تسعير التأمين السيبراني باستخدام النماذج الاكتوارية والجبر الاحتمالي: دراسة تطبيقية على سوق التأمين المصرية

Cyber Insurance Pricing Using Actuarial Models and Probabilistic Algebra: An Empirical Application to the Egyptian Insurance Market

د. رنا محمد عبد الله النحال
مدرس التأمين والعلوم الاكتوارية بكلية التجارة – جامعة القاهرة
Rana_Mohamed_abdallah@foc.cu.edu.eg

د. أية سعيد حنفي محمود
مدرس التأمين والعلوم الاكتوارية بكلية التجارة – جامعة القاهرة
aya.said@foc.cu.edu.eg

ملخص

يهدف هذا البحث إلى معالجة التحديات المرتبطة بتسعير التأمين السيبراني في بيئة تتسم بعدم اكتمال المعلومات، وذلك من خلال تطوير نموذج اكتواري قائم على الجبر الاحتمالي. ويرتكز النموذج المقترح على صياغة رياضية تشمل القيمة المتوقعة للخسارة والانحراف المعياري، بالإضافة إلى معامل تعديل يمثل درجة تحمل المخاطر. كما تم اختبار مرونة النموذج باستخدام تقنيات متقدمة مثل تحليل الحساسية لضمان استقرار نتائج التسعير في مختلف السيناريوهات. وقد أظهرت النتائج أن النموذج المقترح يوفر آلية أكثر دقة وواقعية لتقدير الأقساط، ويعزز قدرة شركات التأمين على التعامل مع المخاطر غير المؤكدة. كما يقدم البحث توصيات منهجية للباحثين والممارسين بضرورة تحسين جودة قواعد البيانات السيبرانية وتطوير مؤشرات للمخاطر السيبرانية من أجل دعم عملية التسعير وتحقيق استدامة السوق التأمينية في ظل التهديدات المتزايدة، وفتح آفاق جديدة للدراسات المستقبلية التي تدمج بين الذكاء الاصطناعي والنماذج الاكتوارية لتحسين أداء قطاع التأمين.

الكلمات المفتاحية: تسعير التأمين السيبراني، الجبر الاحتمالي، النماذج الاكتوارية، تحليل الحساسية، عدم اكتمال المعلومات، الأمن السيبراني، قواعد البيانات السيبرانية، الذكاء الاصطناعي.

Abstract

This research aims to address the challenges associated with cyber insurance pricing in an environment characterized by incomplete information by developing an actuarial model based on probabilistic algebra. The proposed model relies on a mathematical formulation that incorporates the expected loss, standard deviation, and a risk-adjustment coefficient representing the degree of risk tolerance. The model's robustness was evaluated using advanced techniques such as sensitivity analysis to ensure the stability of pricing outcomes across different scenarios. The results demonstrated that the proposed model offers a more accurate and realistic mechanism for premium estimation, enhancing insurers' ability to manage uncertain risks. Moreover, the study provides methodological recommendations for researchers and practitioners, emphasizing the importance of improving the quality of cyber risk databases and developing cyber risk indicators to support pricing strategies and ensure the sustainability of the insurance market amid growing threats. The research also opens new avenues for future studies that integrate artificial intelligence with actuarial models to enhance the performance of the insurance sector.

Keywords: Cyber insurance pricing, probabilistic algebra, actuarial models, sensitivity analysis, incomplete information, cybersecurity, cyber data systems, artificial intelligence.

١- مقدمة

تعرف المخاطر السـيبرانية Cyber Risks بأنها الأضـرار المحتملة التي قد تنشـأ عن الاسـتخدام غير الآمن أو غير المصـرح به للأنظمة الرقمية والبنية التحتية لتكنولوجيا المعلومات، وتشمل هذه المخاطر التهديدات المرتبطة باختراق البيانات، وتعطيل الخدمات، وتسريب المعلومات، والابتزاز الإلكتروني، وغيرها من صور الهجمات الرقمية التي قد تلحق أضراراً مادية ومالية ومعنوية جسيمة بالأفراد والمؤسسات على حدٍ سواء .(Biener, Eling, & Wirfs, 2015) ويرتبط اتساع نطاق هذه المخاطر ارتباطاً مباشـراً بزيادة الاعتماد العالمي على شـبكات الإنترنت والحوسـبة السحابية وإنترنت الأشياء(IoT) ، الأمر الذي ضاعف من نقاط الضعف الممكن استغلالها من قبل المهاجمين.(Romanosky et al., 2019)

وقد أشـارت المنظمة الدولية للمعايير(ISO) ، في المعيار الدولي لإدارة المخاطر السـيبرانيةISO/IEC 27032:2012 ، أن إدارة الأمن السـيبراني لم تعد مقتصـرة على حماية الأجهزة أو الشبكات فحسب، بل أصبحت تمثل مفهوماً أوسع يشمل التعاون والتنسيق بين مختلف الأطراف المعنية للحد من التهديدات وتعزيز مرونة الأنظمة .(ISO/IEC, 2012) ، وفي السياق الأكاديمي، ينظر إلى المخاطر السيبرانية على أنها واحدة من أكثر أنواع الأخطار صعبة التأمين Hard-to-Insureنظراً لصعوبة حصر الأضرار بدقة، واعتمادها على سلوك بشري وتطور تقني مستمر يجعل من احتمالية حدوث الخسائر وشدتها أمراً غير مؤكد إلى حدٍّ كبير (Böhme & Kataria, 2006; Biener et al., 2015).

وفي ضوء ذلك، يتفق الباحثون(Eling & Schnell, 2016 ؛ Romanosky et al., 2019)على أن تصميم منتجات تأمين سيبراني فعالة يتطلب الجمع بين التحليل الكمي والاكتواري من جهة، وفهم دقيق لبنود التغطية والالتزامات القانونية من جهة أخرى، لتوفير آلية مرنة قادرة على التكيف مع طبيعة التهديدات المتغيرة واحتياجات الأسواق المحلية.

وتشـير الاتجاهات العالمية الحديثة إلى أن المخاطر السـيبرانية قد أصـبحت في مقدمة المخاطر التي تهدد استمرارية الأعمال، متفوقة في بعض الحالات على الكوارث الطبيعية والأزمات الاقتصـادية من حيث الأثر المالي والسـمعة والانتشـار المفاجئ. فقد أظهر تقرير Allianz Risk Barometer 2024أن الهجمات السـيبرانية والاضـطرابات التكنولوجية جاءت في المرتبة الأولى

ضمن قائمة المخاطر الرئيسية التي تواجه المؤسسات، حيث تصدرت لأول مرة هذه القائمة بنسبة ٣٦٪ من الاستجابات، متقدمة على المخاطر المرتبطة بالكوارث الطبيعية أو انقطاع الأعمال التقليدي(Allianz Global Corporate & Specialty, 2024) ، وتعكس هذه النسبة إدراكاً متزايداً لدى الشركات العالمية لأهمية تبني سياسات تأمين سيبراني فعالة، خاصةً مع اتساع حجم الأضرار الناتجة عن خروقات البيانات وهجمات الفدية Ransomware، ويدعم هذا الاتجاه أيضاً ما أشار إليه تقرير IBM Cost of a Data Breach Report 2023، الذي بين أن متوسط تكلفة حادثة اختراق البيانات عالمياً بلغ نحو ٤,٤٥ مليون دولار أمريكي، بزيادة مطردة بلغت ١٥٪ خلال السنوات الثلاث الأخيرة.(IBM Security, 2023)

