International Journal of Computers and Informatics (IJCI)
Vol. (5), No. (1)
IJCI
January 2026
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (5)، العدد (1)

# نموذج بيزي لتقدير مخاطر الأمن السيبراني بالاعتماد على مصنف Naive Bayes

**هبة لقمان أمين**
مدرس، الكلية التقنية الإدارية، الجامعة التقنية الشمالية، الموصل، العراق
hebaloqmanmaster@ntu.edu.iq

**عدنان مصطفى حسين**
مدرس دكتور، الكلية التقنية الإدارية، الجامعة التقنية الشمالية، الموصل، العراق
adnan_mustafa@ntu.edu.iq

## المستخلص

تناول البحث تحليل بيانات الأمن السيبراني وتفسير العلاقة بين متغيرين الأول يمثل المتغير المعتمد الذي يطلق عليه (مستوى الخطر) والذي يصنف إلى قسمين (عالي ومتوسط) والمتغير المستقل والذي تضمن ثلاثة أنواع من المتغيرات وهي المتغير الأول ويطلق عليه (نوع الهجوم السيبراني) ويشمل ثمانية أنواع رئيسية تم تحديدها استنادًا إلى أكثر التهديدات شيوعًا في مجال الأمن السيبراني، وهي: (هجوم عبر بريد إلكتروني احتيالي، إدخال برامج ضارة عبر مرفق، هجمات حجب الخدمة Distributed Denial of Service (DDOS)، هجوم عبر حقن Structured Query Language (SQL) في الموقع، هجوم حجب الخدمة على الخوادم الرئيسية، رسائل بريد إلكتروني أو اتصال هاتفي لسرقة الحسابات، فيروس ينُشر عبر رابط ضار)، والمتغير الثاني يطلق عليه (تأثير الهجوم) والذي تضمن أربعة أنواع (فقدان البيانات، تعطل البيانات، تعطل الخدمة، تسريب البيانات) والمتغير الثالث يدعى (مستوى الأمن) ويقسم إلى (منخفض، متوسط، عالي) وتم الحصول عليها من خلال تصميم استمارة معلومات وزعت على (175) من متخصصين بالأمن السيبراني وتضمنت أسئلة حول مدى التأثير المتحقق من الاختراقات التي تجتاح قاعدة بيانات الأمن السيبراني وكيفية الحماية منها، وتحليلها باستخدام مصنف بيز من خلال (لغة البرمجة الإحصائية R)، وأظهرت النتائج وجود فروق واضحة في مستوى الخطورة تبعًا لنوع الهجوم.

**الكلمات المفتاحية:** نظرية بيز، مصنف بيز، الأمن السيبراني، لغة البرمجة الإحصائية R.

International Journal of Computers and Informatics (IJCI)
Vol. (5), No. (1)
IJCI
January 2026
المجلة الدولية للحاسبات والمعلوماتية
الإصدار (5)، العدد (1)

# Bayesian model for assessing cybersecurity risks based on Naive Bayes classifier

**Heba Luqman Amin**
Lecturer, Administrative Technical College, Northern Technical University, Mosul, Iraq
hebaloqmanmaster@ntu.edu.iq

**Adnan Mustafa Hussein**
Lecturer, PhD, Administrative Technical College, Northern Technical University, Mosul, Iraq
adnan_mustafa@ntu.edu.iq

## Abstract

The research analyzed cybersecurity data and interpreted the relationship between two variables. The first variable, the dependent variable, is called the "risk level," which is classified into two categories: high and medium. The second variable, the independent variable, comprised three sub-variables. The first sub-variable, called the "type of cyberattack," included eight main types identified based on the most common cybersecurity threats: (phishing email attacks, malware insertion via attachment, Distributed Denial of Service (DDoS) attacks, SQL injection attacks, denial-of-service attacks on main servers, email or phone calls to steal accounts, and viruses spread via malicious links). The second sub-variable, called the "impact of the attack," included four types: (data loss, data disruption, service disruption, and data leakage). The third sub-variable, called the "security level," was divided into (low, medium, and high). These sub-variables were obtained by distributing a questionnaire to 175 cybersecurity professionals, which included questions about the perceived impact of breaches. The study examined cybersecurity database attacks and how to protect against them, analyzing them using a Bayesian classifier and the R statistical programming language. The results showed clear differences in the level of risk depending on the type of attack.

**Keywords:** Bayesian Theory, Bayesian Classifier, Cybersecurity, R Statistical Programming Language.

## 1. المقدمة

تعتبر أبحاث الأمن السيبراني من وجهة نظر رياضية وإحصائية صعبة بسبب التعقيد المستمر للمشاكل وطبيعة البيانات، ونحن نعتقد أنه من أجل أن يكون هناك استعداد ضد التهديدات السيبرانية الحالية، تقدم إحصائيات بيز (Bayesian Statistics) مجموعة واسعة من نماذج مرنة قد تكون المفتاح لفهم أعمق للعملية التي تواجه الهجمات الخبيثة، وفي الوقت نفسه، بالنسبة لنا أن يكون النماذج التنبؤية قادرة على التعامل مع كميات كبيرة من البيانات المتطورة في الوقت الحالي (Perusqu´ıa, Griffin & Villa, 2021, 1-2)

إن التحليل الإحصائي للبيانات مهم جداً في ساحة تحليل البيانات الضخمة للأمن السيبراني يساعد على فهم التهديدات السيبرانية من خلال تصميم استراتيجيات فعالة للتصدي لهذا النوع من التحليل مما يساعد الشركات والمؤسسات في الوصول لقرارات منطقية مبنية على بيانات موثوقة، ومع التطور المتسارع في تكنولوجيا المعلومات والاعتماد المتزايد على الأنظمة الرقمية في مختلف القطاعات أصبحت مخاطر الأمن السيبراني أحد أبرز التحديات التي تواجه المؤسسات والحكومات على حد سواء تتراوح هذه المخاطر بين الهجمات الخبيثة على البيانات والاختراقات الأمنية والتجسس الرقمي وصولاً إلى الابتزاز الإلكتروني مما يستدعي اعتماد أساليب علمية دقيقة للتقييم والتحليل والتنبؤ.

من بين أبرز الأساليب الحديثة التي لاقت اهتماماً متزايداً في هذا المجال تبرز الإحصائيات البيزية كمنهجية قوية ومرنة في تحليل المخاطر، لا سيما في البيئات غير المؤكدة والمعقدة مثل الأمن السيبراني، إذ تقوم النظرية البيزية على تحديث المعرفة الاحتمالية بشكل تراكمي عبر دمج المعرفة السابقة (Prior) مع البيانات الجديدة (Likelihood) للوصول إلى معرفة محدّثة (Posterior) تكون أكثر دقة وواقعية، وتتيح هذه المقاربة تطوير نماذج ديناميكية يمكنها التكيّف مع التغير المستمر في أنماط الهجمات السيبرانية مما يجعلها أداة مثالية لتقدير احتمالية وقوع حادث أمني وتقييم تأثيره المحتمل وتحديد أنسب وسائل الاستجابة والتخفيف.

## 2. هدف البحث

يهدف هذا البحث إلى استخدام الإحصائيات البيزية لتحليل وتقدير مخاطر الأمن السيبراني، وذلك من خلال تقدير احتمالية وقوع الهجمات السيبرانية وتحديد حجم تأثيرها على الأنظمة الرقمية باستخدام منهجية الإحصاء البيزي التي تسمح بدمج المعرفة السابقة مع البيانات الحديثة لتقديم نتائج دقيقة تدعم اتخاذ القرار الأمني.

