموظفين بالمخاطر الأمنية.

2. التدريب المستمر على الأمن السيبراني.
3. ثقافة الأمان داخل المؤسسة.

رابعًا :التحديات الأمنية في البيئة السحابية

تشمل أبرز التحديات ما يلي:

فقدان السيطرة على البيانات.

.(الاعتماد على طرف خارجي (مزود الخدمة

- الاختراق الداخليDDoS هجمات:احتمالية تعرض البيانات لهجمات إلكترونية مثل

الدراسات السابقة:

1- دراسة أجراها-Ahmed Al-Buqami, Robert Walters, Gary Wells, Madini O. Al "Assafi"(2016) تناقش مقالة الدراسة أمن بيانات الحوسبة السحابية مع التركيز على طرق التشفير والمخاطر والعلاجات. وتلفت الانتباه إلى سوء الإدارة ، والهجمات الخبيثة. تستخدم التخزين السحابي ونقل البيانات تقنيات التشفير مثل وظائف التجزئة، وشفرات الكتلة، وشفرات التدفق. لضمان سلامة البيانات وخصوصيتها وسلامتها، من الأهمية بمكان حل المخاوف الأمنية في الحوسبة السحابية. ومع ذلك، هناك أيضًا مخاوف مرتبطة بقضايا مثل خروقات الواجهة الإدارية، والحذف الجزئي للبيانات، واعتراض البيانات. يتم التأكيد على أهمية طرق التشفير لأمن البيانات في كل من السحابة العامة والخاصة في ورقة البحث[6].

2- في دراسة أجريت في Kurokshtra بالهند عام 2021، أكد (Reshabh Gupta) و Deepika (Saxena)على أهمية أمن البيانات والخصوصية في الحوسبة السحابية. تمت حماية خصوصية البيانات الحساسة من خلال مجموعة متنوعة من التقنيات، بما في ذلك التعلم الآلي والتشفير المتماثل والخصوصية التفاضلية. كما أكدت الدراسة على أهمية الحوسبة الضبابية كامتداد للحوسبة السحابية، مؤكدة على ضرورة رفع معايير الأمان وخفض الأسعار وزيادة كفاءة المعالجة وتقليل فقد البيانات أثناء النقل[10].

3- اما هذه الدراسة فتناولت التهديدات المتعلقة بالخصوصية والأمن في الحوسبة السحابية، ونشرتها كلية المعلومات الإلكترونية والهندسة الكهربائية بجامعة Shanghai Bao Tong in Shanghai بالصين في عام 2019. وتقارن الدراسة بين صعوبات الثقة والسمعة، وتفحص العديد من تقنيات التشفير، وتقترح نموذجًا لحماية الخصوصية. كما تؤكد على مدى أهمية الجمع بين تقنيات السمعة والثقة والتشفير والتحكم في الوصول من أجل تحسين حماية الخصوصية. كما تسلط الضوء على قيود أنظمة حماية الخصوصية الحالية، مثل عدم قدرتها على التوسع وتوفير الحماية الديناميكية، وتسلط الضوء على المراحل المبكرة من أبحاث حماية خصوصية السحابة. وتؤكد المقالة على ضرورة معالجة القضايا بما في ذلك نقل البيانات الآمن، وتخزين البيانات بكفاءة، وآليات التحكم في الوصول الوظيفية، وأمن البيانات في أنظمة السحابة[11].

4- في مناقشته لأمن بيانات الحوسبة السحابية، يركز kufi Emmanuel Jones (2023) على المخاطر والتدابير المضادة وطرق التشفير. ويلفت الانتباه إلى مخاطر التعايش، وسوء الإدارة، والحدود، والعزلة المكسورة، والهجمات الخبيثة. تستخدم التخزين السحابي ونقل البيانات تقنيات التشفير مثل وظائف التجزئة، وشفرات الكتلة، وشفرات التدفق. لضمان سلامة البيانات وخصوصيتها وسلامتها، من الأهمية بمكان حل المخاوف الأمنية في الحوسبة السحابية. ومع ذلك، هناك أيضًا مخاوف مرتبطة بقضايا مثل خروقات الواجهة الإدارية، والحذف الجزئي للبيانات، واعتراض البيانات. يتم التأكيد على أهمية طرق التشفير لأمن البيانات في كل من السحابات الخاصة والعامة في المقال[12].

5- قام Abinit Anand، Naresh Kumar Trivedi ، Ajay Kumar بدراسة مشاكل أمن البيانات والحلول في الحوسبة السحابية في عام 2020 في جامعة Chitkara. كانت التوصية الرئيسية للدراسة هي

بنية أمان لبيانات السحابة تستخدم أساليب تعزيز الأمان مثل تشفير البيانات والتجزئة وإخفاء المعلومات ودمجها. من أجل حماية تخزين البيانات والوصول إليها، تستخدم هذه البنية تجزئة كلمة المرور المملحة والتشفير غير المتماثل وتصنيف البيانات على أساس الأهمية. يؤكد التقرير على الحاجة إلى استخدام تدابير التشفير لتأمين بيانات السحابة وضرورة الصيانة والمراقبة المستمرة لوقف خروقات البيانات أو فقدانها. هناك حاجة لمزيد من التحقيق والتحليل في هذا المجال لأن الدراسة لا تعالج أي نقاط ضعف أو ثغرات محتملة في إطار الأمان المقترح[1].

6- تمت مناقشة وتحليل قضايا أمن الحوسبة السحابية من وجهات نظر مختلفة، مثل البنية والخصائص وأصحاب المصلحة ونماذج تقديم الخدمة، في دراسة بعنوان "تحليل قضايا أمن الحوسبة السحابية" في 2016 أجراها " Ingo Mueller ، John Grande ،Mohamed Al Mursi " في جامعة Swinburne للتكنولوجيا، التي تقع في مدينة (Hawthorn)في ولاية فيكتوريا، أستراليا . وهي تتعرف على المشاكل والصعوبات وتتعامل معها جميعًا بالتفصيل. ومن أجل مساعدة مديري الأمن والباحثين في تحمل مسؤولياتهم الحالية والمساعدة في توفير خدمات سحابية آمنة، تسلط الدراسة الضوء أيضًا على أهمية وجود وعي منهجي بالتحديات الأمنية. كما تؤكد على ضرورة أنظمة إدارة أمن السحابة والأداء القوي والأمن التكيفي[13].