وفي السياق المحلي، يظهر السوق المصري ملامح واضحة لتنامي حجم التهديدات السيبرانية بالتوازي مع التوسع الرقمي في القطاعات المالية والحكومية والخدمية. فقد أفاد تقرير صادر عن شركة Kaspersky لعام ٢٠٢٣ وهي شركة عالمية متخصصة في أمن المعلومات والأمن السيبراني، بأن مصر سجلت أكثر من ١٣ مليون تهديد سيبراني خلال الربع الأول فقط من عام ٢٠٢٣، مع تسجيل زيادة غير مسبوقة بلغت ١٨٦٪ في استهداف القطاع المالي والبنوك مقارنة بالفترة ذاتها من العام السابق. ويرتبط ذلك بازدياد استخدام الخدمات المصرفية الرقمية وضعف تطبيق بعض ضوابط الأمن السيبراني في المنشآت الصغيرة والمتوسطة، ما يجعلها هدفاً سهلاً للمهاجمين. ورغم هذه الأرقام اللافتة، لا يزال السوق المصري يعاني من غياب قاعدة بيانات قومية شاملة وموثوقة يمكن أن يعتمد عليها صانعو القرار وشركات التأمين في تصميم نماذج تسعير دقيقة مبنية على معطيات محلية واقعية. حيث أن نقص البيانات التاريخية الدقيقة عن تكرار الحوادث السيبرانية Frequency وشدة خسائرها Severity يعد أحد العوائق الرئيسية أمام قدرة شركات التأمين على وضع تقديرات موضوعية للقسط المناسب الذي يحقق التوازن بين حماية المؤمن لهم وضمان الاستدامة المالية للشركات حتى في الأسواق المتقدمة ,.Biener et al) (2015 ، وهو ما ينسحب بصورة أشد في الأسواق الناشئة مثل مصر.

وعلى المستوى العملي، تقدم بعض الشركات متعددة الجنسيات العاملة في مصر مثل شركة أمريكان إنترناشيونال (American International Group (AIG وشركة أكسا AXA و شركة أليانز مصر Allianz Egypt منتجات تأمين سيبراني، لكنها غالباً ما تكون نسخاً معدلة من

وثائق عالمية دون وجود وثائق متخصصة مطورة محلياً تلائم الخصائص السوقية المحلية، لا سيما من حيث توزيع الخطر وقابلية تحمل الأقساط لدى الشركات الصغيرة والمتوسطة. ويظهر تحليل Romanosky et al. (2019) أن الوثائق العالمية عادة ما تتضمن بنودا خاصة بتغطية المسؤولية تجاه الغير، وخسائر انقطاع الأعمال، وتكاليف الحوادث، وهي بنود تؤثر جوهريًا على معادلة التسعير.

من هنا تبرز أهمية هذا البحث الذي يستهدف بناء نموذج تسعير للتأمين السيبراني يعتمد على أسس اكتوارية مدعومة بتطبيقات الجبر الاحتمالي بهدف تقدير تكرار الحوادث Frequency وشدة الخسائر Severity بأكبر قدر من الدقة الممكنة رغم نقص البيانات المثالية.

١/١ مشكلة الدراسة

رغم تصاعد حدة المخاطر السيبرانية عالمياً ومحلياً، إلا انه لا يزال سوق التأمين المصري يواجه فجوة واضحة في قدرته على تطوير منتجات تأمين سيبراني متخصصة تستند إلى أسس تسعير علمية مدعومة بنماذج اكتوارية ملائمة لواقع السوق وخصائصه التقنية والتنظيمية. ففي السوق المصرية، تتعقد المشكلة أكثر نتيجة غياب قاعدة بيانات وطنية محدثة توثق الهجمات الإلكترونية والخسائر الناتجة عنها بصورة دورية وموثوقة، ويضاف إلى ذلك أن وثائق التأمين المتاحة حاليا ما هي إلا نسخاً مستمدة من عقود عالمية صممت لأسواق اخري أكثر تقدماً، وبذلك فهي تفتقر إلي وجود صياغات معدلة بالكامل للتعامل مع التحديات المحلية، خاصة فيما يتعلق بقطاع الشركات الصغيرة والمتوسطة الأكثر هشاشة أمام الهجمات السيبرانية.

وتتعمق مشكلة الدراسة عندما يتضح أن غالبية النماذج الاكتوارية التقليدية، حتى على المستوى الدولي، لم تطور بعد لتشمل الجبر الاحتمالي كأداة لإدارة التوزيعات الاحتمالية للمتغيرات المعقدة مثل تكرار الحوادث السيبرانية أو الترابط بينها (Böhme & Kataria, 2006). إذ غالباً ما تتسم هذه المخاطر بدرجات عالية من عدم اليقين وبوجود ارتباطات متداخلة Correlations تجعل من التقديرات البسيطة أداة قاصرة عن توفير الأساس العلمي الكافي لتسعير أقساط التأمين بدقة.

وبالتالي تتمثل مشكلة الدراسة في قصور البنية الإحصائية والبيانية للسوق المصرية من جهة، وعدم تبني مقاربة رياضية اكتوارية متقدمة – مثل الدمج المنهجي بين النماذج الاكتوارية

والجبر الاحتمالي من جهة أخرى، بما يعوق شركات التأمين عن تصميم وثائق تأمين سيبراني مرنة تلائم الخصوصية المحلية وتواكب معايير التغطية العالمية في الوقت نفسه. وتُبرز هذه المشكلة الحاجة إلى بناء إطار علمي تطبيقي قادر على سد فجوة التسعير وتوجيه أصحاب القرار لتبني سياسات تسعير مستندة إلى معطيات كمية، حتى في ظل غياب البيانات المثالية.

٢/١ الهدف من الدراسة

تنطلق هذه الدراسة من إدراك فجوة السوق المصرية في مجال تأمين المخاطر السيبرانية، وتسعى إلى تحقيق الأهداف التالية:

١/٢/١ تحليل واقع التهديدات السيبرانية في مصر وذلك من خلال تجميع وتحليل البيانات المتاحة حول عدد الحوادث السيبرانية، وتوزيعها القطاعي، ومدى تطورها زمنياً، بما يعكس الاتجاهات الرئيسية ونقاط الضعف المحلية.

٢/٢/١ تطوير إطار اكتواري لتقدير المخاطر السيبرانية يستند إلى توزيع التكرار والشدة Frequency & Severity، بهدف الوصول إلى تقدير موضوعي للقسط.

٣/٢/١ توظيف أساليب الجبر الاحتمالي لزيادة دقة معالجة العلاقات الترابطية بين أنواع الحوادث السيبرانية والارتباطات الداخلية (Correlations) التي تؤثر على تباين الخسائر.