## 3. الدراسات السابقة

شهد موضوع الأمن السيبراني اهتمامًا متزايدًا في العقود الأخيرة، لا سيما مع تنامي التهديدات الرقمية وتوسع استخدام التكنولوجيا، وفيما يلي سوف نستعرض أبرز الدراسات التي تناولت هذا الموضوع:

- في عام (2009) استخدموا الباحثين (Mo, Belling) منهجية شبكة بيز ( Bayesian Network-based model) لاقتراح نموذجاً كمياً لتقييم مخاطر الأمن السيبراني في مجال أمن المعلومات والذي يعتمد على بيانات الشركة الأمنية وإحصاءات خرق البيانات كمدخلات، مع توضيح آلية التقييم بناءً على مجموعة من المعايير مثل معيار تحليل خرق البيانات (ISO/IEC 27002).
- في عام (2017) استخدموا كل من الباحثين (Huang, Zhou, Tian, Tu, and Peng) الشبكات البيزية لبناء نموذج ديناميكي وكمي في تقييم مخاطر الأمن السيبراني تم تطبيقه على بيانات شبكات (Supervisory control and data acquisition (SCADA)) التابعة للأنظمة الصناعية مع دمج أنظمة الأمان التقليدية القائمة على شبكات بيز باستخدام بوابة (Leaky Noisy-OR (LNOR)) لدعم تقييم المخاطر للهجمات غير المعروفة، واستخدام تقنيات التعلم الآلي لتقدير معلمات النموذج من البيانات من أجل توليد أكثر دقة لقيمة المخاطر.
- في عام (2019) قدم كل من الباحثين (Wang, Neil, and Fenton) مقارنة بين نتائج كل من نموذج تحليل عامل خطر المعلومات (Factor Analysis of Information Risk (FAIR)) وتحليل عامل خطر المعلومات باستخدام الشبكات البيزية ( Factor Analysis of Information Risk- Bayesian Networks (FAIR-BN)) مع عدد كبير من العينات الناتجة باستخدام تحليل عامل خطر المعلومات بمحاكاة مونت كارلو (Factor Analysis of Information Risk- Monte Carlo (FAIR-MC)) وكانت نتائج (FAIR) و (FAIR-BN) أكثر ملائمة مقارنة بـ (FAIR-MC)، ويحقق نموذج (FAIR-BN) دقة أعلى في العديد من الحالات التي لا يمكن نمذجتها بدقة بواسطة نموذج (FAIR)، وكذلك يقدم نموذج (FAIR-BN) نتائج أكثر دقة في حالة الذيل الطويل (long tail).
- في عام (2021) طبقوا الباحثين (Perusqu´ıa, Griffin, and Villa) نماذج بيزية للكشف عن مشاكل الشذوذ في الأمن السيبراني.
- في عام (2022) اقترحوا الباحثين (Zebrowski, Vieira, and Mancuso) نموذج كمي باستخدام شبكة بيز ((Bayesian network (BN) لتحليل التهديدات السيبرانية للأنظمة الفيزيائية تم تطبيقه على شبكات الطاقة الكهربائية.
- في عام (2023) استخدموا هؤلاء الباحثين (Purushottam, Kumar, Satonkar, Gaikwad,

(Probabilistic risk الأساليب البيزية في تقييم المخاطر الاحتمالية Sonawane, and Shirwadkar) assessment (PRA) في مجال القرصنة باستخدام الدوال الاحتمالية والتوزيعات اللاحقة والاحتمالات السابقة لتحديث تنبؤات المخاطر مع ظهور معلومات جديدة، وباستخدام النمذجة الإحصائية لدراسة الترابط بين المخاطر ونقاط الضعف الإلكترونية المختلفة مما يساعد الشركات تحديد أفضل طريقة لإيقافها.

## 4. نظرية بيز ومصنف بيز:

تُعد نظرية بيز ذات أهمية جوهرية في الإحصاء الاستدلالي وهو منهج منطقي لتحديث احتمالية الفرضيات، وكان القس توماس بيز (Thomas Bayes) أول من اكتشف النظرية التي تحمل اسمه. وقد دوّنها في ورقة بحثية بعنوان "مقال نحو حل مسألة في عقيدة الاحتمالات". وُجدت هذه الورقة بعد وفاته على يد صديقه ريتشارد برايس (Richard Price)، الذي نشرها بعد وفاته في مجلة "المعاملات الفلسفية للجمعية الملكية" عام (1763). أوضح بيز كيفية استخدام الاحتمال العكسي لحساب احتمال وقوع الأحداث السابقة من وقوع الحدث اللاحق. تبنى لابلاس (Laplace) وعلماء آخرون أساليبه في القرن التاسع عشر، لكنها تراجعت بشكل كبير بحلول أوائل القرن العشرين، وبحلول منتصف القرن العشرين تجدد الاهتمام بالأساليب البيزية على يد دي فينيتي وجيفريز وسافاج وليندلي (De Finetti, Jeffreys, Savage, and Lindley) وعلماء آخرون. وقد طوروا طريقة متكاملة للاستدلال الإحصائي تستند إلى نظرية بيز (Bolstad, 2007, 6).

لاشتقاق مبرهنة بيز، لكل حدثين A وB في فضاء العينة وعملية التقاطع بينهما تتميز بخاصية التبادل في الاحتمال المشترك أي أن احتمال وقوع الحدثين معاً لا يتغير باستبدال ترتيب الأحداث وتكتب بالشكل التالي:

(Downey, 2012, 3-4) -

$$P(A \; and \; B) = P(B \; and \; A) \qquad (1)$$

وصيغة احتمال التقاطع بين الحدثين هي:

$$P(A \; and \; B) = P(A)\, P(B \,/\, A) \qquad (2)$$

ويمكن إعادة كتابة الصيغة (2) بشكل آخر كون الحدثين قابلان للتبادل كما يلي:

$$P(B \; and \; A) = P(B)\, P(A \,/\, B) \qquad (3)$$

بتعويض المعادلتين (2) و (3) في المعادلة (1) نحصل على:

$$P(B)\, P(A \,/\, B) = P(A)\, P(B \,/\, A) \qquad (4)$$

وأخيراً بقسمة طرفي المعادلة على $\mathbf{P(B)}$ (بشرط $\mathbf{P(B) \neq 0}$) لنحصل على الصيغة التالية:

$$P(A / B) = \frac{P(B / A)P(A)}{P(B)} \quad (5)$$

تمثل المعادلة (5) (مبرهنة بيز) التي قد تبدو معادلة بسيطة في شكلها الرياضي، لكنها في الواقع تتمتع بقوة تحليلية كبيرة، إذ تُعد من الأدوات الأساسية في الإحصاء الاستدلالي، وتُستخدم على نطاق واسع في مجالات متعددة مثل الذكاء الاصطناعي، والطب، وتحليل المخاطر، والأمن السيبراني، وغيرها.