7. ورقة محمد داود وآخرون من عام 2023" تدرس هذه المقالة مخاطر وثغرات أمن الحوسبة السحابية في سيناريوهات النشر المختلفة. وتدرس قضايا مثل الخصوصية وانتهاكات البيانات وتوصي بحلول أمنية مثل المصادقة متعددة العوامل والتشفير. كما تناقش اتجاهات البحث القادمة مثل تعزيز خصوصية البيانات وتحسين فعالية تعدد المستأجرين. قد لا تحتوي على نتائج بحثية جديدة أو بيانات تجريبية، وقد تفتقر إلى ميزات تنفيذ تقنية محددة لحلول الأمان في أنظمة السحابة في العالم الحقيقي[2].

8. دراسة "Ronak Ravjibhai Pansara، 2023، " في عالم اليوم الذي تحركه البيانات، تؤكد هذه الدراسة على أهمية إدارة بيانات السحابة. وتتناول القيود مثل تأخيرات نقل البيانات، والعيوب الأمنية، والصعوبات في الالتزام باللوائح. ومن الاعتبارات المهمة فعالية الحلول السحابية من حيث التكلفة وقابليتها للتوسع بالإضافة إلى قدرتها على تحسين عملية اتخاذ القرار وتحليل البيانات. وللحصول على رؤى مفيدة، تتناول المقالة أيضًا دراسات الحالة من العالم الفعلي. لا يوجد تحقيق شامل للتقنيات المتطورة مثل الحوسبة المتطورة وتكامل إنترنت الأشياء مع إدارة البيانات السحابية[14].

9. ورقة Akash Shotrani، 2023: تم تسليط الضوء على وظيفة حوكمة المعلومات في شركة السحابة التابعة الجديدة لشركة أوراكل في هذه الدراسة. وهي تعرض قواعد البيانات العلائقية وتحسين الاستعلام بين ميزات قاعدة بيانات أوراكل لإدارة البيانات. كما تم تسليط الضوء على ابتكارات أوراكل الأمنية - مثل ميزات التدقيق والتشفير والمصادقة. كما تستعرض كيف تعمل التشفير وضوابط الوصول وتصنيف البيانات معًا لتحسين أمان بيانات السحابة من خلال حوكمة المعلومات. إنها خالية من التحليل الشامل الذي يقارن بين بنية Oracle Cloud وبنية مقدمي الخدمات البارزين الآخرين، مثل AWS وAzure، والذي قد يقدم أدلة مهمة حول المكانة التنافسية لشركة أوراكل[15].

10. ورقةEpiye Epiye، Jonathan et al، 2023 : تم تقديم تحليل شامل لاستراتيجيات الحوكمة والمخاطر والامتثال (GRC) في البنى التحتية السحابية المعاصرة في هذه الورقة. وتسلط الضوء على الصعوبات التي تواجهها المنظمات في ضمان الامتثال التنظيمي وحماية البيانات. يعد تقييم المخاطر القوي وحلول الحوكمة والمخاطر والامتثال السحابية الأصلية واستخدام الذكاء الاصطناعي والتعلم الآلي للكشف عن التهديدات وأتمتة الامتثال من الاعتبارات المهمة. كما تتناول المقالة تقنية blockchain للتدقيق على الامتثال والتعريف وإدارة الوصول. تزداد تعقيدات الامتثال القانوني والتنظيمي بسبب غياب الفحص الدقيق للصعوبات المرتبطة بالمعايير الدولية في إعدادات السحابة المتعددة[7].

11. ورقة عام 2019 بقلم لبنى الحناكي وآخرون. تدرس هذه الدراسة المخاطر الأمنية والاعتداءات، بما في ذلك الاستيلاء على الحساب وهجمات الحرمان من الخدمة وحقن SQL وفقدان البيانات وانتهاكات البيانات، في إعدادات الحوسبة السحابية. وتغطي عددًا من العيوب الأمنية، مثل واجهات برمجة التطبيقات المعقدة ونظام مراقبة الموظفين غير المبهج والمشكلات المتعلقة بثقة مقدم الخدمة. كما يتم تغطية نقاط الضعف في التكنولوجيا المشتركة وإدارة الهوية الرقمية. قد لا تقدم حلول أمان شاملة للبيئات ذات المستأجرين المتعددين[16].

12. ورقة Sandeep Bodaniوزملائه، 2021: تسلط هذه المقالة الضوء على مخاطر مثل التهديدات الفيروسية، والوصول غير المصرح به، وضعف رؤية البيانات وإدارتها. كما تدرس تحديات أمن البيانات في الحوسبة السحابية عبر مستويات SaaS وPaaS وIaaS. وتلفت الانتباه إلى أوجه قصور أخرى مثل عدم كفاية مراقبة البيانات أثناء النقل وغياب الأطر اللازمة للامتثال التنظيمي. وتؤكد التوصيات على الحاجة إلى تحسين التعاون بين مقدمي الخدمات والمستخدمين وتقترح استخدام جدران الحماية وشبكات VPN والتشفير للأمان.

لا تزال الحوسبة السحابية ميسورة التكلفة وقابلة للتطوير على الرغم من العقبات، ولكن هناك حاجة إلى المزيد من الأمان[17].

13. دراسة أجراها Rajesh Kumar، Tiwari and Sonita Swain، 2020: تصنف هذه المقالة وتفحص مخاوف أمن الحوسبة السحابية، وتقدم نظرة عامة شاملة على المخاطر المتعلقة بالشبكات، والافتراضية، وتخزين البيانات، والتحكم في الوصول. وتجد ثغرات مهمة، مثل عدم كفاية التحكم في وضع البيانات، ومخاطر الافتراضية، ومشاكل أمن الشبكة. وتجد الورقة أن أنظمة الحوسبة السحابية تتطلب نهجًا أمنيًا متكاملًا[18].

14. ورقة Xiao Tong Sun، 2018: تتناول هذه المقالة جوانب أمن الكمبيوتر والشبكات والمعلومات مع التركيز على التحديات الأمنية في الحوسبة السحابية. وتلفت الانتباه إلى المخاطر الداخلية والخارجية، بما في ذلك فقدان البيانات والواجهات غير الآمنة وإساءة استخدام البيانات. وباستعراض العديد من متجهات الهجوم وبروتوكولات التحكم في الوصول وتقنيات التشفير، تشير إلى أن التشفير المتماثل بالكامل (FHE) يحمل وعدًا ولكنه غير قابل للتطبيق بعد. كما تسلط الضوء على غياب الإجابات الشاملة للمشاكل المتعلقة بإدارة الهوية وحماية الخصوصية التي تنشأ عن التهديدات الداخلية والخارجية[19].