٤/٢/١ ربط الإطار النظري بالبنية التعاقدية الفعلية من خلال مقارنة نتائج النموذج بالاستخدامات الفعلية لبنود التغطية في وثائق التأمين السيبراني، بهدف اقتراح تعديلات مرنة تلائم الخصوصية المحلية وتدعم الابتكار في المنتجات التأمينية.

٥/٢/١ صياغة توصيات عملية لشركات التأمين والوسطاء والخبراء الاكتواريين، بما يساعد في ضبط هامش الخطر وتحقيق التوازن بين حماية العملاء وضمان ربحية الشركات واستدامة التغطيات.

٦/٢/١ دعم صانع القرار ومجتمع الأعمال عبر توفير مرجع تطبيقي يسهم في زيادة الوعي التأميني بالمخاطر السيبرانية ويساعد الجهات التشريعية على تطوير بيئة تنظيمية مشجعة على التوسع في هذا النوع من التأمين.

٣/١ الدراسات السابقة

شهد تسعير التأمين في بيئات تتسم بعدم اليقين والمعلومات غير الكاملة اهتماماً متزايداً في الأدبيات الاقتصادية والمالية، وقد ساهمت العديد من الدراسات في بناء الأسس النظرية والمنهجية لفهم سلوك الأسواق التأمينية، وتقييم المخاطر، وتطوير النماذج الاكتوارية. وسوف يتم استعراض أبرز الدراسات السابقة التي تناولت تسعير التأمين في ظل المعلومات غير الكاملة ، والنماذج الرياضية المستخدمة، ومداخل تحسين كفاءة التسعير في الأسواق التنافسية، مع التركيز على التطبيقات المتعلقة بالتأمين السيبراني.

١/١/٣ دراسة(Biener, Eling & Wirfs, 2015)

تناولت هذه الدراسة مدي قابلية التأمين على المخاطر السيبرانية من منظور اكتواري واقتصادي، حيث ركزت على هذه النوعية من المخاطر في ضوء خصائصها الفريدة، مثل ارتفاع درجة عدم اليقين، غموض البيانات، وصعوبة التنبؤ بالتكرار والحدة. استخدمت الدراسة منهجاً تجريبياً لتقييم مدى ملاءمة سوق التأمين للتعامل مع المخاطر السيبرانية، من خلال تحليل قواعد بيانات حوادث إلكترونية فعلية. وخلصت الدراسة إلى أن المخاطر السيبرانية تعد قابلة للتأمين جزئياً ، ولكنها تتطلب تطوير أدوات جديدة لتسعير وتوزيع الخطر، مثل التجميع والتوريق، وفرض حدود وشروط دقيقة على التغطية.

٢/١/٣ دراسة(Eling & Schnell, 2016)

تعد من الدراسات الهامة في تقديم مراجعة شاملة للدراسات المتعلقة بالمخاطر السيبرانية والتأمين عليها، حيث قامت بتحليل أكثر من ٥٠ ورقة بحثية تناولت هذا الموضوع من جوانب نظرية وتطبيقية. وركزت الدراسة على النماذج التي قامت بتقدير حجم الخطر السيبراني وتكاليفه، بالإضافة إلى استراتيجيات تصميم منتجات تأمينية ملائمة. كما ناقشت أوجه القصور في البيانات المتاحة لشركات التأمين، والحاجة إلى نماذج رياضية أكثر مرونة ودقة تعكس واقع التعقيد في الهجمات السيبرانية. وقد أوصت الدراسة بتوسيع استخدام المحاكاة، والاعتماد على أساليب النمذجة الاحتمالية التي تأخذ بعين الاعتبار الارتباط بين الحوادث والقطاعات.

٣/١/٣ دراسة(Eling & Wirfs, 2019)

هدفت الدراسة إلى تقديم تقديرات دقيقة لتكاليف حوادث الخطر السيبراني، بناء على قاعدة بيانات موسعة تضم أكثر من ٥٠٠ حادثة إلكترونية عالمية. وقد اعتمدت الدراسة على تحليل إحصائي لمقاييس الخسارة المتكررة والشديدة، باستخدام أدوات مثل التوزيعات شديدة الالتواء–Heavy tailed distributions والاختبارات غير المعلمية. وأظهرت النتائج أن متوسط الخسائر المالية الناتجة عن الهجمات السيبرانية أعلى بكثير من متوسط خسائر الحوادث الأخرى في التأمين التقليدي، كما أظهرت الدراسة الحاجة الماسة لنماذج تسعير تستند إلى التحليل الكمي لعدم التماثل المعلوماتي والتعرض المشترك للمخاطر Systemic Exposure .

٤/١/٣ دراسة(Romanosky et al., 2019)

هدفت الدراسة إلى تحليل وثائق التأمين السيبراني المعتمدة فعلياً لدى عدد من شركات التأمين العالمية، من خلال إجراء تحليل محتوى لعدد كبير من وثائق التأمين. وقد ركزت على بنية التغطيات، الاستثناءات، حدود التعويض، ونماذج تسعير الأقساط. وأظهرت النتائج أن هناك تباينًا كبيراً في تصميم الوثائق بين الشركات، مع غياب المعايير الموحدة لتقدير المخاطر. كما وجدت الدراسة أن العديد من الشركات لا تستخدم نماذج اكتوارية متقدمة، بل تعتمد على أساليب تسعير تقليدية غير ملائمة لطبيعة الخطر السيبراني، ما يُضعف من كفاءة السوق ويزيد من احتمال الخسارة الإجمالية.

٥/١/٣ دراسة(Awiszus et al., 2023)

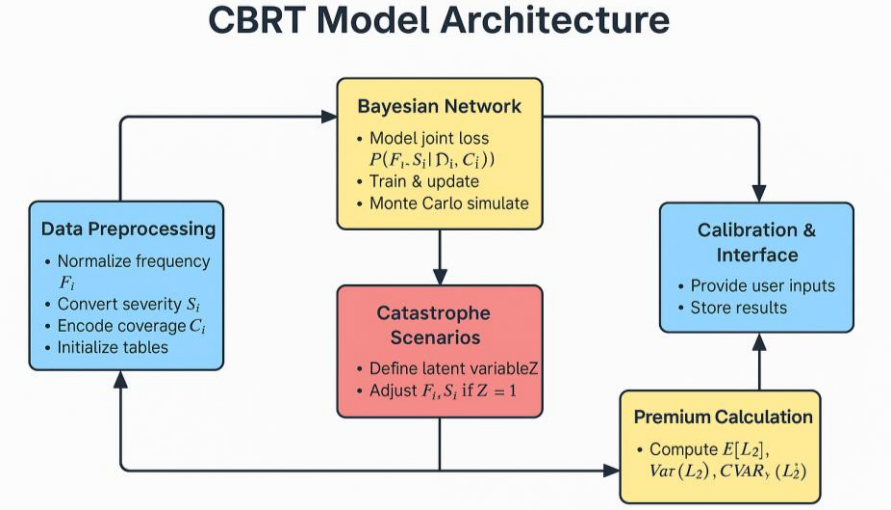
تناولت الدراسة النمذجة الرياضية لتسعير التأمين السيبراني من خلال تقديم إطار اكتواري متكامل يستند إلى توزيع الخسائر ومبدأ القيمة المعرضة للخطر (VAK) ، وقد اعتمد الباحثون على معادلات تفاضلية ونماذج احتمالية مركبة لتقدير القسط في ظل ارتفاع درجة التعقيد والتشابك بين مكونات الخطر السيبراني. كما اقترحت الدراسة استخدام تقنيات مثل محاكاة مونت كارلو Monte Carlo simulationلدراسة السيناريوهات المختلفة للهجوم السيبراني وتأثيرها على الخسائر الكلية.

