مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٣) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (3) 2025

إطار عمل لتسهيل تبني البرمجيات مفتوحة المصدر باستخدام تحليل القرار متعدد المعايير

د. باسل حبيب حسن *

م. مارية أحمد شعبان **

(تاريخ الإيداع ٢٠٢٤/١٠/٢٨ . قُبِل للنشر في ٢٠٢٥/٢/٢)

□ ملخّص □

لم يكن الهدف من البرمجيات مفتوحة المصدر إنشاء شركات تنافسية بقدر ما كان توفير بدائل تقنية مرنة تتميز بالشفافية وإمكانية التعديل والمشاركة المجتمعية، حيث شكل ظهورها تحديًا للعروض التقليدية. ويعد فهم التحديات المحتملة لاستخدام برمجيات المصدر المفتوح في تطوير المنتجات أمراً مهماً للمختصين، بحيث يصبحون على دراية بها ويمكنهم توقعها واتخاذ التدابير المناسبة لمواجهتها.

أثناء انتقال المعلومات عبر الأنظمة يمكن تصور العديد من المشكلات ممكنة الحدوث منها أمنية ومنها تقنية، ويمكن حل هذه المشكلات بشكل استباقي إذا قامت الشركات باستخدام إطار عمل مناسب يوضح لها إرشادات حول مخاطر عملية التبني وكذلك متطلبات الأمان كمحاولة لتخفيض تأثير واحتمال حدوث المخاطر وليجنب أنظمة الشركات من الهجمات الأمنية الناجحة، ومن هنا تأتي أهمية البحث الذي يقترح إطار عمل مفاهيمي (Conceptual Framework) يساعد الشركات في تسهيل تنبي البرمجيات مفتوحة المصدر متضمناً القيام بعملية تحليل لمخاطر المصدر المفتوح، والنظر في بدائله وتشكيل فهم أعمق لتطورها وأمانها عبر الزمن، وتقديم رؤى شاملة حول الاتجاهات والابتكارات والتحديات الحديثة.

الكلمات المفتاحية: البرمجيات مفتوحة المصدر، البرمجيات مغلقة المصدر، أمن البرمجيات، تبني المصدر المفتوح، تحليل القرار متعدد المعايير

* أستاذ في قسم البرمجيات ونظم المعلومات، كلية الهندسة المعلوماتية، جامعة تشرين، اللاذقية، سورية
basel.hasan@tishreen.edu.sy

** طالبة دراسات عليا (ماجستير)، قسم البرمجيات ونظم المعلومات، كلية الهندسة المعلوماتية، جامعة تشرين، اللاذقية، سورية
maria.shaban@tishreen.edu.sy

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٣) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (3) 2025

A Framework for Facilitating the Adoption of Open Source Software Using Multi-Criteria Decision Analysis

Dr. Basel Habib Hasan *
Eng. Maria Ahmad Shaban**

(Received 28/10/2024 . Accepted 2/2/2025)

□ ABSTRACT □

The primary aim of open-source software was not to create competitive companies but rather to provide flexible technological alternatives characterized by transparency, modifiability, and community collaboration, posing a challenge to traditional offerings. Understanding the potential challenges of using open-source software in product development is crucial for practitioners, enabling them to anticipate and address these challenges effectively.

When information flows through systems, numerous issues may arise, including security and technical concerns. These can be proactively addressed if companies employ a suitable framework that provides guidance on adoption risks and security requirements. Such a framework would minimize the impact and likelihood of potential risks, protecting corporate systems from successful security breaches.Therefore, this research proposes a conceptual framework to facilitate businesses' adoption of open-source software. It includes analyzing open-source risks, considering alternative options, gaining a deeper understanding of the evolution and security of open-source software over time, and offering comprehensive insights into modern trends, innovations, and challenges.

Keywords: Open Source Software, Closed Source Software, Software Security, Open Source Adoption, Multi Criteria Decision Analysis

* Professor, Department of Software and Information Systems, faculty of Informatics Engineering ,Tishreen University, Lattakia, Syria basel.hasan@tishreen.edu.sy
* Professor, Department of Software and Information Systems, faculty of Informatics Engineering ,Tishreen University, Lattakia, Syria basel.hasan@tishreen.edu.sy
** Postgraduate Student(M.A), Department of Software and Information Systems, faculty of Informatics Engineering , Tishreen University, Lattakia, Syria maria.shaban@tishreen.edu.sy
** Postgraduate Student(M.A), Department of Software and Information Systems, faculty of Informatics Engineering , Tishreen University, Lattakia, Syria maria.shaban@tishreen.edu.sy

١. مقدمة:

في ظل التطور التكنولوجي المتسارع، أصبحت البرمجيات مفتوحة المصدر خياراً استراتيجياً للعديد من المؤسسات التي تسعى للاستفادة من المرونة والتكلفة المنخفضة لهذه البرمجيات. تشير البرمجيات مفتوحة المصدر (والتي يشار إليها اختصاراً بـ: Open source software(OSS)) إلى البرامج التي يتم توفير كودها المصدري للمستخدمين، مما يسمح للمستخدمين بتعديل وتحسين ونشر البرمجيات وفقًا لمتطلباتهم [1]. وبالمقابل تشير البرمجيات مغلقة المصدر إلى برامج الكمبيوتر التي لا يتم نشر أو مشاركة كودها المصدري مع المستخدمين حتى يتمكن أي شخص من الاطلاع عليه أو تعديله، فقط الأشخاص الذين يصنعون البرنامج يمكنهم رؤية الكود وتغييره [2].

حتى الآن، تختلف الآراء حول الفكرة القائلة " الأمن لا يأتي من الاختباء"، ويدور الجدل الشائع بين كل من المستخدمين والمطورين وكذلك الشركات حول ما إذا كانت البرامج مفتوحة المصدر أكثر أو أقل أماناً من البدائل مغلقة المصدر [3].

يكتسب البحث أهميته من ازدياد التوجه في الآونة الأخيرة نحو اعتماد المصدر المفتوح رغم هذا الجدل، حيث استناداً إلى تقرير حالة المصدر المفتوح لعام ٢٠٢٤ [4] في استطلاع تلقى إجمالي ٢٠٤٦ ردًا من أفراد في جميع أنحاء العالم يعملون مع برامج مفتوحة المصدر في مؤسساتهم، قال ٣٤,٠٧% من المجيبين أن استخدامهم للمصدر المفتوح قد ازداد، في حين أن ٣٣,٥% أجابوا بأن استخدامهم قد ازداد بشكل كبير. أما الذين انخفض استخدامهم فكانوا ٥,٣٤% من المجيبين، وفي الغالب من الشركات الناشئة في المرحلة المبكرة، و٢٧,٠٠% قالوا إن استخدامهم للمصدر المفتوح بقي كما هو. يأتي هذا الازدياد نظراً للميزات والتسهيلات التي يقدمها المصدر المفتوح وبوجود عدة عوامل مساعدة مثل الدعم والموثوقية والأمان والتوافر [5]، بالإضافة للتكلفة المنخفضة والأداء والتأثير الاجتماعي وجودة النظام التي تم تفسيرها على نطاق واسع من خلال السلامة والتشغيل البيني وسهولة الاستخدام باعتبارها أهم العوامل في قرارات التبني، وكذلك وجود مجتمع برمجيات المصدر المفتوح (community) الذي يعد مؤشر إعلامي على نضج البرمجيات وميلها للنمو[6] . وقد أثبت عدم وجود تكلفة ترخيص وانخفاض التكلفة الإجمالية السبب الأكثر إقناعاً لاستخدام البرمجيات مفتوحة المصدر في عام ٢٠٢٣ [4] .