بينما لبناء نماذج الاحتمالية البيزية باستخدام معادلة مصنف بيز من خلال تحديد الاحتمالات الفئوية اللاحقة للحالات$P(Y = y_j|X = x_i)$، ويتم ذلك بتطبيق نظرية بيز في المعادلة (5) للحالات نحصل على (Berrar, 2018, 7-8):

$$P(y_j|x_i) = \frac{P(x_i|y_j)P(y_j)}{P(x_i)} \quad (6)$$

نلاحظ البسط يمثل الاحتمال المشترك بين $x_i$ و $y_j$ يمكن إعادة كتابة البسط وسوف نستخدم x فقط مع حذف i للتبسيط بالشكل التالي:

$$\begin{aligned} P(X|y_j)P(y_j) &= P(X, y_j) \\ &= P(x_1, x_2, \dots, x_p, y_j) \\ &= P(x_1|x_2, x_3, \dots, x_p, y_j)P(x_2, x_3, \dots, x_p, y_j) \\ &= P(x_1|x_2, x_3, \dots, x_p, y_j)P(x_2|x_3, x_4, \dots, x_p, y_j)P(x_3, x_4, \dots, x_p, y_j) \\ &= P(x_1|x_2, x_3, \dots, x_p, y_j)P(x_2|x_3, x_4, \dots, x_p, y_j) \dots P(x_p|y_j)P(y_j) \quad (7) \end{aligned}$$

بما أن قيم $x_i$ مستقلة عن بعضها وأن $P(x_1|x_2, x_3, \dots, x_p, y_j) = P(x_1|y_j)$ إذن يمكن تبسيط معادلة (7) التي تمثل الاحتمال المشترك بين $X$ و $y_j$ بالشكل التالي:

$$\begin{aligned} P(X|y_j)P(y_j) &= P(x_1|y_j).P(x_2|y_j) \dots P(x_p|y_j)P(y_j) \\ &= \prod_{i=1}^{p} P(x_i|y_j)P(y_j) \quad (8) \end{aligned}$$

وبتعويض معادلة (8) في المعادلة (6) سوف نحصل على:

$$P(y_j|X) = \frac{\prod_{i=1}^{p} P(x_i|y_j)P(y_j)}{P(X)} \quad (9)$$

نلاحظ أن المقام $P(X)$ لا يعتمد على التصنيف حيث يمثل كعامل قياس ويؤكد ذلك الاحتمال اللاحق $P(y_j|X)$، ولأجل إثبات قاعدة التصنيف الواضحة هي القاعدة التي تخصص كل حالة لتصنيف واحدة فقط وذلك يكون من خلال حساب قيمة البسط لكل تصنيف ونختار التصنيف التي تكون قيمته القيمة القصوى وتسمى هذه القاعدة قاعدة الاحتمال اللاحق الأقصى، ونتيجة التصنيف تعرف أيضاً بالتصنيف اللاحق الأعظم (Maximum a posteriori(MAP)) ويتم حسابها كـ $(\hat{y})$ للحالة $X$ على النحو التالي:

$$\hat{y} = arg\max_{y_j} \prod_{i=1}^{p} P(x_i|y_j)P(y_j) \qquad (10)$$

وبتطبيق نظرية الاحتمال الكلي التي تمثل:

$$P(X) = P(X|y)P(y) + P(X|y^c)P(y^c) \qquad (11)$$

حيث أن $y^c$: هو متتم الحدث وهو الحدث الذي لا يقع في $y$ .

وبالتعويض في المعادلة (9) فتصبح معادلة مصنف بيز بالشكل التالي:

$$P(y_j|X) = \frac{\prod_{i=1}^{p} P(x_i|y_j)P(y_j)}{\prod_{i=1}^{p} P(x_i|y_j)P(y_j) + \prod_{i=1}^{p} P(x_i|{y_j}^c)P({y_j}^c)} \qquad (12)$$

## 5. مفهوم الأمن السيبراني:

الأمن السيبراني: هو مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة المصممة لحماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الرقمية أو الضرر بها أو الوصول غير المصرح لها لضمان سرية المعلومات، والأمن السيبراني يهتم بأمن كل ما هو موجود على الفضاء الإلكتروني بالإضافة إلى أمن المعلومات مثل الأنظمة والبرامج المتصلة بالإنترنت (حسين، 2023، 3-4).

يتعلق مفهوم الأمن السيبراني بضمان سلامة استخدام الإنترنت، حيث يشير إلى مجموعة من الأنشطة والتدابير، سواء كانت تقنية أو غير تقنية، التي تهدف إلى حماية البيئة الافتراضية والبيانات المحتومة فيها من جميع التهديدات المحتملة، ويعرف الأمن السيبراني على أنه الجهود المبذولة لضمان أمان الشبكات والأنظمة المعلوماتية للمؤسسات، وذلك نظرًا لاعتماد هذه المؤسسات على رقمنة هياكلها لتسهيل التفاعل بين المؤسسة وموردها البشري، باستخدام الأجهزة الحاسوبية المتصلة بالإنترنت (عبد الرزاق، 2023، 3).

إن الهدف من إدارة المخاطر الأمن السيبراني هو تحديد العوامل التي تعرض المعلومات للخطر أو للتعطيل

عن عملها وللقضاء عليها يتم من خلال تطبيق تدابير أمنية تتوافق مع قدرة المنظمة على تحمل المخاطر، وفي مجال الأمن السيبراني يعرف الخطر بأنه احتمال وقوع حدث سلبي وبالتالي يشمل الخطر معيارين رئيسيين: احتمال وقوع الحدث فعلياً وتأثيره والذي يمكن تقييمه بناءً على خطورته المحتملة.

رياضياً يمكن التعبير عن الخطر بأنه انحراف أو اختلاف عن النتيجة المتوقعة لهذا السبب قد تفضل الاستثمارات عالية المخاطر في الأسواق المالية على الاستثمارات منخفضة المخاطر نظراً لوجود فرصة لتحقيق عوائد مرتفعة جداً على الأقل، ومع ذلك في مجال أمن الحاسوب عادة من الضروري تهيئة بيئة ذات مستوى منخفض الخطورة من أجل تقليل التهديدات والأضرار المحتملة والناجمة عنها بشكل فعال.

ويوضح تقرير (المخاطر العالمية لعام 2023) الذي أعده المنتدى الاقتصادي العالمي عن تصنيف المخاطر العالمية بحسب شدتها على المدى القصير (حتى عامين) والمدى الطويل (عشر سنوات) تشمل عدة مجالات من بينها القطاع التكنولوجي وبشكل خاص احتلت (انتشار الجرائم الإلكترونية ونقص الأمن السيبراني) المرتبة الثامنة وكما يشير التقرير إلى أن التقنيات ستؤدي إلى تفاقم التفاوت الرقمي بينما ستظل المخاطر المرتبطة بالأمن السيبراني مشكلة مستمرة، وستسهم المساعدات الحكومية في ضمان معدلات عالية من التطوير والبحث في التقنيات الجديدة خلال العقد القادم، مع التركيز على مجالات مثل الذكاء الاصطناعي، والحوسبة الكمومية، والتقنيات الحيوية (Ohrimenco, Valeriu, 2024, 149).