٢- النموذج الرياضي المستخدم في الدراسة

يهدف هذا الجزء إلى تقديم إطار رياضـــي اكتواري-جبري لتقدير القســـط لوثائق التأمين الســـيبراني في الســـوق المصـــرية، وذلك عبر دمج مبادئ التحليل الاكتواري مع البنية الجبرية لاحتمالية الخطر بما يعكس الطبيعة المترابطة والمتغيرة للخســـائر الرقمية. وينطلق النموذج من التمييز بين نوعي الخسائر الأساسيين في وثائق التأمين السيبراني وهما الخسائر المباشرة First Party Losses وخسائر المسؤولية عن الطرف الثالث Third Party Liability ، فعلى مستوى الأضرار المباشرة، تتحمل شركة التأمين التعويض عن الخسائر التي يتكبدها المؤمن له شخصياً نتيجة وقوع حادث سيبراني داخل بيئته الرقمية. وتشمل هذه التكاليف عادةً نفقات استعادة البيانات التالفة، دفع مبالغ الفدية لمجرمي الإنترنت لاسترجاع الأنظمة، وأجور الخبراء الفنيين لإعادة تشغيل الشبكات والبنى التحتية المعلوماتية، فضلاً عن تكاليف الاتصال بالعملاء وإدارة الأزمات الإعلامية *(Romanosky et al., 2019)*. أما بالنسبة لخسائر المسؤولية عن الطرف الثالث، فتغطي الوثيقة التعويضـــات والالتزامات القانونية التي قد تترتب على المؤمن له تجاه أطراف خارجية متضـــررة بســـبب تســـريب البيانات أو انتهاك ســـرية معلومات العملاء والشـــركاء. وتشـــمل هذه المسؤوليات تكاليف الدفاع القضائي والغرامات المحتملة وأي مبالغ تعويضية تفرض بحكم قضائي، وهو ما يعد من أخطر مكونات الخطر السيبراني نظراً لتشابكه مع القوانين الوطنية والدولية لحماية البيانات *(Biener et al., 2015)*.

هذا التمايز بين نوعي الخسائر يبرز الطبيعة المترابطة للمخاطر السيبرانية وضرورة تقدير التوزيع المركب لها عند حساب القسط، حيث قد تتداخل الأضرار المباشرة مع التزامات المسؤولية بشـكل يعقد التوقعات ويزيد من أهمية دمج التحليل الجبري مع النماذج الاكتوارية لضـمان تقدير تكلفة الأخطار بدقة ومرونة.

واســـتجابة لهذه التحديات، تقترح الدراســـة نموذج رياضـــي هو Cyber Bayesian-Robust Tariffing (CBRT) ، ويهدف هذا النموذج إلى دمج أربعة مكونات أساسية كما يتضح من الشكل (١)، هي :



المصدر :من إعدادالباحثتين

شكل (١) مخطط بناء النموذج المقترح

- **الهيكل الاكتواري الأساسي:Base Actuarial Framework**

يعتمد على حساب القيمة المتوقعة للخسائر والانحراف المعياري، كأساس لتقدير القسط، حيث يعدل لاحقا عبر أوزان تقدرها الشبكة البيزية.

- **الشبكة البيزية:(Bayesian Network)**

والتي تستخدم لتقدير التوزيعات الاحتمالية غير المؤكدة للمدخلات مثل تكرار الهجمات أو شدتها، حيث تسمح هذه الشبكة بتحديث القيم مع ورود بيانات جديدة، وتوظف توزيعات سابقة prior distributionsتُعدل لاحقاً بناء على البيانات اللاحقة(Awiszus et al., 2023).

- **نمذجة ذيل الخطر:(Tail-Risk Modeling)**

يشكل نمذجة ذيل الخطر أحد الأعمدة الأساسية في نموذج CBRT نظراً للطبيعة اللامتناظرة وشديدة التشتت للخسائر السيبرانية، حيث تتسم بالتكرار المنخفض وجسامة الخسائر Low-Frequency High-Severity. وللتعامل مع هذا النوع من المخاطر، يدمج النموذج دوال خطر معدلة قادرة على استشراف سلوك الخسائر في الذيل الأعلى لتوزيع الاحتمال (Eling & Wirfs, 2019)، بما يتجاوز إمكانيات نماذج التسعير التقليدية التي تعتمد على الافتراضات الخطية.

- **التحسين العشوائي:(Robust Stochastic Optimization)**

حيث يتم اســتخدامه لتقدير معاملات النموذج في اطار حالة عدم اليقين لتوزيع الخســائر، وذلك من خلال أســـلوب مثل Robust Mean–Variance أو Distributionally Robust Optimization، مما يسمح بتقدير أقساط تأمينية لا تكون فقط عادلة، بل ومحصنة ضد انحرافات البيانات .(Delage & Ye, 2010; Blanchet et al., 2019) ، ويظهر اســـتخدام هذا الاســـلوب في التأمين الســـيبراني قدرة النماذج القوية على احتواء التقلبات الناتجة عن بيانات غير مكتملة.

٢/١متغيرات الدراسة:

يعتمد النموذج الرياضي المقترح على مجموعة من المتغيرات العشوائية الأساسية التي تمثل السمات الرئيسية للمخاطر السيبرانية ضمن البيئة المصرية، وهي:

١/١/٢ معدل تكرار الحوادث الســـيبرانية F_i، يمثل هذا المتغير تكرار الحوادث التي يتعرض لها القطاع المحدد خلال فترة معينة (عادة سـنة). وقد تم تقدير قيم F_i في هذه الدراسـة اسـتناداً إلى بيانات تقارير شركة(2018–2023) Trend Micro ، حيث تم رصد ملايين التهديدات ســـنوياً، وقد تم تهيئة هذه البيانات بعدد مســـتخدمي الإنترنت وفق بيانات منصـــة DataReportal للحصول على تكرار الحوادث لكل مستخدم.

٢/١/٢ شـدة الخسـارة لكل حادثة S_i، وهي مقدار الخسـارة المالية الناجمة عن حادثة واحدة. وقد اعتمدت الدراســة الحالية على متوســط تكلفة الحادثة الســيبرانية عالمياً كما ورد في تقارير IBM Securityو Allianz Cyber، حيث تم اختيار الحد الأدنى من هذه التقديرات وهو ١٠٠٠ دولار/حادثة أي ما يعادل حوالي ٤٨٠٠٠ جنيه مصـري في ٢٠٢٤ وفقاً لمتوسـط سعر الصرف الرسمي . يفترض النموذج ثبات هذا المتوسط في غياب بيانات رسمية دقيقة، مع إمكانية تعديله عند توفر معطيات دقيقة من السوق المصري مستقبلاً.