15. ورقة Alia Jk Oda وآخرون، 2023: تتناول هذه الدراسة مخاطر وثغرات أمن الحوسبة السحابية مع التركيز بشكل خاص على الشبكات والتخزين والافتراضية. وتدرس المخاوف الأمنية في سياق نماذج (IaaS) و(PaaS) و(SaaS) وتؤكد على العلاقة بين الثغرات والتهديدات. بالإضافة إلى الإشارة إلى قضايا مثل تعدد المستأجرين في (SaaS)، وتعقيد المحاكاة الافتراضية، وغياب التحقق من خلفيات العملاء، تشير الدراسة إلى أن حلول الأمان النموذجية قد لا تكون مناسبة في أنظمة السحابة. بالإضافة إلى ذلك، تلاحظ الدراسة أن بعض الأبحاث تفشل في التمييز بين التهديدات والثغرات الأمنية[20].

أدوات جمع البيانات

الاستبيان هو الأداة المستخدمة لجمع البيانات من المشاركين في الدراسة. تم تصميم الاستبيان ليتضمن مجموعة من الأسئلة التي تهدف إلى فهم كيفية تعامل الشركة مع التهديدات الأمنية ونقاط الضعف في بيئتها السحابية. سيتم توجيه الاستبيان لموظفي شركة الخليج للنفط، مع التركيز على الأقسام التي تتعامل مع إدارة البيانات والأمن.

منهج الدراسة :

باستخدام منهجية OCTAVE-S، سيتم استخدام المنهج الوصفي في هذه الدراسة لتقديم تحليل شامل للمشاكل الأمنية المتعلقة بالبيانات في الشبكات السحابية. تم اختيار هذه المنهجية بسبب فعاليتها في التعرف على التهديدات، تقييم الثغرات، ووضع خطط لتقليل المخاطر. توفر OCTAVE-S تحليلًا شاملًا للأصول والتهديدات مما يساعد المؤسسات على تحسين وضعها الأمني. سيتم استخدام استبيان لجمع المعلومات من المشاركين في شركة الخليج للنفط في بنغازي. باستخدام هذه المعلومات، يمكن وضع خطط لإدارة المخاطر التي تعالج بشكل فعال التهديدات، الثغرات، والأصول الهامة.

عينة الدراسة

تكونت عينة الدراسة من 81 موظفًا من العاملين في شركة الخليج للنفط بمدينة بنغازي. تم اختيار المشاركين بشكل مقصود نظرًا لامتلاكهم الخبرة والمعرفة المتعلقة بإدارة الأصول الأمنية في الشركة. تم تحديد حجم العينة بناءً على القدرة على الوصول إلى الموظفين المعنيين والمتاحين للمشاركة في الاستبيان.

إجراءات جمع البيانات

سيتم توزيع الاستبيانات ورقيًا على المشاركين لضمان جمع البيانات بشكل مباشر. سيتم تحديد فترة زمنية محددة لاستلام الاستبيانات المكتملة، وبعد ذلك ستبدأ عملية التحليل.

طرق تحليل البيانات

بعد جمع البيانات، سيتم استخدام أساليب التحليل الوصفي لفهم النتائج، وذلك باستخدام برنامج SPSS . سيتم تحليل الإجابات بشكل منهجي لتحديد التهديدات الأمنية ونقاط الضعف المرتبطة بالأصول الحيوية للشركة. سيتم عرض النتائج في شكل جداول لتسهيل التفسير.

أدوات الدراسة

تناولت هذه الدراسة البحثية موضوع حماية البيانات الحساسة في المؤسسات، مع التركيز على تقييمات الأمان، إدارة الهوية، مراقبة الوصول، حوكمة البيانات، بيئة السحابة، المخاطر المحتملة، والامتثال التنظيمي.

لنتائج التالية تبين النتائج الإحصائية المتعلقة بآراء عينة من الموظفين من شركة الخليج حول المحاور المحددة في هذه الدراسة.

النتائج والمناقشة

المحور الأول : البيانات الحساسة

الجدول (1): الإحصاء الوصفي لعينة الدراسة – المحور الأول

رقم الفقرة	العبارة	الأهمية النسبية	الانحراف المعياري	المتوسط الحسابي	موافق بشدة	موافق	محايد	غير موافق
1	حماية البيانات الحساسة في مؤسستكم أمر بالغ الأهمية.	96.6%	0.519	4.83	71 (87.7%)	7 (8.6%)	2 (2.5%)	1 (1.2%)
2	تصنيف البيانات بناءً على مستوى حساسيتها يتم بشكل جيد في مؤسستكم.	86.2%	0.736	4.31	36 (44.4%)	36 (44.4%)	7 (8.6%)	2 (2.5%)

3	تطبق مؤسستكم سياسات صارمة لحماية البيانات الحساسة.	86.6%	0.775	4.33	41 (50.6%)	27 (33.3%)	12 (14.8%)	1 (1.2%)
4	يتم تحديث سياسات حماية البيانات بانتظام لمواكبة التهديدات الأمنية.	84.0%	0.781	4.20	33 (40.7%)	32 (39.5%)	15 (18.5%)	1 (1.2%)
5	تعد إجراءات مسح البيانات الحساسة من الأجهزة غير المصرح بها جزءاً من سياسات الأمان في مؤسستكم.	82.0%	0.831	4.10	30 (37.0%)	31 (38.3%)	18 (22.2%)	2 (2.5%)

تحليل النتائج

يوضح جدول رقم (1) أهمية حماية البيانات الحساسة، حيث أظهر 96.6% من المشاركين أن حماية البيانات أمر بالغ الأهمية. هذا يشير إلى وعي عالٍ بأهمية الأمان المعلوماتي في المؤسسات. ومع ذلك، هناك تباين في الآراء حول فعالية تصنيف البيانات وتطبيق السياسات، مما يشير إلى الحاجة لتحسين الإجراءات الحالية، وحيث كانت بالترتيب الفقرة تطبق مؤسستكم سياسات صارمة لحماية البيانات الحساسة بأهمية النسبية 86.6% ، ثم تليها الفقرة تصنيف البيانات بناءً على مستوى حساسيتها يتم بشكل جيد في مؤسستكم بأهمية النسبية 86.2%، ثم تليها الفقرة يتم تحديث سياسات حماية البيانات بانتظام لمواكبة التهديدات الأمنية بأهمية النسبية 84%، واخير الفقرة تعد إجراءات مسح البيانات الحساسة من الأجهزة غير المصرح بها جزءاً من سياسات الأمان في مؤسستكم.