لكن مما لا يمكن إغفال ذكره هو أن تبني البرمجيات مفتوحة المصدر يحمل في طياته مجموعة من التحديات والمخاطر، وخاصة في مجال الأمن، حيث استكمالاً للاستطلاع السابق طُرح على المشاركين السؤال: "ماهي تحديات الدعم عند استخدام المصدر المفتوح؟ "، وسُمح لهم في الاستطلاع باستخدام عدة أجوبة، حيث ٧٩% منهم يجدون أن الحفاظ على السياسات الأمنية أو الامتثال لها يمثل تحديًا لهم. أما ٤٢% قالوا إن الحفاظ على الإصدارات المنتهية من البرامج مفتوحة المصدر يمثل تحديًا كبيرًا، و ٤٠% اعتبروا الافتقار إلى الدعم الفني رفيع المستوى تحدي كبير جداً. وبوجود عوامل أخرى مثل الافتقار إلى التطوير الداخلي، والاتصال، وموارد الحوسبة، والخبرة [5]، كان لابد من فهم أهداف العمل وراء البرامج مفتوحة المصدر ومعرفة الإجراءات الواجب التركيز عليها عند تبنيها وتحليلها بدقة لضمان اتخاذ قرارات أفضل، وتقليل المخاطر محتملة الحدوث لاسيما الأمنية منها [3].

٢. هدف البحث:

يتمثل الهدف الرئيسي لهذا البحث في اقتراح إطار عمل مفاهيمي يساعد المؤسسات على تبني وتقييم البرمجيات مفتوحة المصدر بطرق تتسم بالفعالية والكفاءة والمساعدة في عملية اتخاذ القرار الأنسب عند التبني. ويركز البحث على تحليل مخاطر البرمجيات مفتوحة المصدر باستخدام معيار NISTIR 8286 [7] وإنشاء سجل للمخاطر السيبرانية، بالإضافة إلى استخدام نظرية تحليل القرار متعدد المعايير Multi Criteria Decision Analysis(MCDA)لمقارنة البرمجيات مفتوحة المصدر بالبرمجيات مغلقة المصدر من حيث مجموعة من المعايير المهمة .

٣. مواد وطرائق البحث:

٣,١. تحليل المخاطر:

تم تحديد المخاطر المحتملة التي قد تواجه الشركات عند تبنيها البرمجيات مفتوحة المصدر من خلال البدء بتجميع عدد من المقالات والتقارير الرسمية في هذا السياق [4] [8] [9] [10] [11] [12] ، ومن ثم القيام بعملية تحليل المخاطر، وهي عملية يتم فيها تحديد احتمالية (likelihood) أن تؤدي المخاطر إلى تأثيرات ضارة على أصول النظام (assets)، كذلك تحديد تأثير هذه الخطر(impact) ، ثم حساب مستوى الخطورة (exposure)، وذلك باستخدام مصفوفة الأثر والاحتمال وفق معيار800-30 NIST Sp [7] ، بالإضافة إلى وضع كل خطر في الفئة (category) التي تناسبه.

تُوثَّق عملية تحليل المخاطر بسجل يمثل مدخل لصنّاع القرار يسمى CyberSecurity Risk Register(CSRR) وفقاً لمعيار National Institute of Standards and Technology(NIST) سلسلة NISTIR 8286(A,B,C) [7]، وهذا السجل موجود في ملف Excel منفصل. وفيما يتعلق بالمخاطر المستخرجة، تم تصنيفها ضمن **ست فئات رئيسية**، وهي: **الأمان** (Security)، **التكلفة** (Cost)، **قابلية الصيانة** (Maintainability)، **الموثوقية** (Reliability)، **الامتثال التنظيمي** (Regulatory)، **وسهولة الاستخدام** (Usability).

٣,٢. تحليل القرار متعدد المعايير:

ينظر إلى عمليه صناعه قرار بأنه تلك السلوكيات والاجراءات التي تسبق وتحدد وتلي اتخاذ القرار، حيث تأتي عمليه صناعه القرار كنشاط ذهني مركز لإنتاج خيار محدد. وينظر لتحليل القرار متعدد المعايير على أنه أحد فروع بحوث العمليات الذي يقيّم بشكل صريح معايير متضاربة متعددة في اتخاذ القرار بوجود عدد من البدائل المحددة مسبقاً.

تم تطبيق نظرية تحليل القرار متعدد المعايير لحساب نسبة المخاطرة الإجمالية عند التبني ومساعدة المؤسسات في اتخاذ قرار يتوافق بشكل أفضل مع متطلباتها وأولوياتها عند تبنيها للمصدر المفتوح. و تمتلك هذه النظرية العديد من الطرق لتطبيقها، في هذا البحث تم اختبار اثنتين من الطرق، الأولى هي التحليل الهرمي Analytic Hierarchy Process (AHP)، والأخرى هي نظرية المنفعة متعددة السمات Multi Attribute Utility Theory(MAUT) .

٣,٢,١. خطوات نظرية تحليل القرار متعدد المعايير:

هناك خطوات منطقيه يستخدمها متخذ القرار الوصول الى حل(بديل) مقبول وليس بالضرورة ان يكون هذا البديل هو الحل الأمثل، وتأتي نماذج القرار لتعبر عن هذه الخطوات بشكل او بآخر.

a. تحديد الهدف العام:

والهدف هنا مساعدة المؤسسات في اتخاذ قرار يتوافق بشكل أفضل مع متطلباتها وأولوياتها عند تبنيها للمصدر المفتوح.

b. تحديد المعايير المؤثرة في اتخاذ القرار:

لا يمكن الحكم على بديل بأنه مناسب إلا بناء على المقارنة مع معايير معرفة وقائمة على أساس الحكم على النتائج المحتملة لهذه البدائل، وبناءً على عملية تحليل المخاطر ووفقاً لسجل المخاطر ستكون المعايير المؤثرة باتخاذ القرار هي الفئات (Category) التي تم ذكرها سابقاً في الفقرة (٣-١).

c. تحديد البدائل المتاحة:

تعريف الخيارات التي يمكن أن تطبق للانتقال بمشكله إلى حاله أفضل. يمكن للنظرية أن تقارن أداء عدة بدائل، في بحثنا لدينا بديلين فقط هما البرمجيات مفتوحة المصدر والبرمجيات مغلقة المصدر.

d. حساب وزن ومعدل كل معيار:

يعكس **الوزن (Weight)** الأولوية النسبية للمعيار مقارنةً بالمعايير الأخرى (أهمية كل معيار في عملية التقييم)، فمثلاً بوجود معايير مثل الأمان والتكلفة والموثوقية، عند النظر للأمان على أنه المعيار الأكثر أهمية، يمكن إعطاؤه وزن أعلى.

يعكس **المعدل (Score)** كيفية أداء كل بديل وفقاً للمعيار المحدد (التقييم الفعلي لكل بديل بناءً على المعايير)، ويتم تحديد قيمه من خلال جمع بيانات حول كيفية أداء كل بديل بناءً على المعيار.