٣/١/٢ نوع التغطية التأمينية C_i والذي يعبر عن درجة شـمولية الوثيقة التأمينية، وقد اعتمدت هذه الدراسة على تغطيات قياسة متعارف عليه دولياً في صناعة التأمين السيبراني، والتي تصنف وثائق التأمين السيبراني إلى ثلاث فئات(Allianz & Specialty,2023)

- تغطية محدودة :(C_i= 1) تشمل حماية البيانات الحساسة، والامتثال للتشريعات، وتكاليف الإبلاغ والتنبيه.
- تغطية متوسطة :(C_i= 2) تمتد لتشمل استعادة الأنظمة، وتكاليف توقف الأعمال، والفحص التقني.
- تغطية شاملة :(C_i= 3) تشمل التعويض عن الأضرار غير المباشرة، واستعادة السمعة، وخدمات الاستجابة للحوادث المعقدة.

تم مطابقة هذه التصنيفات مع طبيعة كل قطاع في مصر، استناداً إلى درجة نضجه الرقمي وقدرته على الاستثمار في وثائق تأمين أكثر تعقيداً، فعلى سبيل المثال تعد التغطية الشاملة (C_i= 3)الأنسب لقطاع البنوك وقطاع الاتصالات والتكنولوجيا، بينما التغطية المحدودة =(C_i 1)تعد الأنسب لقطاع التأمين، نظراً لأن أغلب هذه الشركات لا تملك بنية تحتية رقمية متقدمة.

٤/١/٢ قابلية القطاع للتعرض السيبراني D_i يعكس هذا المتغير مدى ضعف البنية التحتية السيبرانية للقطاع واحتمالية اختراقه. وقد تم الاعتماد في حسابه علي تقارير شركة Kaspersky Security Bulletinوالتي صنف القطاعات المصرية من حيث تعرضها للتهديدات.

٢/٢ العلاقة البينية بين المتغيرات

يعتمد نموذج CBRT على شبكة بيزية ديناميكية Dynamic Bayesian Network لتحقيق نمذجة دقيقة وشاملة للمخاطر السيبرانية، وذلك لتقدير التوزيع المشترك للمتغيرين العشوائيين تكرار الحوادث السيبرانيةF_i وشدة الخسارةS_i ، بالاعتماد على المتغيرين التوضيحيين نوع التغطية التأمينيةC_i وضعف البنية السيبرانيةD_i . حيث تأخذ العلاقة الشكل الرياضي التالي:

$$P(F_i, S_i \mid D_i, C_i) = P(F_i \mid D_i) \mid P(S_i \mid C_i)$$

ويعبر هذا الشكل الرياضي عن مبدأ الاستقلال الشرطي Conditional Independence، الذي يعد من الأسس البنيوية للشبكات البيزية (Koller & Friedman, 2009).حيث يمثل التوزيع الاحتمالي$P(F_i \mid D_i)$ نمذجة التكرار المشروط بدرجة القابلية للاختراق. فكلما كانت البنية الرقمية ضعيفة (أي D_i مرتفعة)، زادت احتمالية وقوع الحوادث. بنما يوضح

التوزيع الاحتمالي $P(S_i|\ C_i)$ العلاقة العكسية بين شدة الخسارة ومستوى التغطية. فالتغطية المحدودة تعني أن المؤمن له سيتحمل جزءاً أكبر من الخسارة، بينما التغطية الشاملة تقلل من هذه الشدة(Eling & Schnell, 2016) . ويؤدي الفصل بين $P(F_i|\ D_i)$ و $P(S_i|\ C_i)$ كتوزيعين شرطيين إلي تبسيط عملية التقدير والمعايرة بشكل كبير. حيث أن مثل هذا النهج يقلل من التعقيد الحسابي مقارنة باستخدام توزيعات مشتركة كثيفة الأبعاد(Wüthrich & Merz, 2008) ، مما يساعد في بناء نموذج قابل للتطبيق العملي في ظل نقص البيانات.

٣/٢ صياغة القسط السنوي الأساسي(CBRT Premium Formulation)

تعتمد الصياغة الرياضية للقسط السنوي في نموذج CBRT على إطار اكتواري موسع يأخذ في الاعتبار الطبيعة غير الخطية والمركبة للمخاطر السيبرانية. بخلاف المبادئ التقليدية التي تعتمد فقط على القيمة المتوقعة للخسارة، حيث يدمج هذا النموذج ثلاثة مكونات رئيسية لتقدير القسط الكلي، بما يعكس التوزيع الكامل للخطر واحتمالات التغير المفاجئ في الخسائر.ويعبر عن القسط السنوي المتوقع بالمعادلة التالية:

$$P = E[L] + \alpha\ .Var(L) + \beta\ \cdot\ CVaR_{\gamma}(L)$$

١/٣/٢ المكون الأول: القيمة المتوقعة للخسارة $E[L]$

وتمثل هذه القيمة القسط الأساسي الصافي Net Premium، وهي تعكس المتوسط المتوقع للخسائر خلال فترة التغطية ,والتي عادة ما تكونسنة واحدة ،وتحسب الخسارة الكلية L على النحو التالي:

$$L = \sum_{I=1}^{n} F_i.\ S_i.w(C_i, D_i)$$

حيث

$w(C_i, D_i)$ = دالة الوزن التي تعدل الخسارة وفقاً لمستوى التغطية التأمينية C_i وقابلية التعرض للمخاطر السيبرانية في القطاعD_i.

٢/٣/٢ المكون الثاني: معامل التحميل الإحصائي $\alpha . Var(L)$

ويشـير إلى التباين الإحصـائي في الخسـارة والذي يسـتخدم لقياس درجة عدم التأكد أو التشتت حول القيمة المتوقعة. وكلما زاد التباين دل ذلك على وجود تقلبات كبيرة في توزيع الخسائر، مما يسـتوجب تحميلاً إضـافياً على القسـط لتغطية هذه التقلبات. ويتم تحديد قيمة المعامل α بناء على مدى تحمل شركة التأمين للمخاطر الإحصائية.

٣/٣/٢ المكون الثالث: معامل التحفظ للذيل الخطر $\beta \cdot CVaR_{\gamma}(L)$

يمثل معامل التحفظ المرتبط بـقيمة الخطر المشروط (Conditional Value–at–Risk CVaR) –أحد أهم الإضـافات المنهجية التي يقدمها النموذج الرياضـي المقترح(CBRT) ، وذلك من أجل تعزيز اسـتجابته للأحداث النادرة ولكن ذات الخسـائر الجسـيمة. حيث تسـتخدم CVaR كمقياس إحصـائي يعكس متوسـط الخسـائر في أسـوأ $(1-\gamma)$ % من الحالات، أي في الطرف الأيمن الحاد من توزيع الخسـائر(Rockafellar & Uryasev, 2000). وهذا يعد أكثر ملاءمة من مقياس VaR التقليدي، لأنه لا يقتصر فقط على الحد الأدنى للخسائر الجسيمة بل يأخذ بعين الاعتبار المتوسط المرجح لها ، مما يجعله أكثر تعبيرًا عن طبيعة المخاطر القصوى.