جدول (2): اختبار t حول الوسط النظري (3) حسب المحور الأول

المحور الأول	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية
البيانات الحساسة	81	4.35	0.543	22.411	0.000

يظهر اختبار t (جدول 2) أن المتوسط الحسابي للبيانات الحساسة هو 4.35، مما يدل على أن العينة تميل إلى الاعتقاد بأن حماية البيانات أمر مهم. القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية.

المحور الثاني: تقييمات الأمان

جدول (3) :الإحصاء الوصفي لعينة الدراسة -المحور الثاني (تقييميات الأمان)

م	تقييميات الأمان		غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية
1	بروتوكولات التشفير المستخدمة في مؤسستكم فعالة في حماية البيانات.	العدد	4	18	31	28	4.02	0.88	80.4 %
		النسبة	4.9	22.2	38.3	34.6			
2	يتم تطبيق التشفيرعلى البيانات أثناء النقل والتخزين في مؤسستكم.	العدد	3	21	28	29	4.02	0.88	80.4 %
		النسبة	3.7	25.9	34.6	35.8			
3	تستخدم مؤسستكم أحدث تقنيات التشفير لتأمين البيانات الحساسة.	العدد	1	26	27	27	3.99	0.844	79.8 %
		النسبة	1.2	32.1	33.3	33.3			
4	تتم مراجعة إجراءات التشفير وتحديثها بانتظام في مؤسستكم.	العدد	4	23	26	28	3.96	0.914	79.2 %
		النسبة	4.9	28.4	32.1	34.6			
5	يوجد نظام للكشف عن التشفير الغير مصرح به لحماية البيانات من الوصول غير المشروع.	العدد	10	18	25	28	3.88	1.029	77.6 %
		النسبة	12.3	22.2	30.9	34.6			

يعكس جدول رقم (3) آراء المشاركين حول فعالية بروتوكولات التشفير. على الرغم من أن 80.4% يعتقدون أن بروتوكولات التشفير فعالة، إلا أن هناك حاجة لمزيد من التحسينات في تطبيق التشفير أثناء النقل والتخزين، ثم كانت على الترتيب الفقرة تستخدم مؤسستكم أحدث تقنيات التشفير لتأمين البيانات الحساسة بأهمية النسبية 79.8%، ثم تليها الفقرة تتم مراجعة إجراءات التشفير وتحديثها بانتظام في مؤسستكم. بأهمية النسبية 79.2%، واخير الفقرة يوجد نظام للكشف عن التشفير الغير مصرح به لحماية البيانات من الوصول غير المشروع. بأهمية النسبية 77.6%.

جدول(4) الإحصاء الوصفي لعينة الدراسة – المحور الثاني (إدارة الهوية)

م	إدارة الهوية		غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية
1	تقنيات إدارة الهوية في مؤسستكم تعزز أمان الشبكة السحابية بشكل فعال.	العدد	4	18	31	28	4.02	0.88	80.4%
		النسبة	4.9	22.2	38.3	34.6			
2	نظام المصادقة متعددة العوامل MFA مطبق بشكل صارم في مؤسستكم.	العدد	3	24	37	17	3.84	0.798	76.8%
		النسبة	3.7	29.6	45.7	21			
3	يوجد سياسة لإدارة صلاحيات الوصول الى البيانات في مؤسستكم.	العدد	2	5	29	45	4.44	0.725	88.8%
		النسبة	2.5	6.2	35.8	55.6			
4		العدد	1	7	36	37	4.35	0.692	87.0%

	يتم تطبيق الضوابط الأمنية للمصادقة في مؤسستكم لضمان حماية البيانات.	النسبة	1.2	8.6	44.4	45.7			
5	تتم مراجعة سجلات دخول المستخدمين بانتظام كجزء من سياسة الأمان.	العدد	1	13	31	36	4.26	0.771	85.2%
		النسبة	1.2	16	38.3	44.4			

يظهر جدول رقم (4) أن 88.8% من المشاركين يعتقدون أن يوجد سياسة لإدارة صلاحيات الوصول الى البيانات في مؤسستكم مما يعزز إدارة الهوية من حيث تقييمات الأمان ثم كانت الفقرة يتم تطبيق الضوابط الأمنية للمصادقة في مؤسستكم لضمان حماية البيانات بأهمية النسبية 87%، ثم الفقرة تتم مراجعة سجلات دخول المستخدمين بانتظام كجزء من سياسة الأمان بأهمية النسبية 85.2%، ثم الفقرة تقنيات إدارة الهوية في مؤسستكم تعزز أمان الشبكة السحابية بشكل فعال بأهمية النسبية 80.4%، واهمية النسبية 76.8%نظام المصادقة متعددة العوامل (MFA) مطبق بشكل صارم. ومع ذلك، يجب تعزيز السياسات المتعلقة بإدارة صلاحيات الوصول لضمان حماية البيانات بشكل أفضل.

جدول (5): الإحصاء الوصفي لعينة الدراسة - المحور الثاني (مراقبة الوصول)

رقم الفقرة	العبارة	الأهمية النسبية	الانحراف المعياري	المتوسط الحسابي	موافق بشدة	موافق	محايد	غير موافق
1	إلى أي مدى توافق على أن المصادقة متعددة العوامل تعزز أمان الوصول إلى البيانات في مؤسستكم؟	81.2%	0.812	4.06	27 (33.3%)	34 (42.0%)	18 (22.2%)	2 (2.5%)
2	يتم مراقبة جميع محاولات الوصول إلى البيانات الحساسة في مؤسستكم.	83.8%	0.808	4.19	32 (39.5%)	35 (43.2%)	11 (13.6%)	3 (3.7%)
3	توفر مؤسستكم تنبيهات فورية عند رصد محاولات وصول غير مصرح بها.	83.4%	0.721	4.17	28 (34.6%)	40 (49.4%)	12 (14.8%)	1 (1.2%)
4	يوجد نظام لتحقيق مستمر لأي حوادث وصول مشبوهة.	85.6%	0.693	4.28	34 (42.0%)	36 (44.4%)	11 (13.6%)	–
5	إلى أي مدى توافق على أن نموذج التحكم القائم على الدور (Role-Based Access Control) فعال في حماية البيانات في مؤسستكم؟	81.4%	0.818	4.07	30 (37.0%)	27 (33.3%)	24 (29.6%)	–