## 6. الجانب التطبيقي

**وصف المتغيرات:**

تم إعداد استمارة معلومات تضمنت أسئلة حول الأمن السيبراني وزعت على (175) من متخصصين بالأمن السيبراني، ومتغيرات الدراسة التي تمثل كل من المتغير المعتمد (Y) هو مستوى الخطر (متوسط (1)، عالي (2)) واختير عدد من المتغيرات المستقلة وكما يأتي:

نوع الهجوم (X1): ويتضمن عدة أنواع وهي:

- هجوم عبر بريد إلكتروني احتيالي (1).
- إدخال برامج ضارة عبر مرفق (2).
- هجمات DDOS (3).
- اختراق قاعدة البيانات (4).
- هجوم عبر حقن SQL في الموقع (5).

- هجوم حجب الخدمة على الخوادم الرئيسية (6).
- رسائل بريد إلكتروني أو اتصال هاتفي لسرقة الحسابات (7).
- فيروس ينشر عبر رابط ضار (8).

تأثير الهجوم (X2): ويتضمن عدة تأثيرات وهي:

- فقدان البيانات (1).
- تعطل البيانات (2).
- تعطل الخدمة (3).
- تسريب البيانات (4).

مستوى الأمن (X3): ويتضمن عدة مستويات وهي:

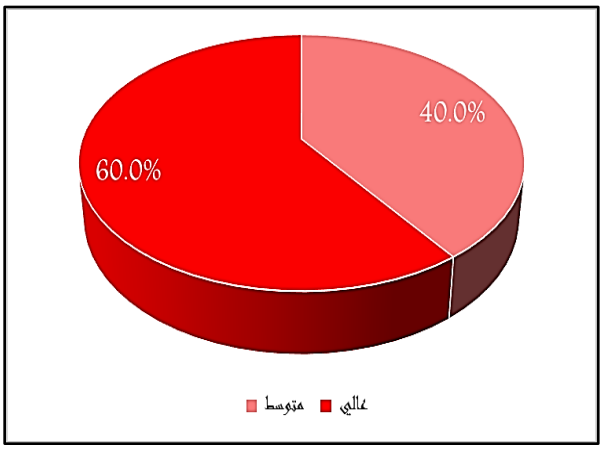
- منخفض (1).
- متوسط (2).
- عالي (3).

**وصف البيانات:**

إن البيانات التي استخدمت في هذا البحث تتكون من (175) إجابة عن أسئلة وضعت في تفسير مخاطر الأمن السيبراني، وقد تم تقسيمها إلى بيانات تدريب (Training) بنسبة 70% من البيانات بواقع 123 مفردة وبيانات اختبار (Testing) بنسبة 30% بواقع 52 مفردة، والجداول (1) و(2) و(3) تمثل أصناف مستويات الخطر للبيانات الكلية وبيانات التدريب وبيانات الاختبار على التوالي. والغرض من التقسيم هو لمنع overfitting ولتقييم أداء النموذج على بيانات جديدة غير مشاهدة.

جدول (1): الجدول التكراري لفئات مستويات الخطر الكلية

| الفئات | التكرار | النسبة |
|---|---|---|
| متوسط | 70 | %40 |
| عالي | 105 | %60 |
| المجموع | 175 | %100 |

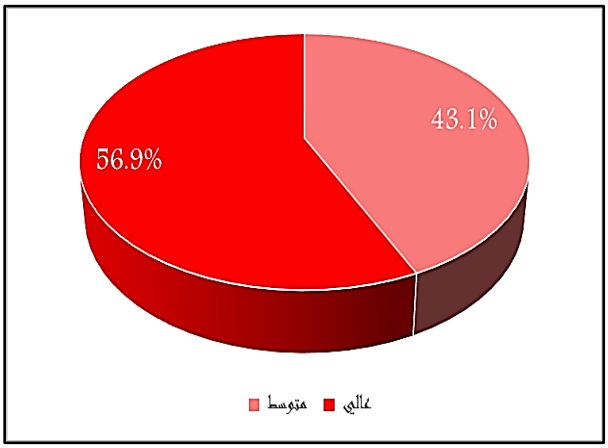



شكل (1): نسب فئات مستويات الخطر الكلية

يظهر الجدول (2) والشكل (1) توزيع عينات مستويات الخطر إلى فئتين: (متوسط) و(عالي)، ويتضح أن النسبة الأكبر تقع ضمن الفئة عالي بنسبة 60% (105 حالة)، بينما تقع 40% (70 حالة) ضمن الفئة متوسط. ورغم أن هذا الاختلاف في التوزيع ليس شديد التطرف، إلا أنه يوضح وجود عدم توازن نسبي في الفئات (Class Imbalance)، وهو أمر ينبغي أخذه في الاعتبار عند بناء نماذج التصنيف.

جدول (2): الجدول التكراري لفئات مستويات الخطر لبيانات التدريب

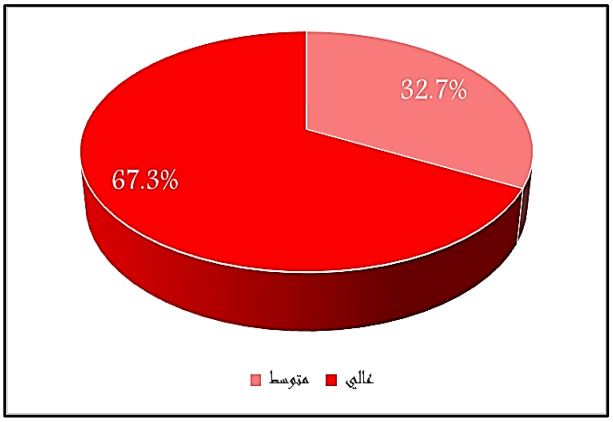
| الفئات | التكرار | النسبة |
|---|---|---|
| متوسط | 53 | %43.1 |
| عالي | 70 | %56.9 |
| المجموع | 123 | %100 |




شكل (2): نسب فئات مستويات الخطر لبيانات التدريب

جدول (3): الجدول التكراري لفئات مستويات الخطر لبيانات الاختبار

| الفئات | التكرار | النسبة |
|---|---|---|
| متوسط | 17 | %32.7 |
| عالي | 35 | %67.3 |
| المجموع | 52 | %100 |




شكل (3): نسب فئات مستويات الخطر لبيانات الاختبار

يتضح من الجداول (2) و(3) الخاصة ببيانات التدريب والاختبار أن نسب الفئات (متوسط وعالي) بقيت متقاربة جداً مع نسبها في البيانات الكلية (الجدول 1). فقد كانت نسبة الفئة متوسط في البيانات الكلية 40%، وفي بيانات التدريب 43.1%، وفي بيانات الاختبار 32.7%. وبالمثل، كانت نسبة الفئة عالي في البيانات الكلية 60%، وفي التدريب 56.9%، وفي الاختبار 67.3%. يشير ذلك إلى أنه تم إجراء عملية التقسيم باستخدام أسلوب يحافظ على التمثيل النسبي للفئات (Stratified Sampling)، مما يضمن أن نموذج التصنيف يتعلم ويختبر ضمن توزيع مشابه للتوزيع الأصلي للبيانات. وتُعد هذه الخطوة مهمة للغاية في حالات عدم توازن الفئات (Class Imbalance)، لأنها تمنع تحيز النموذج لصالح الفئة الأكبر، وتوفر تقييماً أكثر عدالة وموثوقية في كل من بيانات التدريب والاختبار.