ويتم تحديد قيمة γ بما يتناسب مع سياسة الشركة أو الجهة الرقابية. ففي تطبيقات التأمين السيبراني، تستخدم عادة مستويات ثقة مثل ٩٥٪ أو ٩٩٪(Blanchet et al., 2019) ، ما يعني أن النموذج يأخذ في اعتباره متوسط أسوأ ٥٪ أو ١٪ من حالات الخطر، على التوالي، ما يضـمن تقدير أقساط عادلة ولكن أكثر تحفظًا في مواجهة الحالات الكارثية.

٤/٢ تمثيل سـيناريوهات الكوارث السـيبرانية Scenario–Based Adjustment for Cyber Catastrophes

في ظل التحول الجذري في طبيعة الهجمات السـيبرانية، من عمليات فردية إلى حملات منسـقة ذات أثر منظومي، بات من الضـروري أن تتضـمن النماذج الاكتوارية الحديثة آليات لاسـتيعاب هذه السـيناريوهات النادرة ولكن عالية التأثير. حيث يعد تمثيل الكوارث السـيبرانية أحد المكونات الأساسـية في النموذج المقترح CBRT، والذي يعكس الحاجة إلى تضـمين سـيناريوهات احتمالية مشروطة لوقوع أحداث قصوى تؤثر في تكرار وشدة الخسائر معاً.

لذلك، يقترح النموذج إدراج متغير كامن يُرمز له بـــــ Z ، يســـتخدم لتمثيل وقوع حادث ســيبراني كارثي (مثل هجوم على بنية تحتية ســيادية أو تســرب ضــخم للبيانات). وعند تحقق هذا المتغير، تعدل متغيرات النموذج الرئيسية كالتالي:

$$F_i^Z = F_i \,.\, \theta(Z), \qquad S_i^Z = S_i \,.\, \gamma(Z),$$

حيث

$$\theta(Z) > 1$$

يمثل معامل تضخيم لتكرار الحوادث F_i عند تحقق الكارثة

و

$$\gamma(Z) > 1$$

يمثل معامل تضخيم لشدة الخسارة S_i تحت نفس السيناريو.

هذه الصيغة تعكس مبدأ أن الكوارث السيبرانية لا تؤدي فقط إلى زيادة الخسارة الواحدة، بل تُحدث تكراراً متزامناً ومتعدداً للهجمات نتيجة تفاعلات الأنظمة الرقمية وإرتباطها المتبادل (Kott, 2020). وقد دعمت الدراســـات الحديثة المتعلقة بإدارة المخاطر الســـيبرانية ضـــرورة تضـــمين سيناريوهات الكوارث ضمن نماذج التسعير، خصوصاً في ضوء الاتجاه العالمي نحو تقييم المخاطر الســـيبرانية النظامية Systemic Cyber Risk ، كما أشـــارت إليه تقارير (Allianz Global Corporate & Specialty , 2023) والتي أكدت أن هجوماً منسقاً واحداً على خدمات سحابية قد يصيب آلاف المؤسسات في وقت متزامن.

ويفترض النموذج أن المتغير Z يكون كمتغير يتبع توزيع ثنـائي الحـالـة Bernoulli، بحيث:

$Z = 1$ يشير إلى تحقق سيناريو كارثي.

$Z = 0$ يشير إلى عدم تحقق الكارثة.

ويمكن معايرة هذا التوزيع اسـتناداً إلى بيانات خارجية مثل تقديرات التصـعيد الجيوسـياسـي Geopolitical escalation estimates أو مؤشـــرات التهديد الســـادي Sovereign threat indicators (ENISA Threat Landscape, 2023) .

٥/٢ الصياغة التكاملية لقسط التأمين النهائي

في ضوء المكونات السابقة، يعاد تعريف الخسارة الكلية L للقطاع i تحت سيناريو محتمل لوقوع كارثة سيبرانية، لتأخذ الشكل التالي:

$$L_i^Z = F_i \,.\, \theta(Z) \,.\, S_i \,.\, \gamma(Z) \,.\, w(C_i, D_i)$$

ثم يحسب القسط السنوي النهائي وفقاً لمعادلة التالية

$$P = E[L^Z] + \boldsymbol{\alpha} \,.\, \boldsymbol{Var}(L^Z) + \ \beta \ \cdot \ CVaR_\gamma(L^Z)$$

٣ بيانات الدراسة

نظراً لغياب قواعد بيانات رسمية منشورة حول التأمين السيبراني في مصر سواء كانت سجلات الأقساط، أو وثائق المطالبات، أو حتى معدلات التكرار والشدة المجمعة حسب القطاع . فقد واجهت الدراسة تحدياً أساسياً في الوصول إلى بيانات كمية مباشرة. ولهذا، تم اللجوء إلى استراتيجية بناء قاعدة بيانات بديلة ترتكز على مصادر دولية موثوقة.

وقد تضمنت مصادر البيانات المستخدمة ما يلي:

- تقارير شركة Trend Micro السنوية عن التهديدات السيبرانية Trend Micro Annual Cybersecurity Report ، والتي وفرت تفاصيل كمية عن أنواع الهجمات (مثل البريد الإلكتروني الضار، الروابط الخبيثة، والبرمجيات الضارة) للفترة ٢٠١٨–٢٠٢٣.
- تحليلات شركة Kaspersky التي سلطت الضوء على خصائص المخاطر في البيئة الرقمية المصرية، مثل قابلية الاختراق حسب القطاع، وانتشار هجمات الفدية، والهندسة الاجتماعية.
- إحصاءات عدد مستخدمي الإنترنت النشطين في مصر من البنك الدولي ومنصة DataReportal، والتي استخدمت تهيئة البيانات الكلية للتهديدات من أجل حساب تكرار الخطر الاحتمالي للفرد أو المنشأة.

- تقديرات شـدة الخسـارة المالية للحادثة الواحدة، والتي تم تحديدها عند ١,٠٠٠ دولار كقيمة مرجعية منخفضـــة بناءً على تقارير شـــركتي IBM وAllianz، ومن ثم تم تحويلها إلى الجنيه المصري بقيمة ٤٨,٠٠٠ جنيه (بمتوسط سعر صرف ٢٠٢٤).

١/٣ التهديدات السيبرانية

يوضح الجدول (١) أعداد التهديدات التي تم اكتشافها في مصر من قبل شركة Trend Micro في الفترة ٢٠١٨: ٢٠٢٣ ، وتشمل تهديدات البريد الإلكتروني، الروابط الخبيثة، واكتشافات البرمجيات الضارة.