يتناول جدول رقم (5) آراء المشاركين حول فعالية تقنيات مراقبة الوصول. النتائج تشير إلى أن هناك اهتمامًا يوجد نظام لتحقيق مستمر لأي حوادث وصول مشبوهة بأهمية النسبية 85.6%، ثم تليها الفقرة يتم

مراقبة جميع محاولات الوصول إلى البيانات الحساسة في مؤسستكم بأهمية النسبية 83.8%، تليها الفقرة توفر مؤسستكم تنبيهات فورية عند رصد محاولات وصول غير مصرح بها بأهمية النسبية 83.4%، ثم تليها الى أي مدى توافق على أن المصادقة متعددة العوامل تعزز أمان الوصول إلى البيانات في مؤسستكم. بأهمية النسبية 81.2%، واخير إلا أن هناك حاجة لتحسين الأنظمة الحالية لمراقبة الوصول وتوفير تنبيهات في مدى توافق على أن نموذج التحكم القائم على الدور (Role-Based Access Control) فعال في حماية البيانات في مؤسستكم. بأهمية النسبية 81.4%.

جدول (6): اختبار t حول الوسط النظري (3) حسب المحور الثاني

المحور الثاني	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية-p value
تقنيات الأمان	81	3.98	0.747	11.75	0.00
إدارة الهوية	81	4.18	0.545	19.53	0.00
مراقبة الوصول	81	4.16	0.579	17.97	0.00
المحور ككل	81	4.10	0.554	17.94	0.00

يقدم جدول رقم (6) نتائج اختبار t لمتوسط تقييمات الأمان وإدارة الهوية ومراقبة الوصول. النتائج تظهر أن المتوسطات الحسابية لجميع المحاور تتجاوز المتوسط النظري 3، مما يدل على أن المشاركين يميلون إلى الاعتقاد بأن هذه الجوانب مهمة. وان القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية.

المحور الثالث: حوكمة البيانات

تشير النتائج في جدول رقم (7) إلى أن 81% من المشاركين يعتقدون أن يتم تدقيق سياسات الأمان بانتظام لضمان الامتثال في مؤسستكم وان 80.4%، وحيث ان الفقرة مؤسستكم تلتزم بسياسات واضحة لحوكمة البيانات،

جدول(7): الإحصاء الوصفي لعينة الدراسة – المحور الثالث

م	حوكمة البيانات		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية
1	مؤسستكم تلتزم بسياسات واضحة لحوكمة البيانات	العدد	1	1	19	34	26	4.02	0.851	80.4%
		النسبة	1.2	1.2	23.5	42	32.1			
2	مؤسستكم ملتزمة بالمعايير التنظيمية (مثل GDPR، ISO 27001) لضمان أمان البيانات	العدد	1	3	28	22	27	3.88	0.967	77.6%
		النسبة	1.2	3.7	34.6	27.2	33.3			
3	يتم تدقيق سياسات الأمان بانتظام لضمان الامتثال في مؤسستكم	العدد	-	4	14	37	26	4.05	0.835	81.0%
		النسبة	-	4.9	17.3	45.7	32.1			
4	توفر مؤسستكم إرشادات دورية لموظفيها حول حماية البيانات وفقاً لسياسات الحوكمة	العدد	2	4	20	33	22	3.85	0.963	77.0%

				27.2	40.7	24.7	4.9	2.5	النسبة
5	يتم تحديث سياسات الحوكمة في مؤسستكم بشكل دوري	العدد	1	4	25	33	18	3.78	0.894	75.6%
		النسبة	1.2	4.9	30.9	40.7	22.2			
6	يتم تقييم سياسات حوكمة البيانات في مؤسستكم لضمان فعاليتها	العدد	-	5	25	30	21	3.83	0.891	76.6%
		النسبة	-	6.2	30.9	37	25.9			

ثم تليها مؤسستكم ملتزمة بالمعايير التنظيمية (مثل GDPR، ISO 27001) لضمان أمان البيانات بأهمية النسبية 77.6%، ثم تليها الفقرة توفر مؤسستكم إرشادات دورية لموظفيها حول حماية البيانات وفقاً لسياسات الحوكمة بأهمية النسبية 77%، والفقرة يتم تقييم سياسات حوكمة البيانات في مؤسستكم لضمان فعاليتها بأهمية النسبية 76.6%، ثم تليها الفقرة يتم تحديث سياسات الحوكمة في مؤسستكم بشكل دوري بأهمية النسبية 75.6%، ومع ذلك هناك حاجة لتحديث السياسات بانتظام لضمان الامتثال للمعايير التنظيمية.

جدول (8): اختبار t حول الوسط النظري (3) حسب المحور الثالث

المحور الثالث	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية
حوكمة البيانات	81	3.90	0.753	10.77	0.00

يعرض جدول رقم (8) نتائج اختبار t لحوكمة البيانات. المتوسط الحسابي هو (3.90) أكبر من متوسط النظري وأن القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية، مما يدل على أن المشاركين يعتقدون أن مؤسساتهم تلتزم بسياسات واضحة لحوكمة البيانات. ومع ذلك، يجب تحديث السياسات بانتظام لضمان الامتثال للمعايير التنظيمية.

المحور الرابع: بيئة السحابة

جدول(9):الإحصاء الوصفي لعينة الدراسة – المحور الرابع

ر	العبارة	الأهمية النسبية	الانحراف المعياري	المتوسط الحسابي	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	اختيار مزود الخدمة السحابية يتم بناءً على مستوى الأمان المطلوب.	79.2%	0.749	3.96	20 (24.7%)	39 (48.1%)	21 (25.9%)	1 (1.2%)	–
2	يوجد اتفاقيات واضحة بشأن خصوصية البيانات بين مؤسستكم	76.2%	0.760	3.81	14 (17.3%)	41 (50.6%)	23 (28.4%)	3 (3.7%)	–

								ومزود الخدمة السحابية.	
–	4 (4.9%)	19 (23.5%)	35 (43.2%)	23 (28.4%)	3.95	0.850	79.0%	يتم تقييم مزودي الخدمة السحابية بانتظام للتأكد من توافقهم مع سياسات الأمان.	3
1 (1.2%)	3 (3.7%)	22 (27.2%)	32 (39.5%)	23 (28.4%)	3.90	0.903	78.0%	يتم تحديد ومتابعة المعايير الأمنية في كل تحديث لمزود الخدمة السحابية.	4
–	2 (2.5%)	20 (24.7%)	31 (38.3%)	28 (34.6%)	4.05	0.835	81.0%	مزود الخدمة السحابية يلتزم بمعايير الأمان المطلوبة لحماية البيانات.	5