ولحساب الأوزان والمعدلات تم استخدام **طريقة التحليل الهرمي** وهي إحدى طرق نظرية تحليل القرار متعدد المعايير التي طورها Saaty [14] بهدف المساعدة في اتخاذ القرار في البيئات المعقدة. تستخدم هذه الطريقة مفهوم المقارنات الزوجية Pairwise Comparisons الذي يمثل بمصفوفة موضحة بالجدول (١)، وهي عملية مقارنة كل معيار مع الآخر (معيارين في وقت واحد) بشكل زوجي وفقًا لأهميته النسبية في تحقيق الهدف الرئيسي. وهذا التقييم يكون باستخدام مقياس التفضيل الأساسي الذي اقترحه Saaty [14] والموضح بالشكل (١):

Criteria preferences	Security	Reliability	Regulatory	Maintainability	Usability	Cost
Security	a11	a12	a13	a14	a15	a16
Reliability	a21	a22	a23	a24	a25	a26
Regulatory	a31	a32	a33	a34	a35	a36
Maintainability	a41	a42	a43	a44	a45	a46
Usability	a51	a52	a53	a54	a55	a56
Cost	a61	a62	a63	a64	a65	a66

الجدول (١): مصفوفة المقارنات الزوجية – الشكل العام

القيم المعطاة في المقارنة يتم تعيينها وفقاً لرؤى الشركة وأصحاب الخبرة فيها وتقديرهم لأهمية المعيار.

ويتراوح مقياس التفضيل المستخدم بين ١ و ٩ كما هو موضح في الشكل (1)، حيث تعكس كل قيمة مستوى معينًا من الأهمية النسبية بين معيارين أو بديلين.

شدة الأهمية	التعريف	التفسير
١	أهمية متساوية	نشاطان يساهمان بالتساوي في تحقيق الهدف.
٢	أهمية ضعيفة أو طفيفة	
٣	أهمية معتدلة	الخبرة والحكم يميلان بشكل متوسط لصالح أحد الأنشطة على الآخر.
٤	أهمية معتدلة زائدة	
٥	أهمية قوية	الخبرة والحكم يميلان بشدة لصالح أحد الأنشطة على الآخر.
٦	أهمية قوية زائدة	
٧	أهمية قوية جداً أو مؤكدة	يتم تفضيل نشاط على الآخر بقوة كبيرة؛ يظهر هيمنته في التطبيق العملي.
٨	أهمية قوية للغاية	
٩	أهمية قصوى	الأدلة التي تدعم تفضيل نشاط على الآخر هي الأعلى من حيث الأهمية الممكنة.
مقلوب ماسبق	إذا كان للنشاط i قيمة غير صفرية مقارنة بالنشاط j ، فإن لـ j قيمة مقلوبة عند المقارنة بـ i	افتراض معقول.
1.1 – 1.9	إذا كانت الأنشطة قريبة جداً من بعضها البعض	قد يكون من الصعب تحديد القيمة الأفضل، لكن عند مقارنتها بأنشطة أخرى ذات تباين، لن تكون الارقام الصغيرة ملحوظة للغاية، الا انها لاتزال تشير إلى الأهمية النسبية للأنشطة

الشكل (1): مقياس الأعداد المطلقة الأساسي [14]

في مصفوفة المقارنات الزوجية يتم مقارنة معيارين اثنين فقط بالوقت نفسه، وتمثل عناصرها بـ a_{ij} .

- عند مقارنة المعيار مع نفسه (i = j) تكون قيمة الخلية واحد $a_{ij} = 1$ (لذلك القطر الرئيسي دائما واحد). مثلاً: معيار الأمن $a_{11} = 1$ ، معيار الموثوقية $a_{22} = 1$ ....وهكذا.

- إذا كان $a_{ij} = a$ فإن: $a_{ji} = \frac{1}{a}$ مثلاً: عند مقارنة معيار الأمن مع الكلفة وكانت قيمة الخلية $a_{16} = 2$ فهذا يدل على أن لمعيار الأمن ضعف أهمية معيار الكلفة. وبالمقابل تكون أهمية الكلفة بالنسبة للأمن هي النصف $a_{61} = \frac{1}{2}$.
- إذا كان في المصفوفة بديلين متساويين في الأهمية، فإن: $a_{ij} = a_{ji} = 1$

بعد ملء المصفوفة يتم يحسب المتوسط الهندسي Geometric mean (القيمة المتوسطة لمجموعة من الأرقام وجدت باستخدام حاصل ضرب قيمها، بدلًا من المجموع) ويرمز له (V)، ثم الوزن النسبي للمعايير Normalized weights ويرمز له (W)، وتحسب هاتان القيمتان وفقاً للعلاقتين(١) و(٢) [14]:

Geometric mean

(١) $v_1 = \sqrt[n]{x_1 x_2 \dots . x_n}$ $n: number\ of\ criteria,\ x_i\ cells\ of each\ row$

(٢) Normalized weights $w_1 = \frac{v_1}{\sum_1^n v_i}$

e. تحديد الخيار الأفضل وحساب المنفعة (Utility):

يتم حساب المنفعة الإجمالية (تمثيل رقمي لمدى أهمية شيء ما أو فائدته) لكل بديل وفقاً لعدة توابع تعود لنظرية المنفعة متعددة السمات سيتم ذكرها لاحقاً في فقرة (٣-٢-٢)، وثم مقارنة هذه القيم، والخيار الذي يعطي قيمة منفعة أعلى يكون هو الخيار الأمثل وفقاً للمعايير المعطاة وقيمها المدخلة.

٣,٢,٢. نظرية المنفعة متعددة السمات (MAUT):

هي أداة هندسية لصنع وتحليل القرار من خلال إجراء المقارنة المنطقية بين مجموعة البدائل وصولاً للقرار الأكثر فعالية من خلال تعيين قيم المنفعة (utility) لمعايير مختلفة وترجيحها بناءً على أهميتها النسبية، ويعتمد نهج القرار المقترح على مجموعة مرجحة من توابع المنفعة وهي: تابع المنفعة الجمعي الموزون(WAUF) (٥)، تابع المنفعة الهندسي الموزون(WGUF) (٦)، تابع المنفعة التوافقي الموزون (WHUF) (٧)، مع مراعاة (٣) (٤) [15] :

(٣) $\sum_{j=1}^{N} w_j = 1$ and $0 \le w_j \le 1$ alternatives $\{A_i \mid i=1,\dots, m\}$ A=

(٤) $0 < u_j(a) < 1$ weights $\{w_j \mid j=1\dots, n\}$ W=

- (WAUF): Weighted arithmetic utility function

$U(A_1,\dots, A_n) = \sum_{i=1}^{n} w_i\ U_i(a_i) = w_{A_1} \text{ x } u(A_1) + w_{A_2} \text{ x } u(A_2) + \dots + w_{A_n} \text{ x } u(A_n)$ (٥)

- (WGUF): Weighted Geometric utility function

$U(A_1,\dots, A_n) = \prod_1^n U_i(a_i)^{w_i} = u(A_1)^{w_{A_1}} . u(A_2)^{w_{A_2}} \dots . u(A_n)^{w_{A_n}}$ (٦)

Weighted harmonic utility function (WHUF):

$U(A_1,\dots, A_n) = \sum_{i=1}^{n} w_i \frac{1}{U_i(a_i)} = w_{A_1} \text{ x} \frac{1}{u(A_1)} + w_{A_2} \text{ x} \frac{1}{u(A_2)} + \dots + w_{A_n} \text{ x } \frac{1}{u(A_n)}$ (٧)

التابع الجمعي الموزون (WAUF) :

يعتمد هذا التابع على **استقلالية المعايير**، أي أن تأثير كل معيار على البديل يكون مستقلاً عن تأثير المعايير الأخرى. بعبارة أخرى، تغيير وزن معيار معين لن يؤثر على أوزان أو قيم المعايير الأخرى. على سبيل المثال، إذا كان معيار الأمان مهمًا، فإن قيمته ستبقى كما هي سواء كان هناك تركيز على معيار الكلفة أم لا.