**نتائج التحليل:**

تم تطبيق مصنف بيز (Naive Bayes Classifier) على بيانات مستويات الخطر باستخدام دالة (naiveBayes) في حزمة (e1071) ضمن بيئة لغة R، وذلك ضمن ثلاثة سيناريوهات تحليلية تهدف إلى تقييم أداء الطريقة بشكل شامل وتحت ظروف مختلفة:

**السيناريو الأول – البيانات الكلية (Full Data):**

في هذا السيناريو تم بناء النموذج باستخدام كامل البيانات المتاحة دون فصلها إلى تدريب واختبار. ويتيح هذا السيناريو فهماً أولياً لأداء النموذج عندما تتوفر له كل المعلومات، لكنه لا يعكس القدرة الحقيقية على التعميم.

**السيناريو الثاني – بيانات التدريب (Training Data):**

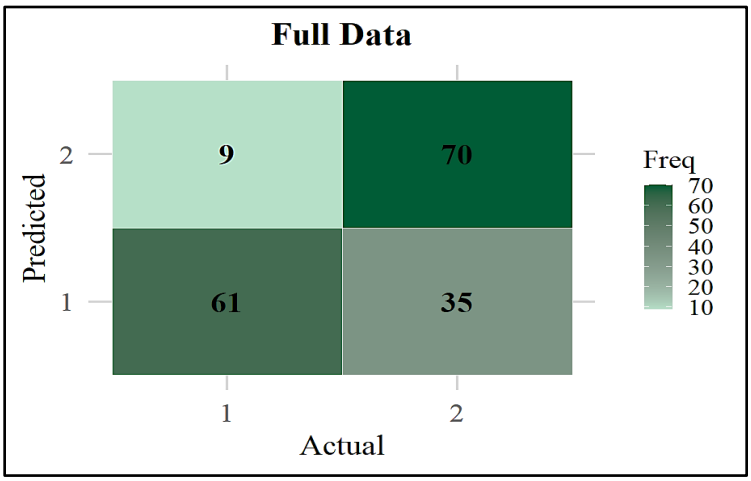
في هذا السيناريو جرى تقسيم البيانات بطريقة طبقية (Stratified Sampling) للحفاظ على نسب الفئات، وتم استخدام جزء من البيانات لبناء نموذج بيز، ويهدف هذا السيناريو إلى تقييم استقرار التقدير عند توفر جزء محدود من البيانات فقط.

**السيناريو الثالث – بيانات الاختبار (Testing Data):**

يعتمد هذا السيناريو على النموذج المدرب في السيناريو الثاني من أجل التنبؤ بفئات بيانات الاختبار غير المشاهدة اعتبارها خارج العينة. ويعد هذا السيناريو الأكثر واقعية، لأنه يقيس قدرة النموذج على التنبؤ وتعميم المعرفة على بيانات جديدة.

تسمح هذه السيناريوهات الثلاثة بإجراء تقييم لأداء مصنف بيز في ظروف متنوعة، بدءاً من الأداء الداخلي للنموذج وصولاً إلى القدرة التنبؤية الفعلية. وقد تم اعتماد مجموعة من مقاييس التقييم الإحصائية لتقييم أداء هذا المصنف، شملت: الدقة (Accuracy)، والدقة الإيجابية (Precision)، ومعامل الاستدعاء (Recall)، والنوعية (Specificity)، ودرجة الاتساق F1-Score، والدقة المتوازنة (Balanced Accuracy)، إضافة إلى مؤشري كابا (Kappa) ومعامل ارتباط ماثيوز (MCC) Matthews Correlation Coefficient.

وفيما يخص السيناريو الأول، فإن نتائج مصفوفة الالتباس (Confusion Matrix) معرفة كما في الشكل (4)، وكما أن معايير المقارنة معرفة كما في الجدول (4).




شكل (4): مصفوفة الالتباس للبيانات الكلية

يظهر تحليل مصفوفة الالتباس الخاصة بجميع البيانات (Full Data) قدرة مصنف بيز على التمييز بين فئتي مستوى الخطر متوسط (1) وعالي (2) بدرجة متفاوتة. إذ توضح النتائج أن النموذج تمكن من تصنيف 70 حالة من أصل 105 حالة تنتمي فعلياً إلى الفئة عالي بشكل صحيح، بينما قام بتصنيف 35 حالة منها على أنها متوسط، مما يشير إلى وجود نسبة من الأخطاء في التعرف على الحالات ذات مستوى الخطر العالي. وبالمقابل، نجح النموذج في تصنيف 61 حالة من أصل 70 حالة تنتمي فعلياً إلى الفئة متوسط بشكل صحيح، بينما تم تصنيف 9 حالات ضمن هذه الفئة بشكل خاطئ على أنها عالي. وبصورة عامة، يمكن القول إن النموذج يميل بدرجة أكبر إلى التعرف على الفئة متوسط مقارنة بقدرته على التعرف على الفئة عالي، مما قد يكون مرتبطاً بتداخل خصائص بعض الهجمات أو تأثير عدم التوازن النسبي في توزيع الفئات داخل البيانات الأصلية. وتعد هذه النتائج خطوة أولية مهمة لفهم أداء النموذج في تصنيف مستويات الخطر، على أن يتم تقييمه بشكل أدق باستخدام بيانات التدريب والاختبار ومقاييس أداء إضافية مثل الحساسية والدقة والـ F1-score وغيرها، وكما في الجدول الآتي:

جدول (4): مقاييس تقييم الأداء للبيانات الكلية

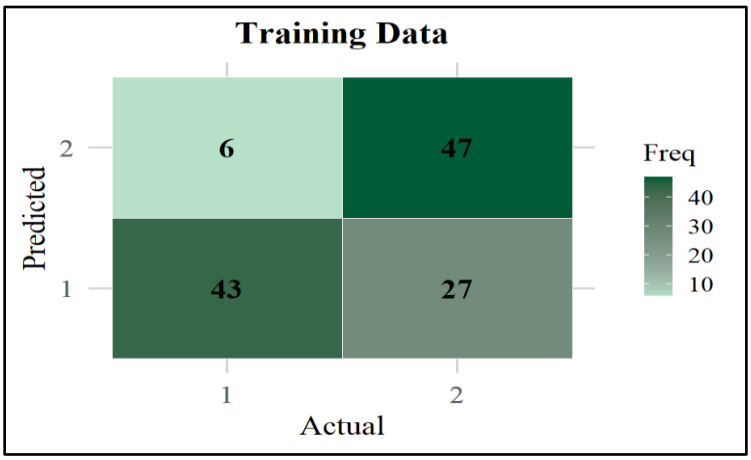
| Metrics | Bayes Classifier |
|---|---|
| Accuracy | 0.7486 |
| Precision | 0.8861 |
| Recall | 0.6667 |
| Specificity | 0.8714 |
| F1-Score | 0.7609 |
| Balanced Accuracy | 0.7690 |
| Kappa | 0.5067 |
| MCC | 0.5297 |
| AUC | 0.7573 |

يوضح جدول (4) مقاييس تقييم الأداء الخاصة بمصنف بيز عند تطبيقه على البيانات الكلية، حيث حقق النموذج دقة تصنيف عامة (Accuracy) بلغت 74.86%، مما يشير إلى أن ما يقرب من ثلاثة أرباع الحالات قد جرى تصنيفها بشكل صحيح. أما من حيث التمييز بين الفئتين، فقد كانت قيمة الدقة الإيجابية (Precision) التي بلغت (88.61%) وهي مرتفعة نسبياً، وهو ما يدل على قدرة النموذج على تقليل معدلات الإنذارات الخاطئة عند التنبؤ بالفئة عالي، في حين بلغت الحساسية (Recall) قيمة أقل (66.67%)، مما يشير إلى وجود نسبة من الحالات الفعلية عالي لم يتم التعرف عليها بالشكل المطلوب. وبالمقابل، حققت النوعية (Specificity) قيمة مرتفعة (87.14%)، مما يعكس قدرة جيدة للنموذج على تمييز الحالات متوسط بصورة صحيحة. وتبين قيمة (F1-Score) والتي تساوي (0.7609) وجود توازن مقبول بين الدقة والحساسية، وإن كان الأداء لا يزال منحازاً نسبياً نحو تقليل الأخطاء في الفئة الإيجابية أكثر من القدرة على التقاطها جميعاً.