يظهر جدول رقم (9) أن 81% من المشاركين يعتقدون مزود الخدمة السحابية يلتزم بمعايير الأمان المطلوبة لحماية البيانات يعتمد على مستوى الأمان المطلوب، وان 79.2%اختيار مزود الخدمة السحابية يتم بناءً على مستوى الأمان المطلوب مما يعزز من بيئة الساحبة ،تليها الفقرة يتم تقييم مزودي الخدمة السحابية بانتظام للتأكد من توافقهم مع سياسات الأمان بأهمية النسبية 79%، ثم تليها الفقرة يتم تحديد ومتابعة المعايير الأمنية في كل تحديث لمزود الخدمة السحابية 78%، ثم تليها الفقرة يوجد اتفاقيات واضحة بشأن خصوصية البيانات بين مؤسستكم ومزود الخدمة السحابية 76.2%، ومع ذلك، يجب تعزيز الاتفاقيات بشأن خصوصية البيانات لضمان حماية المعلومات الحساسة.

جدول (10): اختبار t حول الوسط النظري (3) حسب المحور الرابع

المحور الرابع	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية
بيئة الساحبة	81	3.94	0.711	11.84	0.00

يوضح جدول رقم (10) أن المتوسط الحسابي لبيئة السحابة هو 3.94، أكبر من متوسط النظري وأن القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية، مما يشير إلى أن المشاركين يعتقدون أن اختيار مزود الخدمة السحابية يعتمد على مستوى الأمان المطلوب. ومع ذلك، هناك حاجة لتعزيز الاتفاقيات بشأن خصوصية البيانات.

المحور الخامس: المخاطر المحتملة

جدول (11):الإحصاء الوصفي لعينة الدراسة – المحور الخامس

تشير النتائج جدول رقم (11) إلى أن 81.2% يتم اتخاذ تدابير وقائية ضد الهجمات السيبرانية بشكل استباقي، وان 81% أهمية النسبية تُساهم استراتيجيات إدارة الثغرات الأمنية في حماية البيانات في مؤسستكم.، ثم تليها الفقرة مؤسستكم تعتمد على فريق متخصص لرصد وتقييم المخاطر السيبرانية بأهمية النسبية 80.4%، ثم الفقرة الهجمات السيبرانية المحتملة يتم رصدها بشكل مستمر في مؤسستكم. بأهمية النسبية 79.8%، من المشاركين يعتقدون تتم مراجعة وتحديث خطط الاستجابة للطوارئ السيبرانية بانتظام. بأهمية النسبية 79.6% أن الهجمات السيبرانية يتم رصدها بشكل مستمر. ومع ذلك، يجب أن تكون هناك استراتيجيات أكثر فعالية لإدارة الثغرات الأمنية.

جدول(12):اختبارات حول الوسط النظري (3) حسب المحور الخامس

المحور الخامس	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية
المخاطر المحتملة	81	4.02	0.754	12.17	0.00

يظهر جدول رقم (12) أن المتوسط الحسابي للمخاطر المحتملة هو 4.02، أكبر من متوسط النظري وأن القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية، مما يدل على أن المشاركين يعتقدون أن الهجمات السيبرانية يتم رصدها بشكل مستمر. ومع ذلك، هناك حاجة لاستراتيجيات أكثر فعالية لإدارة الثغرات الأمنية.

المحور السادس: الامتثال التنظيمي

جدول (13): الإحصاء الوصفي لعينة الدراسة – المحور السادس

م	الامتثال التنظيمي		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية
1	تطبق مؤسستكم الإجراءات اللازمة لضمان الامتثال للمعايير الأمنية الدولية.	العدد	-	1	19	27	34	4.16	0.829	83.2 %
		النسبة	-	1.2	23.5	33.3	42			
2	يتم مراجعة السياسات الأمنية لضمان التوافق مع المعايير الجديدة.	العدد	-	2	17	32	30	4.11	0.822	82.2 %
		النسبة	-	2.5	21	39.5	37			
3	يتم توثيق جميع العمليات المتعلقة بحماية البيانات والامتثال للوائح التنظيمية بشكل دقيق ومنظم.	العدد	1	2	17	30	31	4.09	0.897	81.8 %
		النسبة	1.2	2.5	21	37	38.3			
4	تلتزم مؤسستكم بالإبلاغ عن أي حوادث أمان تؤثر على البيانات وفقاً للوائح التنظيمية المتبعة.	العدد	1	2	15	30	33	4.14	0.891	82.8 %
		النسبة	1.2	2.5	18.5	37	40.7			
5		العدد	-	1	11	34	35	4.27	0.742	85.4 %

	في حالة حدوث خرق أمني يتم اتخاذ إجراءات تصحيحية لضمان الامتثال الكامل مع اللوائح التنظيمية.	النسبة	-	1.2	13.6	42	43.2			

تشير النتائج جدول رقم (13) إلى أن 85.4% من المشاركين يعتقدون في حالة حدوث خرق أمني يتم اتخاذ إجراءات تصحيحية لضمان الامتثال الكامل مع اللوائح التنظيمية، وان أهمية النسبية 83.2% تطبق مؤسستكم الإجراءات اللازمة لضمان الامتثال للمعايير الأمنية الدولية ثم تليها أن 82.8% تلتزم مؤسستكم بالإبلاغ عن أي حوادث أمان تؤثر على البيانات وفقاً للوائح التنظيمية المتبعة، ثم الفقرة يتم مراجعة السياسات الأمنية لضمان التوافق مع المعايير الجديدة بأهمية النسبية 82.2%، ثم تليها تلتزم مؤسستكم بالإبلاغ عن أي حوادث أمان تؤثر على البيانات وفقاً للوائح التنظيمية المتبعة. بأهمية النسبية 81.8% ، ومع ذلك، يجب توثيق العمليات المتعلقة بحماية البيانات بشكل دقيق لضمان الشفافية.