التابع التوافقي الموزون (WHUF) :

يهدف هذا التابع إلى **التعامل مع القيم المنخفضة** للمعايير والحد من تأثيرها السلبي على المنفعة الكلية، مما يساعد في تحقيق التوازن .بمعنى أنه يقلل من تأثير القيم الصغيرة، بحيث لا تؤدي إلى إضعاف قيمة المنفعة النهائية بشكل كبير.

التابع الهندسي الموزون (WGUF) :

في هذا التابع، **تأثير المعايير ليس مستقلاً**، بل يمكن أن تتفاعل القيم مع بعضها البعض، بحيث يؤدي تغيير قيمة معيار ما إلى تغيير قيمة معيار آخر أو التأثير على النتيجة النهائية للمنفعة الكلية. على سبيل المثال، زيادة الأمان قد تتطلب زيادة في التكلفة، مما يمكن أن يقلل من سهولة الصيانة.

٣,٢,٣. الاتساق:Consistency

نظراً لأن القيم الرقمية المسندة في مصفوفة المقارنات الزوجية مستمدة من التفضيلات الذاتية للأفراد، من الصعب جداً تجنب بعض التناقضات في المصفوفة النهائية للتحكيم. لتحديد ما إذا كانت اختيارات صانعي القرار متسقة في نهج التحليل الهرمي، يتم حساب ما يسمى بنسبة التوافق Consistency Ratio، وتعد نسبة التوافق لكل بديل مقبولة على نحو كافٍ إذا كانت قيمتها أقل من (10%)، وخلافه يجب إعادة النظر في حسابات الأهمية النسبية لعدم دقة التخمين الوارد في مصفوفة المقارنة الثنائية. وتحسب هذه النسبة وفقاً لـ Saaty كما يلي:

يحسب أولا مؤشر التوافق(الاتساق) Consistency Index وفقاً للعلاقة (8) [13] :

$$CI = \frac{\lambda max - n}{n-1} \quad (٨)$$

حيث أن λmax تمثل القيمة الذاتية الأعلى لكل معيار، وتحسب بإيجاد جداء كل سطر بمصفوفة المقارنات الزوجية بعمود الأوزان، و n هو عدد المعايير التي تم تقييمها في المصفوفة، ثم تحسب نسبة التوافق Consistency Ratio(CR) وفقاً للعلاقة (٩) [13]:

$$CR = CI/RCI \quad (٩)$$

يمثل Random Consistency Index (RCI) مؤشر التطابق العشوائي وتؤخذ قيمته وفقاً لعدد البدائل كما هو موضح بالشكل (٢):

n	1	2	3	4	5	6	7	8	9
RCI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

الشكل (٢): مؤشر التطابق العشوائي[14]

٣,٣. تحليل التقارير:

عند مقارنة البرمجيات مفتوحة المصدر بمغلقة المصدر، قد يكون من الصعب تقييم أيهما أنسب بشكل عام دون تحليل ميزات وأداء كل منتج على حدة. لذلك، تم اختيار اثنين من أنظمة إدارة موارد الشركات Enterprise Resource Planning (ERP) كحالة دراسية، وهي أنظمة تهدف إلى تحسين التنظيم الداخلي للشركات وزيادة الكفاءة من خلال دمج مختلف الوظائف والعمليات في نظام مركزي واحد .حيث تمت عملية تحليل المعلومات وفق منهجية منظّمة شملت الخطوات التالية:

a. **اختيار المنتجات:** تم اختيار Odoo وSAP كممثلين عن البرمجيات مفتوحة المصدر ومغلقة المصدر على التوالي، نظرًا لانتشارهما الواسع واعتماد المؤسسات المختلفة عليهما.

b. **جمع البيانات من مصادر متنوعة:**

- تم جمع تقارير دوريّة لكلا النظامين من المواقع الرسمية الخاصة بـ Odoo و SAP [16] [17] [18] حيث توفر بيانات حول تحديثات الأمان والإصلاحات والتهديدات الأمنية المسجلة وغيرها.
- تم استخدام مقالات علمية حديثة من مجلات موثوقة ومدونات متخصصة تتناول واقع النظامين و التحديات الأمنية التي يواجهانها [19] [20].

c. **تحليل البيانات:**

- بعد جمع التقارير والمقالات، تم إجراء التحليل باستخدام Google Colab ولغة Python

تم إجراء التحليل باستخدام تقنيات معالجة اللغات الطبيعية **Natural Language Processing (NLP)** المتقدمة بشكل منهجي واستخلاص المعلومات المتعلقة بالثغرات الأمنية، استراتيجيات تخفيف المخاطر، ومدى متانة النظامين وغيرها من المعلومات.

تم استخدام **Google Colab** كبيئة تطوير لتنفيذ وتحليل البيانات، وتم اعتماد لغة Python نظرًا لانتشارها الواسع في تطبيقات تحليل البيانات. كما تم استخدام **منصة Cohere** التي توفر خدمات معالجة اللغة الطبيعية باستخدام نماذج لغوية كبيرة Large Language Models (LLMs) مدربة مسبقًا يمكن ضبطها بدقة. بالإضافة إلى ذلك تم توظيف عدد من **المكتبات المتخصصة في لغة بايثون** مثل: pandas لمعالجة البيانات، numpy للعمليات العددية، matplotlib و seaborn لتصور البيانات، وقدم هذا المزيج من المكتبات والأدوات دعمًا شاملاً لكل من مهام تحليل البيانات والتنبؤ.

ومن خلال الإحصائيات المقدمة على موقع https://www.cvedetails.com/، تم تحديد العدد الإجمالي للثغرات الأمنية المسجلة في كل من نظامي Odoo وSAP على مدار فترة زمنية محددة (من ٢٠١٠ إلى ٢٠٢٤). هذه البيانات وفرت رؤية حول معدل اكتشاف الثغرات لكل نظام ومدى تعرضهما للتهديدات الأمنية. واستنادًا إلى تلك الإحصائيات (من ٢٠١٠ إلى ٢٠٢٤) تبين أن:

نظام Odoo يمتلك ٥٢ ثغرة أمنية، وهذا يُظهر مخاطر أمنية إجمالية أقل مقارنةً بـ SAP. ومع ذلك، فإن غالبية الثغرات لها درجات خطورة CVSS عالية نسبيًا (١٠-٦)، مما يعني أنها تشكل مخاطر كبيرة على الرغم من أن العدد أقل.

نظام SAP يمتلك 1439 ثغرة أمنية خلال نفس الفترة، مما يشير إلى سطح هجوم أكبر بكثير. على الرغم من أن الثغرات الأمنية تمتد على نطاق CVSS أوسع (من ٢ إلى ١٠)، فإن حجم الثغرات الأمنية الأعلى خطورة (٧–١٠) كبير، مما يتطلب إدارة أمنية دقيقة.