وتعزز قيمة (0.7690) Balanced Accuracy من تفسير الأداء، إذ تعكس متوسط الحساسية والنوعية، وتوضح قدرة أكثر عدلاً للنموذج عند التعامل مع توزيع الفئات غير المتوازن. كما تظهر قيمتا Kappa التي تساوي (0.5067) وMCC التي تساوي (0.5297) أن هناك مستوى متوسطاً من الاتفاق الحقيقي بين التوقعات والواقع، بما يشير إلى أداء مستقر لكنه ليس مثالياً في تمييز الفئتين. وأخيراً، تظهر مساحة تحت منحنى ROC (AUC = 0.7573) أن النموذج يمتلك قدرة جيدة على الفصل بين الفئات بشكل احتمالي، وأن أداءه يتجاوز الأداء العشوائي بدرجة واضحة، مع وجود مجال لتحسين الحساسية عند التنبؤ بالحالات ذات الخطر العالي.

وبصورة عامة، يمكن القول إن أداء مصنف بيز على البيانات الكلية يُعد مقبولاً وجيداً نسبياً في التنبؤ بمستويات الخطر، مع وجود اتجاه واضح نحو تحقيق أداء أفضل في تمييز الفئة متوسط مقارنة بالفئة عالي. ويمثل هذا الجدول نقطة انطلاق مناسبة للمقارنة مع نتائج بيانات التدريب والاختبار، ولتقييم مدى قدرة النموذج على التعميم عند التعامل مع بيانات جديدة.

أما بخصوص السيناريو الثاني، فأن نتائج مصفوفة الالتباس معرفة كما في الشكل (5)، وكما أن معايير المقارنة معرفة كما في الجدول (5).




شكل (5): مصفوفة الالتباس لبيانات التدريب

توضح مصفوفة الالتباس الخاصة ببيانات التدريب قدرة مصنف بيز على التعرف على الفئتين متوسط (1) وعالي (2) بدرجة مقبولة، مع وجود حالات التباس بين الفئتين. فقد نجح النموذج في تصنيف معظم الحالات ذات مستوى الخطر المتوسط بصورة صحيحة، حيث تم التعرف على 43 حالة من أصل 49 حالة تنتمي فعلياً إلى الفئة متوسط، في حين جرى تصنيف 6 حالات بشكل خاطئ ضمن الفئة عالي. وبالمقابل، استطاع النموذج التعرف بصورة صحيحة على 47 حالة من أصل 74 حالة تنتمي فعلياً إلى الفئة عالي، بينما جرى تصنيف 27 حالة ضمن هذه الفئة على أنها متوسط. وتشير هذه النتائج إلى أن النموذج يحتفظ بقدرة تصنيفية أعلى للحالات متوسط مقارنة بالحالات عالي، بالرغم من تدريبه على البيانات ذاتها، مما قد يعكس تداخلاً في خصائص الحوادث أو تأثيراً ناتجاً عن توزيع المتغيرات التفسيرية في العينة. وبصورة عامة، تعد هذه النتائج مؤشراً أولياً على أداء النموذج قبل اختباره على بيانات غير مشاهدة، كما أنها تساهم في الكشف عن مدى اتساق النموذج مع البيانات المستخدمة في التدريب ومدى احتمالية ظهور الأخطاء التصنيفية عند الانتقال إلى بيانات جديدة. والجدول الآتي يوضح نتائج مقاييس تقييم الأداء لبيانات التدريب:

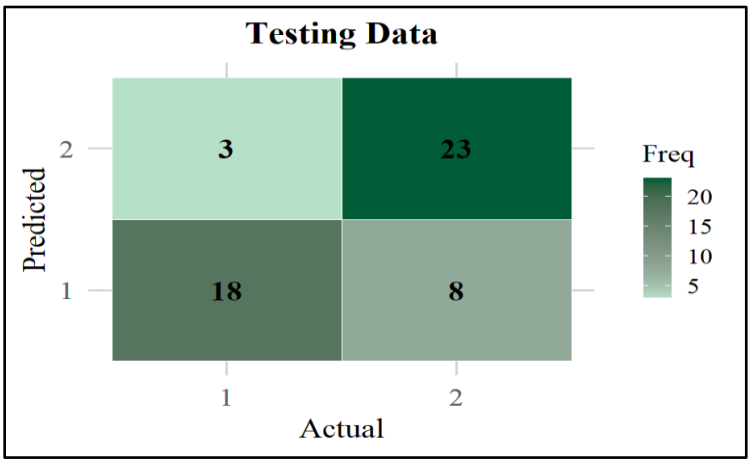
جدول (5): مقاييس تقييم الأداء لبيانات التدريب

| Metrics | Bayes Classifier |
|---|---|
| Accuracy | 0.7317 |
| Precision | 0.8868 |
| Recall | 0.6351 |
| Specificity | 0.8776 |
| F1-Score | 0.7402 |
| Balanced Accuracy | 0.7563 |
| Kappa | 0.4781 |
| MCC | 0.5068 |
| AUC | 0.7144 |

يوضح جدول (5) مقاييس تقييم الأداء الخاصة بمصنف بيز عند تطبيقه على بيانات التدريب، حيث حقق النموذج دقة تصنيف عامة (Accuracy) بلغت 73.17%، وهي قيمة قريبة نسبياً من دقة البيانات الكلية، مما يشير إلى قدرة النموذج على الاحتفاظ بجزء كبير من أنماط التصنيف ضمن البيانات التي تم التعلم منها. وقد بلغت الدقة الإيجابية (Precision) قيمة مرتفعة (88.68%)، مما يدل على قدرة النموذج على تجنب تصنيف الحالات متوسط بشكل خاطئ على أنها عالي، وبالتالي تقليل الإنذارات الكاذبة عند التنبؤ بفئة الخطر العالي. أما الحساسية (Recall) فكانت قيمتها (63.51%) وهي أقل مقارنة بالدقة الإيجابية، وهو ما يعكس استمرار وجود نسبة من الحالات عالي التي لم يتم التعرف عليها بصورة صحيحة، مما يشير إلى محدودية نسبية في قدرة النموذج على التقاط جميع الحالات ذات مستوى الخطر العالي خلال التدريب. وبالمقابل، تظهر النوعية (Specificity) قدرة جيدة للنموذج على التعرف على الحالات متوسط بصورة صحيحة فكانت قيمتها (87.76%)، في حين تعكس قيمة F1-Score التي بلغت (0.7402) توازناً مقبولاً بين الدقة والحساسية، وإن كان الأداء يميل — كما في البيانات الكلية — إلى تقليل الأخطاء الإيجابية أكثر من التقاط جميع الحالات الحقيقية ذات الخطر العالي. وتعزز قيمة Balanced Accuracy (0.7563) هذا التفسير، إذ تجمع بين الحساسية والنوعية وتعكس أداءً متوازناً نسبياً رغم عدم توازن الفئات. أما مؤشرا Kappa التي تساوي (0.4781) وMCC التي تساوي (0.5068) فيشير كلاهما إلى وجود اتفاق متوسط بين القيم الحقيقية والمتوقعة مع وجود نسبة من الالتباس، مما يدل على أداء مستقر لكنه لا يخلو من جوانب للتحسين، بينما تظهر مساحة تحت منحنى ROC (AUC = 0.7144) قدرة تصنيفية جيدة وإيجابية تفوق الأداء العشوائي بوضوح، مع بقاء مجال لتعزيز الحساسية في المستقبل.