الجدول (١) بيانات تهديدات Trend Micro في مصر في الفترة ٢٠١٨: ٢٠٢٣

السنة	تهديدات البريد الإلكتروني	الروابط الخبيثة	اكتشافات البرمجيات الضارة	إجمالي التهديدات
2018	36600000	593654	740305	37933959
2019	29000000	125000	720,000	29845000
2020	20300000	1880000	740,000	22920000
2021	25000000	2450000	5500000	32950000
2022	28530000	3160000	9410000	41100000
2023	18000000	2000000	8000000	28000000

المصدر: Trend Micro Annual Threat Reports, www.trendmicro.com

٢/٣عدد مستخدمي الإنترنت

تم اسـتخدام بيانات البنك الدولي وتقارير منصـة DataReportal لحسـاب عدد مسـتخدمي الإنترنت النشـطين في مصـر(جدول – ٢) ، وهو ما يسـتخدم لتطبيع عدد التهديدات حسـب عدد المستخدمين في كل سنة.

الجدول (٢) عدد مستخدمي الإنترنت في مصر في الفترة ٢٠١٨: ٢٠٢٣

السنة	نسبة المستخدمين من السكان (%)	عدد المستخدمين (مليون)
2018	54.60	53
2019	57.30	56.7
2020	71.90	75.7
2021	72.10	78.2
2022	72.20	79.6
2023	72.70	82

المصدر : World Bank Data, data.worldbank.org & DataReportal, www.datareportal.com

٣/٣ قابلية التعرض السيبراني

اعتمدت الدراسة على تقارير Kaspersky Security Bulletin لتقدير مدي قابلية البنية التحتية الرقمية في القطاعات المصـرية المختلفة للتعرض للخطر السـيبراني (جدول – ٣). حيث تظهر التقارير أن مصر من بين أكثر الدول تعرضاً لهجمات البرمجيات الخبيثة، الفدية، والهندسة الاجتماعية، مع نسب تهديد تتراوح من ٣٠٪ إلى ٣٥٪ سنوياً.

الجدول (٣) مؤشرات ضعف البنية السيبرانية حسب القطاع

القطاع	قابلية التعرض D_i	أبرز المخاطر حسب Kaspersky
البنوك	0.25	Phishing، Banking Malware
شركات التأمين	0.40	Social Engineering ،Data Theft
الشركات الصغيرة والمتوسطة	0.65	Ransomware، Endpoint Attacks
قطاع الاتصالات والتكنولوجيا	0.5	Botnets ،Web Exploits

المصدر : Kaspersky Security Bulletin Reports, www.kaspersky.com

٤/٣ شدة الخسائر S_i

استنادًا إلى تقارير من IBM Security و Allianz Cyber، تم تقدير متوسط تكلفة الحادثة السيبرانية الواحدة عالمياً بين ١,٠٠٠ – ٥,٠٠٠ دولار. ونظراً لانخفاض مستوى تغلغل التأمين السيبراني في مصر، تم اختيار الحد الأدنى من هذه القيمة (١,٠٠٠ دولار)، وتم تحويلها إلى الجنيه المصري بسعر صرف ٢٠٢٤:

$$S_i = 1000 \times 48 = 48{,}000 \text{ جنيه مصري/الحادثة}$$

٤- التطبيق الرياضي للنموذج

يشكل التطبيق الرياضي لنموذج **CBRT** المرحلة الأهم في هذه الدراسة، حيث ينتقل التحليل من الإطار المفاهيمي المجرد إلى التحقق العددي التطبيقي، بهدف اختبار فعالية النموذج في تقدير أقساط تأمينية تعكس الواقع العملي للسوق المصرية، مع مراعاة محدودية البيانات المحلية وتفاوت المخاطر عبر القطاعات. وتعد هذه المرحلة بمثابة منصة لتقييم مدى تواؤم النموذج مع خصائص الخطر السيبراني ، وكذلك قدرته على التكيف مع التغيرات في تكرار الحوادث، شدة الخسائر، وأنماط التغطية.

يعتمد هذا التطبيق علي مجموعة من البيانات الحقيقية التي تم جمعها وتحليلها من مصادر دولية موثوقة مثلTrend Micro ، Kaspersky، وIBM، وتم دمجها داخل الإطار الرياضي للنموذج. وقد تم تنظيم العلاقات بين المتغيرات الأساسية (مثل تكرار الحوادث، شدة الخسارة، وقابلية التعرض) داخل مصفوفات وحلقات حسابية تحاكي الهيكل الشرطي لاحتمالات وقوع الخطر، مع توظيف مكونات المخاطر الإحصائية والهيكل البنائي لـ CVaR لتمثيل المخاطر القصوى التي لا تغطيها النماذج الخطية التقليدية.

ويهدف هذا التطبيق إلى الإجابة عن مجموعة من الأسئلة المحورية، من بينها:

- ما القيمة العادلة للقسط التأميني السيبراني في كل قطاع؟
- كيف يتغير القسط عند تعديل معاملات التحفظ (α,β) أو عند تغيير مستوى الثقة (γ) ؟
- ما مدى قدرة النموذج على تقدير أقساط متوازنة تعكس كلاً من العدالة الاكتوارية والتحفظ الرقابي؟

ولتنفيذ هذه الحسابات، تم الاعتماد على بيئة برمجية مرنة مع توظيف مكتبات رياضية متقدمة لحساب المتوسط، التباين، وقيم الخطر المشروط .CVaR كما تم إدماج تقنية محاكاة Monte Carlo لتقدير المخاطر تحت سيناريوهات متعددة، مع تنفيذ تحليلات حساسية لقياس مدى استقرار النموذج. ويوفر هذا الدمج بين البنية البيزية والبرمجة العددية للنموذج بعداً تطبيقياً قوياً يجعله أداة قابلة للتكييف في بيئات اتخاذ القرار التأميني، لا سيما في الأسواق الناشئة ذات معلومات غير مكتملة مثل السوق المصري.

ولضمان دقة الحسابات وإمكانية تكرارها ديناميكياً، تم بناء النموذج البرمجي باستخدام لغة Python، بالاعتماد على المكتبات الرياضية التالية:

- استخدام مكتبة NumPy لحساب التوقعات والتباينات وتحليل سلاسل المتغيرات.
- تطبيق مكتبة SciPy لحساب CVaR عبر توليد توزيع احتمالي عبر محاكاة Monte Carlo.
- توليد مصفوفات متعددة تعكس قيمة الخسارة المحتملة لكل سيناريو قطاعي.