جدول (14): اختبار t حول الوسط النظري (3) حسب المحور السادس

المحور السادس	العدد	المتوسط الحسابي	الانحراف المعياري	اختبار t	القيمة الاحتمالية
الامتثال التنظيمي	81	4.15	0.736	14.06	0.00

يعرض جدول رقم (14) نتائج اختبار t للامتثال التنظيمي، حيث يظهر أن المتوسط الحسابي هو 4.15، أكبر من متوسط النظري وأن القيمة الاحتمالية (p-value) أقل من 0.05، مما يعني أن النتائج ذات دلالة إحصائية، مما يدل على أن 83.2% من المشاركين يعتقدون أن مؤسساتهم تطبق الإجراءات اللازمة لضمان الامتثال للمعايير الأمنية الدولية.

العوامل المؤثرة على تحسين امن البيانات والتحكم في الوصول في البيئة السحابية لشركة الخليج

جدول (15): الإحصاء الوصفي – جميع المحاور

م	المحور الأول	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية
1	البيانات الحساسة	4.35	0.543	87.1%
2	تقنيات الأمان	4.10	0.554	82.1%
3	حوكمة البيانات	3.90	0.753	78.0%
4	بيئة الساحبة	3.94	0.711	78.7%
5	المخاطر المحتملة	4.02	0.754	80.4%
6	الامتثال التنظيمي	4.15	0.736	83.1%

يقدم جدول رقم (15) المتوسطات الحسابية لكل محور من المحاور الستة المتعلقة بحماية البيانات. يظهر أن البيانات الحساسة حصلت على أعلى متوسط (4.35) بأهمية النسبية 87.1%، تليها الامتثال التنظيمي (4.15) بأهمية النسبية 83.1%، ثم تليها تقنيات الأمان بمتوسط الحسابي (4.10) وأهمية النسبية 82.1%، ثم تليها المخاطر المحتملة بمتوسط الحسابي (4.02) واهمية النسبية 80.4%، ثم بيئة الساحبة بمتوسط الحسابي (3.94) واهمية النسبية 78.7%، ثم تليها حوكمة البيانات بمتوسط الحسابي (3.90) وأهمية النسبية 78%.

خلاصة النتائج:

الدراسة أظهرت أن شركة الخليج تبذل جهودًا واضحة في حماية البيانات الحساسة والالتزام بالمعايير الدولية. ومع ذلك، تحتاج الشركة إلى:

1. تعزيز تقنيات التشفير والمصادقة متعددة العوامل (MFA).
2. تحسين توثيق العمليات الأمنية.
3. مراجعة وتحديث السياسات الأمنية بشكل منتظم.
4. تعزيز الاتفاقيات مع مزودي الخدمة السحابية لضمان حماية خصوصية البيانات.

التوصيات:

من خلال النتائج التي تحصلنا عليها من دراسة بحثنا نوصي بالاتي :

1- كانت الأهمية النسبية لمحور البيانات الحساسة (87.1%)، مما يشير إلى وعي الموظفين بأهمية حماية البيانات، ولكن هناك حاجة إلى تحسين تصنيفها وتحديث سياسات الأمان الخاصة بها. يوصى بتحديث تصنيف البيانات الحساسة بشكل دوري، وتطبيق سياسات صارمة للتحكم في الوصول إليها، ومراجعة سياسات الحماية بانتظام لمواكبة التهديدات الأمنية.

2- بلغت الأهمية النسبية لمحور تقنيات الأمان (82.1%)، مما يعكس إدراكًا جيدًا لأهمية التشفير وأمن البيانات، ولكن لا تزال هناك حاجة لاعتماد تقنيات تشفير أكثر تطورًا. يوصى بتعزيز بروتوكولات التشفير أثناء نقل وتخزين البيانات، وتبني أحدث تقنيات الحماية، وإجراء مراجعات دورية لاختبار فعاليتها ومعالجة أي نقاط ضعف محتملة.

3- كانت الأهمية النسبية لمحور حوكمة البيانات (78%)، مما يشير إلى الحاجة إلى وضع سياسات واضحة لحوكمة البيانات لضمان الامتثال للمعايير الدولية. يوصى بتحديد أدوار ومسؤوليات جميع الموظفين فيما يتعلق بإدارة البيانات، وتحديث السياسات وفقًا لأي متغيرات تنظيمية، وإجراء عمليات تدقيق دورية لضمان الامتثال المستمر.

4- بلغت الأهمية النسبية لمحور بيئة السحابة (78.7%)، مما يعكس الحاجة إلى التأكد من أن بيئة التخزين السحابي المستخدمة لحفظ البيانات آمنة وموثوقة. يوصى بإجراء تقييم دوري لمزودي الخدمات السحابية للتأكد من التزامهم بالمعايير الأمنية، والتأكد من وجود اتفاقيات واضحة تضمن حماية البيانات المخزنة في السحابة، وفرض قيود صارمة على عمليات نقل البيانات لتجنب أي مخاطر أمنية.

5- سجل محور المخاطر المحتملة أهمية نسبية بلغت (80.4%)، مما يدل على إدراك الموظفين للتهديدات التي قد تواجه بيانات المؤسسة، ولكن هناك حاجة إلى تدابير أكثر فعالية للحد منها. يوصى بوضع استراتيجيات متقدمة لإدارة الثغرات الأمنية، مثل تنفيذ فحوصات أمنية دورية على الأنظمة لاكتشاف أي نقاط ضعف، وتحسين استجابة المؤسسة للهجمات السيبرانية من خلال وضع خطط طوارئ واضحة وتدريب الفرق التقنية على تنفيذها بفعالية.

6- حقق محور الامتثال التنظيمي أهمية نسبية بلغت (83.1%)، مما يعكس وعي الموظفين بضرورة الالتزام باللوائح والأنظمة المتعلقة بحماية البيانات. لضمان الامتثال المستمر، يوصى بتوثيق جميع العمليات الأمنية، ومراجعة السياسات التنظيمية بشكل دوري للتأكد من توافقها مع أحدث المعايير الدولية، وضمان الإبلاغ الفوري عن أي انتهاكات أمنية وفق اللوائح التنظيمية المعتمدة.

7. تطبيق النموذج (الإطار) الأمني المقترح في الشكل(1) كنظام متكامل لإدارة أمن البيانات في شركة الخليج، مع تضمين جميع مراحله لضمان حماية شاملة.

8. تحليل دوري للتهديدات الأمنية باستخدام أدوات النموذج الأمني لتحديد نقاط الضعف وتقييم المخاطر بشكل مستمر.