وبصورة عامة، تبين هذه النتائج أن أداء مصنف بيز على بيانات التدريب مقبول وجيد نسبياً، وأن النموذج تعلم الأنماط الأساسية للتمييز بين الفئتين مع استمرار صعوبة نسبية في التعرف الكامل على الحالات عالية الخطر. وتمثل هذه النتائج أساساً لمقارنة أداء النموذج مع بيانات الاختبار، بهدف تقييم مدى استقرار قدرته التنبؤية عند تطبيقه على بيانات جديدة غير مستخدمة في التدريب.

وبالنسبة للسيناريو الثالث، فإن نتائج مصفوفة الالتباس معرفة كما في الشكل (6)، وكما أن معايير المقارنة معرفة كما في الجدول (6).




شكل (6): مصفوفة الالتباس لبيانات الاختبار

تظهر مصفوفة الالتباس الخاصة ببيانات الاختبار — وهي بيانات لم تستخدم أثناء تدريب النموذج — قدرة مصنف بيز على التمييز بين فئتي مستوى الخطر متوسط (1) وعالي (2)، مع ملاحظة استمرار وجود حالات التباس بين الفئتين. فقد تمكن النموذج من تصنيف 18 حالة من أصل 26 حالة تنتمي فعلياً إلى الفئة متوسط بصورة صحيحة، في حين جرى تصنيف 8 حالات ضمن هذه الفئة على أنها عالي. وفي المقابل، نجح النموذج في التعرف على 23 حالة من أصل 26 حالة تنتمي فعلياً إلى الفئة عالي، بينما تم تصنيف 3 حالات فقط منها بشكل خاطئ ضمن الفئة متوسط. وتشير هذه النتائج إلى أن النموذج حقق أداءً تصنيفياً أفضل نسبياً في التعرف على الحالات ذات مستوى الخطر عالي مقارنة بالحالات متوسط في مرحلة الاختبار، وهو ما قد يعكس تحسن قدرة النموذج على التمييز بين الفئتين عند التعامل مع بيانات جديدة غير مشاهدة سابقاً. كما تعد هذه النتائج مؤشراً مهماً على قابلية النموذج للتعميم، حيث تظهر قدرة مقبولة على الاحتفاظ بأنماط التصنيف المكتسبة أثناء التدريب عند تطبيقها على بيانات خارجية، الأمر الذي يعزز من موثوقية أداء النموذج في سياقات تطبيقية مستقبلية. والجدول الآتي يوضح نتائج مقاييس تقييم الأداء لبيانات التدريب:

جدول (6): مقاييس تقييم الأداء لبيانات الاختبار

| Metrics | Bayes Classifier |
|---|---|
| Accuracy | 0.7885 |
| Precision | 0.8846 |
| Recall | 0.7419 |
| Specificity | 0.8571 |
| F1-Score | 0.8070 |
| Balanced Accuracy | 0.7995 |
| Kappa | 0.5769 |
| MCC | 0.5879 |
| AUC | 0.8272 |

يبين جدول (6) مقاييس تقييم الأداء الخاصة بمصنف بيز عند تطبيقه على بيانات الاختبار، وهي البيانات التي لم تستخدم أثناء تدريب النموذج، مما يسمح بتقييم قدرته على التعميم والتنبؤ بحالات جديدة. وقد حقق النموذج دقة تصنيف عامة (Accuracy) بلغت 78.85%، وهي أعلى من دقة بيانات التدريب، مما يشير إلى استقرار أداء النموذج عند الانتقال من البيانات المستخدمة في التعلم إلى بيانات غير مشاهدة مسبقاً. أما الدقة الإيجابية (Precision) فجاءت مرتفعة (88.46%) ومقاربة لما تحقق في البيانات السابقة، بما يعكس قدرة النموذج على تقليل معدلات الإنذارات الكاذبة عند التنبؤ بالفئة عالية الخطر. وبالمقابل، جاءت الحساسية (Recall) بقيمة (74.19%) وهي أعلى مما كانت عليه في بيانات التدريب، مما يدل على تحسن قدرة النموذج على التقاط الحالات ذات مستوى الخطر العالي والتعرف عليها بشكل صحيح. كما تشير النوعية (Specificity) التي تساوي (85.71%) إلى أن النموذج احتفظ بقدرة جيدة على تمييز الحالات متوسط بصورة صحيحة، في حين تعكس قيمة (0.8070) F1-Score توازناً أفضل بين الدقة والحساسية مقارنة بما تحقق في البيانات الكلية وبيانات التدريب، الأمر الذي يشير إلى تحسن شامل في الأداء التصنيفي. وتؤكد Balanced Accuracy (0.7995) هذا الاتجاه، حيث تشير إلى أداء متوازن عبر الفئتين حتى في ظل عدم التوازن النسبي بين حالات متوسط وعالي. وتدعم قيمتا (0.5769) Kappa و(0.5879) MCC هذا التفسير من خلال الإشارة إلى مستوى اتفاق متوسط يميل نحو الجيد بين التوقعات والواقع، وبنسبة أعلى مما تحقق في بيانات التدريب، مما يدل على ثبات النموذج وتحسن ملحوظ في دقة التنبؤ خارج عينة التدريب. وأخيراً، تظهر مساحة تحت منحنى ROC (AUC = 0.8272) قدرة تصنيفية قوية للنموذج في الفصل الاحتمالي بين الفئتين، وهي أعلى قيمة مسجلة بين البيانات الثلاثة، مما يعكس قابلية جيدة للنموذج في تمييز مستويات الخطر عند التعامل مع بيانات جديدة.

وبشكل عام، يمكن القول إن أداء مصنف بيز على بيانات الاختبار جيد إلى حد كبير، ويشير إلى قدرة مناسبة على التعميم، مع تحسن واضح في الحساسية وF1-Score وAUC مقارنة ببيانات التدريب. وتعزز هذه النتائج من صلاحية النموذج للاستخدام في سيناريوهات تنبؤية مستقبلية، مع بقاء إمكانية تطوير إضافي لتعزيز التعرف على الحالات عالية الخطر بصورة أكثر شمولاً.