٣,٤. مثال نظرية تحليل القرار متعدد المعايير:

فيما يلي تطبيق عملي لنظرية تحليل القرار متعدد المعايير على البديلين (SAP و Odoo) وفقاً لمعايير (الأمن، الموثوقية، الامتثال التنظيمي، قابلية الصيانة، سهولة الاستخدام، التكلفة)، حيث يتم البدء بملء مصفوفة المقارنات الزوجية كما هو موضح بالجدول (٢) وفقاً لمقياس التفضيل الموضح بالشكل (١)، وكما ذكر سابقاً هذه القيم تعبر عن أهمية كل معيار مقارنةً بباقي المعايير، ويتم تعيينها وفقاً لرؤى الشركة وأصحاب الخبرة فيها:

الجدول (٢): مصفوفة المقارنات الزوجية للمعايير – مثال تطبيقي

Criteria preferences	Security	Reliability	Regulatory	Maintainability	Usability	Cost	Geometric Mean	weight
Security	1	2	3	3	4	3	2.449	0.3491
Reliability	1/2	1	2	1	3	2	1.348	0.1852
Regulatory	1/3	1/2	1	1/3	3	2	0.832	0.1207
Maintainability	1/3	1	3	1	3	2	1.348	0.1953
Usability	1/4	1/3	1/3	1/3	1	1/2	0.408	0.0575
Cost	1/3	1/2	1/2	1/2	2	1	1	0.0922

تحليل قيم المقارنات الزوجية:

لحساب الأوزان:

عند مقارنة معيار الأمن مع معيار الموثوقية: تشير **القيمة ٢** إلى أن معيار الأمن يُعتبر أكثر أهمية من معيار الموثوقية **بمرتين**، ولكن هذه الأفضلية ليست شديدة (أي أن الفارق بينهما واضح ولكنه ليس كبيرًا للغاية). وبالمقابل عند مقارنة معيار الموثوقية مع معيار الأمن يكون لمعيار الموثوقية **نصف** أهمية معيار الأمن. وذلك وفقًا لقيمة المقارنة **1/2** في مصفوفة المقارنات الزوجية.

عند مقارنة معيار الأمن مع معيار الامتثال التنظيمي: تشير **القيمة ٣** إلى أن معيار الأمن أكثر أهمية من معيار الامتثال التنظيمي **بثلاث** مرات **أي** له **أفضلية معتدلة** يمكن ملاحظتها بوضوح لكن ليس بشكل مبالغ فيه. وبالمقابل يكون الامتثال التنظيمي أقل أهمية من معيار الأمن بمقدار **الثلث** .ويتم الإكمال بنفس الطريقة بما يخص جميع المعايير....

- يتم حساب المتوسط الهندسي وفقاً للعلاقة (١) لكل معيار من المعايير بإيجاد الجذر السادس (بسبب وجود ٦ معايير) لجداء قيم الصف الواحد كما يلي:

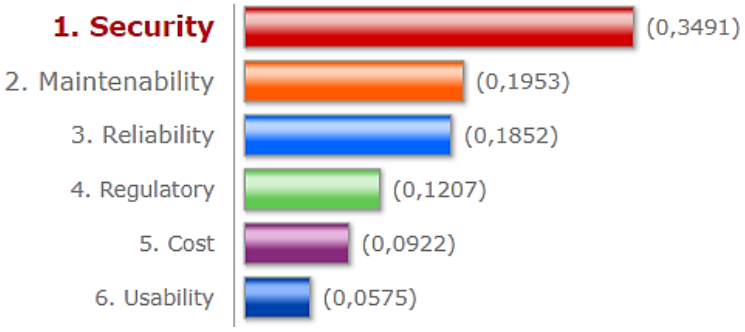
$$\text{v}_1 = \sqrt[6]{1*2*3*3*4*3} = ٢,٤٤٩ \quad \text{v}_2 = \sqrt[6]{\frac{1}{2}*1*2*1*3*2} = ١,٣٤٨$$

ويتم الإكمال بنفس الطريقة لجميع صفوف المصفوفة.

- يتم حساب أوزان المعايير من المصفوفة السابقة وفقا للعلاقة (2) التي سبق ذكرها كما يلي:

$$w_1 = \frac{v_1}{\sum_1^n v_i} = \frac{2.449}{7.385} = 0.3491 \quad w_2 = \frac{v_2}{\sum_1^n v_i} = \frac{1.348}{7.385} = 0.1953$$

يتم حساب باقي الأوزان بنفس الطريقة، وبناءً على ذلك تم التوصل إلى الأوزان النسبية الموضحة بالشكل (٣) ومرتبة بدءاً من المعيار الأكثر وزناً بالتالي الأكثر أهمية بالنسبة لنا، حيث أن الأمن هو المعيار الأكثر أهمية يليه معيار قابلية الصيانة، بينما جاء معيار سهولة الاستخدام كأقل المعايير أهمية.



الشكل (٣): أوزان المعايير

لحساب المعدلات:

في الخطوة التالية يتم حساب معدلات المعايير(scores)، وكما ذكر سابقاً هذه القيم تعبر عن كيفية أداء كل بديل وفقًا للمعيار المحدد، وتم تعيينها وفقاً للمعلومات المستخلصة من تحليل التقارير الذي تم إجراءه سابقاً وهي كالتالي:

- تم إعطاء معيار الأمن في نظام SAP **القيمة ٢** التي تشير الى أن SAP أكثر أمان **بمقدار الضعف** من نظام Odoo، أي هذه يدل على وجود تحسينات أو ميزات أمان إضافية في SAP مقارنةً بـ Odoo، لكنها ليست بالقدر الذي يجعلها تسيطر تماماً على هذا المعيار. والسبب في ذلك أن:

طبيعة النظام:

كنظام مفتوح المصدر تسمح الشفافية في Odoo باكتشاف أسرع لقضايا الأمان من قبل المجتمع (Community). ولكن بالمقابل يمكن للجهات الفاعلة السيئة التقاط الثغرات الأمنية بسهولة. أما الطبيعة المغلقة لـ SAP تجعل من الصعب على المهاجمين العثور على نقاط الضعف. ولكن بالمقابل يعتمد المستخدمون بالكامل على التحديثات والتصحيحات الرسمية من SAP، مع وجود قدر أقل من الشفافية حول كيفية التعامل مع نقاط الضعف.

التشفير:

يدعم Odoo تشفير(SSL/TLS) لتأمين البيانات أثناء النقل. يتم تجزئة كلمات المرور باستخدام Password-Based Key Derivation Function 2(PBKDF2) ، وهي طريقة آمنة لتخزين كلمات المرور. بينما يدعم SAP التشفير الشامل، سواء أثناء النقل (SSL/TLS) أو في حالة السكون، وغالبًا ما تكون معايير التشفير فيه أكثر تقدمًا بسبب متطلبات الصناعات التي يقوم بتخديمها.

التصحيحات الأمنية:

يصدر Odoo تحديثات متكررة، ولكن نظراً لطبيعة النظام مفتوح المصدر، تكون الشركات مسؤولة عن تطبيق التحديثات يدويًا أو الاعتماد على مساهمات المجتمع. بالمقابل تصدر SAP تحديثات تصحيح الأمان الشهرية. تعالج هذه التحديثات الثغرات الأمنية المحددة ويتم تسليمها من خلال القنوات الرسمية. ونظرًا لحجمها، فإن نهج SAP في تحديثات الأمان شامل ومنهجي.