9. تطوير خطة استجابة للحوادث تعتمد على الإطار الأمني لضمان سرعة الاستجابة وتقليل تأثير أي اختراقات أمنية محتملة.
10. تحديث النموذج الأمني بشكل مستمر لمواكبة التغيرات في طبيعة التهديدات السيبرانية والتقنيات الجديدة.
11. دمج الإطار الأمني في جميع العمليات التشغيلية للشركة لضمان أن الأمان ليس مجرد إجراء مستقل بل جزء من الثقافة المؤسسية.
12. قياس فعالية النموذج الأمني بانتظام من خلال اختبارات واختراقات تجريبية لتقييم مدى قدرة النظام على التصدي للتهديدات.
13. تطبيق إجراءات مراقبة ذكية باستخدام تقنيات تحليل البيانات لدعم النموذج الأمني في الكشف المبكر عن أي نشاط مشبوه.
14. تعزيز التعاون بين الفرق التقنية وفريق إدارة الأمن لتطبيق الإطار الأمني بفعالية وضمان تبادل المعرفة والخبرات.
15- تدعم هذه التوصيات تعزيز أمن البيانات في البيئة السحابية لشركة الخليج من خلال تطبيق أفضل الممارسات الأمنية، مع التركيز على أهمية النموذج الأمني (الإطار) كعنصر أساسي لضمان حماية البيانات، وتقليل المخاطر، والاستجابة الفعالة للتهديدات.

المراجع

[1]A. Anand, N. K. Trivedi, and A. Kumar, "Data security issues and their solutions in cloud computing," Journal of Critical Reviews, vol. 7, no. 14, pp. 2597-2604, 2020. [Online]. Available: https://www.researchgate.net/publication/344336303_DATA_SECURITY_ISSUES_AND_THEIR_SOLUTIONS_IN_CLOUD_COMPUTING.

[2] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," Symmetry, vol. 15, no. 11, p. 1981, Oct. 2023. DOI: 10.3390/sym15111981.

[3] M. Nazir, "Cloud Computing: Overview & Current Research Challenges," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 8, no. 1, pp. 14-22, Nov.-Dec. 2012. [Online]. Available: www.iosrjournals.org.

[4] GeeksforGeeks, "Cloud Networking," GeeksforGeeks, [Online]. Available: https://www.geeksforgeeks.org/cloud-networking/. Accessed: Feb. 10, 2025.

[5] Arabian Gulf Oil Company, "2025 ",شركة الخليج العربي للنفط. [Online]. Available: http://agoco.ly/index.php/ar/. [Accessed: Feb. 25, 2025].

[6]A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data security in cloud computing," IEEE, pp. 55–59, 2016. DOI: 10.1109/FGCT.2016.7605062.

[7]A. J. Apeh, A. O. Hassan, O. O. Oyewole, O. G. Fakeyede, P. A. Okeleke, and O. R. Adaramodu, "GRC strategies in modern cloud infrastructures: A review of compliance challenges," Computer Science & IT Research Journal, vol. 4, no. 2, pp. 111–125, Nov. 2023. DOI: 10.51594/csitrj.v4i2.609.

[8]D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud," Journal of Computer and System Sciences, vol. 78, pp. 1359–1373, 2012. DOI: 10.1016/j.jcss.2011.12.019.
[9]C. Alberts, A. Dorofee, J. Stevens, and C. Woody, OCTAVE®-S Implementation Guide, Version 1.0, Volume 1: Introduction to OCTAVE-S, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2003-HB-003, Jan. 2005.
[10]R. Gupta, D. Saxena, and A. K. Singh, Data Security and Privacy in Cloud Computing: Concepts and Emerging Trends, arXiv:2108.09508, arXiv, 21 Aug. 2021. DOI: 10.48550/arXiv.2108.09508.

[11]P. J. Sun, "Privacy protection and data security in cloud computing: A survey, challenges, and solutions," IEEE Access, vol. 7, pp. 147420–147452, 2019. DOI: 10.1109/ACCESS.2019.2946185.
[12]K. I. Jones and R. Suchithra, "Information security: A coordinated strategy to guarantee data security in cloud computing," International Journal of Data Informatics and Intelligent Computing, vol. 2, no. 1, pp. 11–31, Mar. 2023. DOI: 10.59461/ijdiic.v2i1.34.
[13] M. Al Morsy, J. Grundy, and I. Müller, An Analysis of the Cloud Computing Security Problem, arXiv:1609.01107, arXiv, 5 Sept. 2016. DOI: 10.48550/arXiv.1609.01107.
[14] R. R. Pansara, "Navigating data management in the cloud - Exploring limitations and opportunities," Transactions on Latest Trends in IoT, vol. 6, no. 6, 2023. [Online]. Available: https://ijsdcs.com/index.php/TLIoT/article/view/348.
[15]A. Chotrani, "Information governance within cloud," International Journal of Information Technology (IJIT), vol. 4, no. 2, pp. 38–44, Jul.–Dec. 2023. [Online]. Available: https://www.researchgate.net/publication/376892752_INFORMATION_GOVERNANCE_WITHIN_CLOUD.
[16] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A survey on the security of cloud computing," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), IEEE, pp. 1–7, 2019. DOI: 10.1109/CAIS.2019.8769497.
[17] M. Joshi, S. Prakash, S. Budhani, and N. Tewari, "Analytical review of data security in cloud computing," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), IEEE, pp. 362–366, 2021. DOI: 10.1109/ICIEM51511.2021.9445355.
[18]S. Swain and R. K. Tiwari, "Cloud security research - A comprehensive survey," International Journal of Electronics Engineering and Applications, vol.

8, no. 2, pp. 29–39, Jul.–Dec. 2020. [Online]. Available: https://www.ijeea.in/wp-content/uploads/04-Volume-8-Issue-2-Sunita.pdf.
[19] X. Sun, "Critical security issues in cloud computing: A survey," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE, pp. 216–221, 2018. DOI: 10.1109/BDS/HPSC/IDS18.2018.00053.
[20] A. J. Ouda, A. N. Yousif, A. S. Hasan, H. M. Ibrahim, and M. A. Shyaa, "The impact of cloud computing on network security and the risk for organization behaviors," Webology, vol. 19, no. 1, pp. 195–206, Jan. 2022. DOI: 10.14704/WEB/V19I1/WEB19015.
[21] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access, vol. 8, pp. 131723-131740, Jul. 2020, doi: 10.1109/ACCESS.2020.3009876.
[22] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," IEEE Transactions on Engineering Management, Dec. 2020, doi: 10.1109/TEM.2020.3045661.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.