تشير المقارنة بين الجداول (4)، (5) و(6) إلى أن أداء مصنف بيز احتفظ بمستوى تصنيفي متقارب عبر البيانات الكلية والتدريب والاختبار، مع تحسن ملحوظ عند تطبيقه على بيانات الاختبار. فقد أظهر النموذج ارتفاعاً في كل من الدقة العامة والحساسية وF1-Score وAUC في بيانات الاختبار مقارنةً ببيانات التدريب، مما يدل على قدرة أفضل على التعرف على الحالات عالية الخطر عند التعامل مع بيانات جديدة غير مستخدمة في التعلم. كما حافظ النموذج على قيم مرتفعة نسبياً للدقة الإيجابية والنوعية في الجداول الثلاثة، مما يعكس

اتساقاً في تقليل الأخطاء التصنيفية للحالات الإيجابية وتمييز الفئة متوسط بصورة صحيحة. وبصورة عامة، تعكس هذه النتائج أداءً مستقراً للمصنف، مع وجود اتجاه تحسن عند الانتقال من بيانات التدريب إلى بيانات الاختبار، وهو ما يشير إلى قابلية مناسبة للتعميم دون ظهور أعراض واضحة للإفراط في التعلم.

## 7. الاستنتاجات (Conclusions)

يمكن الاستنتاج أن مصنف بيز يقدم أداءً تصنيفياً مقبولاً وجيداً نسبياً في التنبؤ بمستويات الخطر ضمن البيانات المدروسة، مع قدرة واضحة على التمييز بين الفئتين على الرغم من عدم التوازن النسبي في توزيع الحالات. وقد أظهر النموذج قابلية للتعميم انعكست في تحسن مؤشرات الأداء عند اختبار البيانات الجديدة، مما يدعم إمكانية استخدامه كأساس أولي في نظم دعم القرار الخاصة بتقييم مخاطر الهجمات السيبرانية. ومع ذلك، لا تزال الحساسية منخفضة نسبياً مقارنة بالدقة الإيجابية، الأمر الذي يشير إلى الحاجة إلى تعزيز قدرة النموذج على التقاط جميع الحالات عالية الخطر بشكل أدق. وعليه، يمكن أن تسهم أساليب إعادة التوازن أو تحسين اختيار المتغيرات أو دمج نماذج تصنيف إضافية في تحسين الأداء المستقبلي للنموذج وتطوير نهج أكثر موثوقية في التنبؤ بمستويات التهديد.

## 8. المصادر

**العربية:**

1. برادة، عبد الرزاق، 2023، "الأمن السيبراني وشروط تطبيقه"، جامعة أحمد زبانة غليزان (الجزائر)، مخبر الدراسات الاجتماعية والنفسية والأنثروبولوجية، رابط البحث:

https://www.researchgate.net/publication/386547316_alamn_alsybrany_wshrwt_ttbyqh_Cybersecurity_and_conditions_for_its_application#fullTextFileContent.

2. حسين، قاسم محمد، 2023، "أساسيات في الأمن السيبراني"، مؤتمر كلية الكنوز الجامعية، DOI:10.13140/RG.2.2.12437.13285، رابط البحث:

file:///C:/Users/PC/Downloads/1%20(3).pdf

**الأجنبية:**

1. Berrar, Daniel. (2018). Bayes' Theorem and Naive Bayes Classier. DOI: 10.1016/B978-0-12-809633-8.20473-1. Encyclopedia of Bioinfor -matics and Computational Biology, Volume 1, Elsevier, pp. 403-412. file:///C:/Users/PC/Downloads/Berrar_EBCB_Naive_Bayes_preprint%20(1).pdf.
2. Bolstad, William M. (2007). Introduction to Bayesian Statistics. Published by John Wiley & Sons, Inc. Hoboken. New Jersey. Published simultaneously in Canada. ISBN 978-0-470-141 15-1 (cloth). Printed in the United States of America. [Online]. Available:

https://www.stat.cmu.edu/~brian/BurkeBooks/Introduction%20to%20Bayesian%20Statistics%20-%202007%20-%20Bolstad.pdf?utm_source=chatgpt.com.

3. Downey, Allen B. (2012). Think Bayes Bayesian Statistics Made Simple. Green Tea Press. 9 Washburn Ave. Needham MA 02492. [Online]. Available: https://www.greenteapress.com/thinkbayes/thinkbayes.pdf.
4. Huang, Kaixing, Zhou, Chunjie, Tian, Yu-Chu, Tu, Weixun, and Peng, Yuan. (2017). Application of Bayesian Network to Data-Driven Cyber-Security Risk Assessment in SCADA Networks. Queensland University of technology in Gregory. M A (Ed.) Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). Institute of Electrical and Electronics Engineers Inc. United States of America pp. 96-101. [Online]. Available: https://ieeexplore.ieee.org/document/8215355.
5. Mo, Sheung Yin Kevin, and Beling, Peter Adam. (2009). Quantitative Assessment of Cyber Security Risk using Bayesian Network-based model. Published in: 2009 Systems and Information Engineering Design Symposium. Date of Conference: 24-24 April 2009. Date Added to IEEE Xplore: 17 July 2009, ISBN Information. DOI: 10.1109/SIEDS.2009.5166177. Publisher: IEEE. Conference Location: Charlottesville. VA. USA. [Online]. Available: file:///C:/Users/PC/Downloads/beling.mo.crowther.siedsfinal%20(1).pdf.
6. Ohrimenco, Serghei, and Valeriu, Cernei. (2024). Cybersecurity Risk. DOI: 10.53486/escst2023. Proceedings of International Conference. Chisinau. Moldova. Economic security in the context of systemic transformations. ISBN 978-9975-167-43-7. [Online]. Available: https://irek.ase.md/xmlui/bitstream/handle/123456789/3165/17.%20Ohrimenco_Securitatea%20economica-145-154.pdf?sequence=1&isAllowed=y.
7. Perusquia, Jose A., Griffin, Jim E., and Villa, Cristiano. (2021). Bayesian Models Applied to Cyber Security Anomaly Detection Problems. arXiv:2003.10360v4 [cs.CR] 3 Jun 2021. Volume 90. Issue 1. DOI: 10.1111/insr.12466. [Online]. Available: https://arxiv.org/pdf/2003.10360.
8. Purushottam, Fulsundar Amita, Kumar, Ajay, Satonkar, Vikas Haribhau, Gaikwad, Shweta Kundlik, Sonawane, Stefi Diliprao, and Shirwadkar, Bhushan. (2023). Probabilistic Risk Assessment in Cybersecurity: Bayesian Methods for Quantifying and Mitigating Cyber Risks. Panamerican Mathematical Journal. ISSN: 1064-9735. Vol 33. No 2. [Online]. Available: file:///C:/Users/PC/Downloads/04_P-271.pdf.
9. Wang, Jiali, Neil, Martin, and Fenton, Norman Elliott. (2019). A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model. Published by the journal: Computers & Security. Volume 89. ISSN: 0167-4048. DOI: 10.1016/j.cose.2019.101659. [Online]. Available: file:///C:/Users/PC/Downloads/ABNApproachforCRAImplementingandExtendingtheFAIRModel.pdf.

10. Zebrowski, Piotr, Vieira, Aitor Couce, and Mancuso, Alessandro. (2022). A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems. Risk Analysis published by Wiley Periodicals LLC on behalf of Society for Risk Analysis. Volume 45. Issue 5. ISSN: 0272-4332, DOI: 10.1111/risa.13900. [Online].
Available:https://onlinelibrary.wiley.com/doi/epdf/10.1111/risa.13900.