- تم إعطاء معيار التكلفة في نظام Odoo **القيمة ٣** للدلالة على أن Odoo أكثر أهمية من حيث التكلفة بمقدار **ثلاث أضعاف** من نظام SAP. والسبب في ذلك أن:

يعتبر نموذج ترخيص SAP معقد ومكلف، وغالبًا ما ينطوي على تكاليف أولية كبيرة بناءً على عدد المستخدمين والوحدات المطلوبة. بينما إصدار المجتمع ل Odoo مجاني للاستخدام ولكنه قد يتطلب تكاليف الاستضافة والدعم والتطوير المخصص، وعادةً ما تكون تكاليف الصيانة والدعم السنوية لشركة SAP أعلى عادةً، كما تعتبر تكاليف التنفيذ في نظام SAP أعلى بكثير من Odoo.

- تم إعطاء معيار سهولة الاستخدام في نظام Odoo **القيمة ٣** للدلالة على أن Odoo أكثر أهمية من حيث سهولة الاستخدام بمقدار **ثلاث أضعاف** من نظام SAP والسبب في ذلك أن:

يتمتع Odoo بواجهة حديثة وبديهية مصممة لسهولة التنقل، حتى للمستخدمين غير الفنيين. كما تسمح هيكلية Odoo للمستخدمين بإضافة وتخصيص الوظائف بناءً على احتياجاتهم المحددة دون تعقيد الواجهة. بينما غالبًا ما تتطلب SAP تدريبًا متخصصًا وشهادات لاستخدامها بشكل فعال، وقد يؤدي عمق الميزات إلى صعوبة استخدامها وتكوينها.

- تم إعطاء معيار الموثوقية في نظام SAP **القيمة ٢** للدلالة على أن SAP أكثر أهمية من حيث سهولة الاستخدام **بمرتين** من نظام Odoo والسبب في ذلك أنه:

على الرغم من اكتساب Odoo شعبية، إلا أنه أحدث نسبيًا وقد لا يتمتع بنفس مستوى الموثوقية في بيئات المؤسسات الحرجة. كذلك اعتماد الدعم فيه على موارد المجتمع يمكن أن يؤدي إلى تباين في الموثوقية حسب خبرة المستخدم.

أما SAP فيقدم خدمات دعم شاملة وتحديثات منتظمة، وغالبًا ما يكون لدى الشركات الكبيرة عقود دعم مخصصة تضمن حلًا سريعًا للمشكلات. وتساهم بنيته التحتية الراسخة ودعمه الشامل وميزات الأمان القوية في سمعته كنظام موثوق به.

- تم إعطاء معيار الامتثال التنظيمي في نظام SAP **القيمة ٣** للدلالة على أن SAP أكثر أهمية من حيث سهولة الاستخدام بمقدار **ثلاث أضعاف** من نظام Odoo والسبب في ذلك أن:

نظام SAP هو الخيار المفضل بشكل عام لضمان الامتثال بشكل فعال خاصة بالنسبة للمؤسسات والصناعات الأكبر حجمًا ذات المتطلبات التنظيمية الصارمة حيث يشتهر ببروتوكولات الأمان القوية والميزات التي تساعد في حماية البيانات الحساسة وضمان الامتثال للخصوصية. أما نظام Odoo فعلى الرغم من وجود تدابير أمنية، إلا أن طبيعتها مفتوحة المصدر قد تقدم تباينًا في كيفية إدارة أمان البيانات والخصوصية.

- تم إعطاء معيار قابلية الصيانة في نظام Odoo **القيمة ٣** للدلالة على أن Odoo أكثر أهمية من حيث قابلية الصيانة بمقدار **ثلاث أضعاف** من نظام SAP والسبب في ذلك أن:

سهولة التحديثات:

Odoo التحديثات المنتظمة سهلة التنفيذ، والبنية المعيارية تسمح للمستخدمين بتطبيق التغييرات بشكل انتقائي دون التأثير على النظام بأكمله، بينما التحديثات في نظام SAP يمكن أن تكون أكثر تعقيدًا وتستغرق وقتًا طويلاً بسبب حجم النظام وطبيعته المتكاملة.

التخصيص:

نظراً لكونه مفتوح المصدر، يسمح Odoo بتخصيص وتعديلات أسهل. كما يتمتع بمجتمع قوي وتوثيق شامل يمكن أن يساعد المستخدمين في استكشاف الأخطاء وإصلاحها، مما يجعل الصيانة أكثر مرونة. بالمقابل يمكن أن تكون التخصيصات في SAP أكثر صرامة وتتطلب اختبارات مكثفة، مما يجعلها أقل قابلية للتكيف عند الحاجة إلى التغييرات.

بعد تعيين هذه القيم يتم تشكيل مصفوفة المقارنات الزوجية لكل معيار بالنسبة لكل بديل وذلك لحساب معدلات المعايير وفقاً للبدائل بنفس طريقة حساب الأوزان بناءً على القيم الموضحة أعلاه، وفي الجدولين (٣) (٤) مثال لذلك:

الجدول (٣): مصفوفة المقارنات الزوجية للبدائل بالنسبة لمعيار الأمن

Security	SAP	Odoo	Geometric Mean	Score
SAP	1	2	1.4142	0.666
Odoo	1/2	1	0.7071	0.333

حساب المتوسط الهندسي لمعيار الأمن:

$$1.4142 = \sqrt[2]{1*2} = v_1 \qquad = \sqrt[2]{1/2*1} = 0.7071 v_2$$

حساب معدلات معيار الأمن بالنسبة للبديلين:

$$= \frac{v_1}{\sum_1^n v_i} = \frac{1.4142}{2.1213} = 0.666 s_1 \qquad = \frac{v_2}{\sum_1^n v_i} = \frac{0.7071}{2.1213} = 0.333_1 s$$

الجدول (٤): مصفوفة المقارنات الزوجية للبدائل بالنسبة لمعيار التكلفة

Cost	Odoo	SAP	Geometric Mean	Score
Odoo	1	3	1.7320	0.7500
SAP	1/3	1	0.5773	0.2500

حساب المتوسط الهندسي لمعيار الكلفة:

$$1.7320 = \sqrt[2]{1*3} = v_1 \qquad = \sqrt[2]{1/3*1} = 0.5773 v_2$$

حساب معدلات معيار الكلفة بالنسبة للبديلين:

$$= \frac{v_1}{\sum_1^n v_i} = \frac{1.7320}{2.1213} = 0.7500 s_1 \qquad s_1 = \frac{v_2}{\sum_1^n v_i} = \frac{0.5773}{2.1213} = 0.2500$$

ويتم الإكمال بنفس الطريقة لجميع المعايير لحساب معدلاتها بالنسبة لكل بديل من المصفوفات السابقة فتكون النتيجة كما هو موضح بالجدول (٥):

الجدول (٥): معدلات المعايير

Criteria preferences	Security	Maintainability	Reliability	Regulatory	Cost	Usability
SAP	0.6667	0.2500	0.6667	٠,٧٥٠٠	0.2500	0.2500
Odoo	0.3333	0.7500	0.3333	٠,٢٥٠٠	0.7500	0.7500

وفيما يلي ترتيب البدائل مع إظهار الهيكلية بالتفصيل لكل معيار وحساب الفائدة الاجمالية للبدائل وفقا لنظرية التحليل الهرمي و التي توضحها العلاقة (6) [15] ، وهي إيجاد مجموع جداءات وزن كل معيار بمعدله وذلك لكل بديل:

$$U(A_1,\ldots,A_n) = \sum_{i=1}^{n} w_i \; U_i(a_i) = w_{A_1} \text{ x } u(A_1) + w_{A_2} \text{ x } u(A_2) + \ldots + w_{A_n} \text{ x } u(A_n) \quad (6)$$

$$U(sap) = 0.3491 * ٠,٦٦٦٧ + 0.1852*0,6667 + 0.1953*0,2500$$

$$+ 0.0575*0.2500 + 0.0922* 0.2500 + 0.1207* 0.7500 = \mathbf{0.5 ٣٣٠}$$

$$U(Odoo) = 0.3491* ٠,٣٣٣٣ + 0.1852*0.3333 + 0.1953*0.7500 +$$

$$0.0575*0.7500 + 0.0922* 0.7500 + 0.1207* 0.2500 = \mathbf{0.٤٦٧٠}$$

ويظهر الشكل (٤) القرار النهائي الناتج عن تنفيذ النظرية حيث أن ٠,٥٣٣٠ > ٠,٤٦٧٠ بالتالي يكون النظام SAP وفقاً للنتائج والقيم التي تم اسنادها منذ البداية هو الخيار الأمثل.

الشكل (٤): القرار النهائي

وكما تم الإشارة في الفقرة (3-2-3) يجب التحقق من اتساق القيم المسندة للمعايير في مصفوفة المقارنات الزوجية لذلك يحسب معدل الاتساق وفقا للعلاقتين (٨) (٩)، وبالحساب نجد أن: consistency ratio (CR): 0,0363 < **0.1** **أي أقل من ١٠%**

بالتالي القيم التي تم افتراضها من البداية متّسقة وليست عشوائية ونسبة التناقض فيها تعتبر مقبولة. كذلك المصفوفة متناسقة بشكل جيد وبالتالي الأوزان المستخرجة موثوقة للاستخدام.

وبتطبيق قوانين نظرية المنفعة متعددة السمات المذكورة مسبقاً في الفقرة (٣-٢-٢) تظهر لدينا النتائج الموضحة بالجدول(٦):

الجدول (٦): نتائج توابع طريقة المنفعة متعددة السمات

MAUT functions	SAP	Odoo
WAUF	0.6521	0.4379
WAHUF	2.2840	2.8953

WHUF	0.5023	0.3851

نظراً لأن المعايير ليست مستقلة عن بعضها، يُعتبر التابع الهندسي (WHUF) هو الأكثر ملاءمة لتقييم هذه الحالة. وتشير نتائجه إلى أن نظام SAP هو البديل الأكثر تفضيلاً مقارنةً ب نظام Odoo عند أخذ التفاعل بين المعايير في الحسبان.

حيث حقق نظام SAP منفعة قدرها ٠,٥٠٢٣ بينما نظام Odoo حقق منفعة قدرها 0.3851 مما يشير الى فارق بالمنفعة قدره **30.43%** وهذا يدل على أن نظام SAP مازال البديل الأكثر تفضيلاً، لأن المنفعة الأعلى تعني أن تفاعل المعايير يصب في مصلحة SAP، وهذه النتيجة تساعد في توجيه صناع القرار نحو اختيار نظام SAP .

٤. النتائج والمناقشة:

وفقاً لإحصائيات موقع cvedetails زاد عدد نقاط الضعف في SAP بشكل كبير من عام ٢٠١٤ إلى عام ٢٠٢٤، وبلغ ذروته حوالي عام ٢٠٢٢. وهذا يشير إلى خطر متزايد محتمل او لزيادة الوعي والإبلاغات، ويظهر عامي ٢٠٢٢ و٢٠٢٣ أعلى عدد من نقاط الضعف، حيث تعد XSS وOverflow و Memory Corruption أكثر الأنواع شيوعًا. توجد XSS وMemory Corruption في كل عام تقريبًا، مما يشير إلى وجود ثغرات أمنية مستمرة في هذه المجالات.

بينما يظهر Odoo نمطًا أقل اتساقًا، مع ارتفاعات حادة في عامي ٢٠١٩ و٢٠٢٠، وتعد ثغرات XSS هي الاكثر بروزاً. ويشير العدد الكبير والتنوع في نقاط الضعف في SAP إلى أنها قد تتطلب إدارة أمنية أكثر صرامة مقارنةً بنظامOdoo .

وبناءً على التحليل التفصيلي الذي تم إجراءه لمقارنة أمان نظامي SAP وOdoo تبين أن SAP يتمتع بمستوى أمان أعلى مقارنة بـ Odoo. هذه النتيجة جاءت بناءً على دراسة معمقة لعدد الثغرات الأمنية المسجلة، وتحليل مستويات خطورتها، ومدى قابلية استغلالها، بالإضافة إلى فعالية الاستجابة الأمنية لكل نظام. حيث يشير عدد الثغرات الأمنية الأصغر في Odoo إلى مخاطر أقل، ولكن كل ثغرة أمنية يمكن أن يكون لها تأثير أكثر شدة. كما يشير العدد الأكبر من الثغرات الأمنية في SAP إلى تعرض أعلى، ولكن التوزيع يسمح بتحليل أعمق للمناطق الأكثر عرضة للخطر.

ووفقاً للتحليل الذي تم إجراءه وفقاً للفقرة (٣-٣) تم استنتاج ما يلي:

- لا يأتي Odoo بنفس مستوى ميزات الامتثال والشهادات المضمنة، مما يعني أن الشركات بحاجة إلى تكوينه لتلبية متطلباتها التنظيمية المحددة بالرغم من أن الاتجاهات الأخيرة تشير إلى أن Odoo يشهد تبنيًا متزايدًا وخاصة بين الشركات التي تبحث عن حلول ميسورة التكلفة وقابلة للتخصيص، ويساهم نظامه البيئي المتنامي ودعم المجتمع في شعبيته المتزايدة.
- يوفر Odoo أمانًا كافيًا، خاصة بوجود فريق متخصص في تكنولوجيا المعلومات/الأمان لإدارة التحديثات والتكوينات بنشاط. كما يعتبر فعال في بيئة أقل تعقيدًا وغير خاضعة للتنظيم.

- على الرغم من إمكانية تخصيص Odoo لتحقيق مستوى أمان أعلى، إلا أنه غالبًا ما يتطلب خبرة وموارد إضافية.
- يتفوق SAP من حيث السرية نظرًا لخيارات التشفير الشاملة، وضوابط الوصول وإخفاء البيانات، وآليات التدقيق.
- قد يظل Odoo موثوقًا به للشركات الصغيرة والمتوسطة الحجم، ولكن أداءه قد يكون أكثر تنوعًا بناءً على التنفيذ والاستخدام.
- يُعتبر SAP أكثر أمانًا للمؤسسات الأكبر حجمًا والمعقدة، بينما يوفر Odoo أمانًا قويًا للشركات الصغيرة.

ونظرًا لوجود تباين في نتائج التحليل الأولي باستخدام تقنيات المعالجة اللغوية الطبيعية للتقارير الأمنية، حيث أظهر كل من SAP و Odoo نقاط قوة وضعف متفاوتة في بعض الجوانب، لم يكن من السهل تحديد النظام الأفضل بشكل قاطع. لذلك، تم اللجوء إلى نظرية تحليل القرار متعدد المعايير. وبالنتيجة، أظهرت النظرية تفوق نظام SAP من حيث المنفعة الإجمالية، مما جعله الخيار الأكثر تفضيلاً في هذا التحليل.

٥. الاستنتاجات والتوصيات:

الأمان ليس سمة جوهرية مرتبطة بنوع البرمجيات (مفتوحة المصدر أو مغلقة المصدر)، ولا يمكن الحكم على مستوى الأمان لأي من النوعين بشكل عام دون تحديد منتج بعينه واجراء تحليل أمني دقيق له. وذلك لأن الأمان يعتمد على عدة عوامل متداخلة، منها تصميم المنتج، واستجابة المجتمع أو الشركة المصنعة للثغرات، وممارسات الأمان المتبعة في تطوير وإدارة هذه الأنظمة. مما يستدعي الحذر في التعميم واعتماد تقييمات دقيقة لكل حالة على حدة.

على الرغم من أن النتائج تشير إلى تفوق نظام مغلق المصدر (SAP) في هذه الحالة الدراسية، **ومن الناحية الأمنية وفي الشركات الكبيرة بشكل خاص**، فلا بد من التأكيد على نجاح نظام (Odoo) في الشركات متوسطة الحجم وتزايد عدد مستخدميه في كل عام. كذلك من الضروري عدم تعميم هذه النتيجة على جميع البرمجيات مفتوحة أو مغلقة المصدر، كما ينبغي على المنظمات تقييم متطلباتها المحددة والقيود المفروضة على الميزانية عند الاختيار بين النظامين. وفيما يلي بعض الإرشادات التي يمكن تقديمها للشركات التي تسعى لتبني المصدر المفتوح:

- إدارة المخاطر: حتى بعد اتخاذ قرار التبني، يجب على الشركات الاستمرار في مراقبة المخاطر وتقييم النظام دورياً.
- التدريب ورفع الوعي: خصوصاً فيما يتعلق بأفضل ممارسات الأمان وكيفية التعامل مع التحديات المحتملة.
- مراجعة الدعم المجتمع: من المهم مراجعة مستوى الدعم المتاح من مجتمع المطورين والمستخدمين.
- اعتماد نهج تجريبي قبل التبني الكامل.
- التكامل مع الأنظمة القائمة: يفضل النظر في مدى سهولة تكامل البرمجيات مفتوحة المصدر مع الأنظمة القائمة في الشركة.
- تقييم تكاليف الملكية الشاملة: مثل تكاليف الصيانة، الدعم الفني، التدريب، والتخصيص.

- إجراء تدقيق أمني دوري: ينصح الشركات بإجراء تدقيق أمني منتظم لأنظمتها مفتوحة المصدر.
- فهم الأنواع المختلفة من تراخيص البرمجيات مفتوحة المصدر: حيث تفرض بعض التراخيص متطلبات على إعادة توزيع البرمجيات أو استخدام الكود في مشاريع تجارية.
- التأكد من تراخيص التبعيات (Dependencies): البرمجيات مفتوحة المصدر غالبًا ما تعتمد على مكتبات أخرى مفتوحة المصدر. يجب التأكد من توافق تراخيص تلك التبعيات مع الترخيص الرئيسي للبرمجية ومع سياسة الشركة فيما يتعلق بالتراخيص.

٦. المراجع:

[1] Open Source Initiative. (2006, July 7). *The Open Source Definition*. Last modified February 16, 2024. https://opensource.org/osd.

[٢] Kaspersky. (2024). *Closed-source software (proprietary software)*. Retrieved October 1, 2024, from https://encyclopedia.kaspersky.com/glossary/closed-source/.

[3] Zlaugotne, B., Zihare, L., Balode, L., Kalnbalkite, A., Khabdullin, A., & Blumberga, D. (2020). Multi-Criteria decision analysis methods comparison. Environmental and Climate Technologies, 24(1), 454–471. https://doi.org/10.2478/rtuect-2020-0028

[4] OpenLogic by Perforce. (2024). *2024 State of Open Source Report*. Retrieved October 1, 2024, from https://www.openlogic.com/resources/state-of-open-source-report.

[5] Yaseen, N. M. G., Abd, N. S. A., & Adeeb, N. I. (2020). Critical factors affecting the adoption of open source software in public organizations. Iraqi Journal for Computer Science and Mathematics, 29–37. https://doi.org/10.52866/ijcsm.2020.01.02.005

[6] Silva, D. G., Coutinho, C., & Costa, C. J. (2023). Factors influencing free and open-source software adoption in developing countries—an empirical study. Journal of Open Innovation Technology Market and Complexity, 9(1), 100002. https://doi.org/10.1016/j.joitmc.2023.01.002

[7] Stine, K. , Quinn, S. , Witte, G. and Gardner, R. (2020), Integrating Cybersecurity and Enterprise Risk Management (ERM), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, ,Retrieved from: https://doi.org/10.6028/NIST.IR.8286

[8] Linh, N. D., Hung, P. D., Diep, V. T., & Tung, T. D. (2019). Risk management in projects based on Open-Source software. 2019 8th International Conference on Software and Computer Applications, 32, 178–183. https://doi.org/10.1145/3316615.3316648

[9] 2024 Open Source Security and Risk Analysis Report. (2024). In https://Synopsys.com. Fred Bals. https://www.blackduck.com/blog/open-source-trends-ossra-report.html

[10] Javier Perez. (2024). Https://www.openlogic.com/resources/2023-state-open-source-report: Open source usage, market trends, & analysis. In https://OpenLogic.com. https://www.openlogic.com/resources/state-of-open-source-report

[11] [2023]OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT. (2023). https://synopsys.com. https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html#introMenu

[12] O'Donoghue, E., Reinhold, A. M., & Izurieta, C. (2024). Assessing Security Risks of Software Supply Chains Using Software Bill of Materials. Ieeexplore, 134–140. https://doi.org/10.1109/saner-c62648.2024.00023

[13] Zlaugotne, B., Zihare, L., Balode, L., Kalnbalkite, A., Khabdullin, A., & Blumberga, D. (2020). Multi-Criteria decision analysis methods comparison. Environmental and Climate Technologies, 24(1), 454–471. https://doi.org/10.2478/rtuect-2020-0028

[14] Saaty, T.L. (1987). Principles of the Analytic Hierarchy Process. In: Mumpower, J.L., Renn, O., Phillips, L.D., Uppuluri, V.R.R. (eds) Expert Judgment and Expert Systems. NATO ASI Series, vol 35. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-86679-1_3

[15] Anand, A., Agarwal, M., Aggrawal, D. et al. Successive generation introduction time for high technological products: an analysis based on different multi-attribute utility functions. Environ Dev Sustain (2022). https://doi.org/10.1007/s10668-022-02357-9

[16] Security in Odoo. (n.d.). https://www.odoo.com/. Retrieved October 6, 2024, from https://www.odoo.com/documentation/17.0/developer/reference/backend/security.html

[17] Secure data, applications, and data centers. (n.d.). https://www.sap.com/. Retrieved October 6, 2024, from https://www.sap.com/about/trust-center/security.html

[18] Odoo vs SAP Business One. (n.d.). https://www.odoo.com/. Retrieved October 6, 2024, from https://www.odoo.com/page/odoo-vs-SAP-business-one

[19] Robert Holland. (2023). Cybersecurity Threats to SAP Systems 2023. In https://sapinsider.org/. Retrieved October 6, 2024, from https://sapinsider.org/research-reports/cybersecurity-threats-to-sap-systems/

[20] Souabni, H., Benbrahim, H., & Amine, A. (2022, October). Secure Data Acces in Odoo System. In 2022 8th International Conference on Optimization and Applications (ICOA) (pp. 1-5). IEEE. https://doi.org/10.1109/ICOA55659.2022.9934479