وقد تم تنفيذ النموذج على أربعة قطاعات هي: البنوك، شركات التأمين، الشركات الصغيرة والمتوسطة، والاتصالات. وتم احتساب الخسارة المتوقعة، التباين، وقيمة CVaR لكل منها كما في الجدول(٤):

جدول (٤): نتائج تطبيق النموذج حسب القطاع

القطاع	E[L] (جنيه مصري)	Var(L)	$CVaR_{0.95}$	متوسط القسط السنوي P (جنيه مصري)
البنوك	13,824	5,000,000	28,000	~770,824
التأمين	18,144	5,500,000	30,000	~840,144
الشركات الصغيرة والمتوسطة	29,040	6,000,000	35,000	~1,034,040
الاتصالات والتكنولوجيا	24,000	5,200,000	32,000	~915,000

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

وتعكس نتائج المعايرة التطبيقية للنموذج الاكتواري المقترح (CBRT) ما يلي :

- هناك تفاوتاً جوهرياً في قيمة الأقساط السنوية بين القطاعات الاقتصادية المختلفة، وهو تفاوت يمكن تفسيره من منظور اكتواري بحت استناداً إلى خصائص كل قطاع من حيث تكرار الحوادث السيبرانية(F_i) ، شدة الخسارة(S_i) ، وقابلية التعرض للمخاطر السيبرانية (D_i)، إضافة إلى نوع التغطية التأمينية المستخدمة.(C_i)
- تعد الشركات الصغيرة والمتوسط من أكثر القطاعات تعرضاً للمخاطر السيبرانية، وهو ما انعكس بوضوح في النموذج من خلال ارتفاع كل من $\boldsymbol{F}_i$ و $\boldsymbol{D}_i$ لهذا القطاع. فضعف نظم الحماية الإلكترونية، وانخفاض الاستثمارات في البنية التحتية الرقمية، فضلًا عن اعتماد هذه الشركات في كثير من الأحيان على برمجيات غير محدثة أو بدون دعم تقني مستمر، يؤدي إلى ارتفاع معدل الحوادث المحتملة. علاوة على ذلك، فإن نوع التغطية المتاح لهذا القطاع غالبًا ما يكون محدودا أو متوسطا، ما يزيد من حجم الخسائر التي تتحملها المنشأة نفسها قبل أن تفعل وثيقة التأمين، وبالتالي ترتفع القيمة المحسوبة للقسط استجابة لهذه المتغيرات. هذا الانعكاس يتماشى مع المبادئ الاكتوارية التي تنص على أن ارتفاع تكرار الحوادث وشدتها، مع ارتفاع قابلية التعرض، يؤدي إلى زيادة في القسط المطلوب لتغطية الخطر ضمن حدود الاستدامة المالية لشركة التأمين.
- على النقيض، تظهر نتائج النموذج أن قسط البنوك أقل نسبياً، وذلك رغم القيمة المالية المرتفعة لأصولها الرقمية. ويرجع ذلك إلى أمرين رئيسيين: أولاً، أن البنوك تطبق سياسات أمن إلكتروني صارمة تتضمن تحديثا دورياً للأنظمة، واستخدام تقنيات كشف التسلل، وفرق أمن سيبراني متخصصة، مما يؤدي إلى انخفاض معدل وقوع الحوادث .($\boldsymbol{F}_i$) ثانياً، أن التغطية التأمينية المتوفرة لهذا القطاع عادةً ما تكون شاملة($C_i = 3$) ، مما يقلل من عبء الخسارة المتوقع الذي تتحمله المنشأة، وهو ما ينعكس في قيمة أقل لدالة الوزن $w(C_i, D_i)$.وبالتالي، فإن انخفاض كل من D_i و$w(C_i, D_i)$، رغم شدة الخسارة المحتملة، يؤدي إلى قسط سنوي أقل مقارنة بالقطاعات الأخرى، بما يتماشى مع المبادئ الاكتوارية لتحديد القسط بناء على الخطر الصافي المحسوب بدقة.

- يظهر النموذج قدرة عالية على التمييز بين الأنماط المختلفة للمخاطر السيبرانية باختلاف القطاعات، ويعكس علاقات منطقية واتساقاً اكتوارياً مع المعايير المهنية المستخدمة في تسعير التأمين تحت ظروف عدم اليقين.

١/٤ تحليل الحساسية للنموذج الرياضي

يعد تحليل الحساسية خطوة هامة في تقييم مدى كفاءة ومرونة النموذج الرياضي المستخدم في تسعير التأمين السيبراني، خاصة في بيئات تتسم بعدم اليقين والتقلبات المتسارعة تتباين فيها أنماط الخطر باختلاف طبيعة القطاع. ويتيح تحليل الحساسية الكشف عن مدى حساسية الأقساط التأمينية للتغيرات في المعاملات الأساسية عبر قطاعات اقتصادية مختلفة، الأمر الذي يمكن صانعو القرار من ضبط سياسة التسعير وفقاً لطبيعة المخاطر التي تواجه القطاع ومستوى التحمل المطلوب.

وفي هذا السياق، تم إجراء تحليل حساسية شامل للنموذج الرياضي المقترح لحساب القسط للتأمين السيبراني، وذلك من خلال دراسة التغيرات في ثلاثة معاملات رئيسية:

١. معامل التحفظ :(α) يمثل هذا المعامل درجة تجنب المخاطر لدى شركة التأمين. فكلما زادت قيمته، دل ذلك على ميل أكبر نحو التحفظ وزيادة الاحتياط لمواجهة الخسائر غير المتوقعة.

٢. القيمة المتوقعة للخسارة :($E(L)$) وهي المتوسط الرياضي لقيمة الخسائر المحتملة، وتعد أحد أهم المدخلات التي تستند إليها الشركة في تقدير التزاماتها.

٣. الانحراف المعياري للخسارة :($\sigma(L)$) ويعكس هذا المؤشر مدى تشتت الخسائر حول متوسطها، ما يُعد مؤشرًا على درجة عدم اليقين في التقديرات.

١/١/٤ تحليل تأثير التغير في معامل التحفظ α

يمثل معامل α درجة تجنب المخاطر لشركة التأمين، ويستخدم لمعايرة هامش الأمان في تسعير القسط. وقد تم تطبيق تحليل الحساسية عن طريق زيادة معامل α تدريجياً من ١.٢٥ إلى ٢.٠٠ مع إبقاء ($E(L)$) و ($\sigma(L)$) ثابتين داخل كل قطاع (جدول – ٥) ، ومنه تبينما يلي:

جدول(٥) تأثير تغير معامل التحفظ α على القسط P

* القسط بالجنيه المصري

القطاع	α = 1.25	α = 1.50	α = 1.75	α = 2.00
البنوك	755,824	770,824	785,824	800,824
التأمين	820,144	840,144	860,144	880,144
الشركات الصغيرة والمتوسطة	1,004,040	1,034,040	1,064,040	1,094,040
الاتصالات والتكنولوجيا	890,000	915,000	940,000	965,000

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

- يزداد متوسط القسط السنوي بشكل منتظم مع ارتفاع قيمة معمل التحفظ α مما يعكس العلاقة الخطية الإيجابية بين معامل التحفظ ومتوسط القسط حيث انه كلما زاد تحفظ شركة التأمين تجاه المخاطر، كلما رفعت القسط لتعويض عدم اليقين في توقع الخسائر.
- الشركات الصغيرة والمتوسطة هي الأكثر تأثراً بزيادة α ، حيث يزداد القسط بمقدار 90,000 جنيه عند زيادة α من 1.25 إلى 2.00 .
- البنوك هي الأقل تأثراً، حيث لا يتجاوز الفارق في القسط لنفس الزيادة في α حاجز 45,000 جنيه (جدول – ٦) .

جدول (٦) الفروق المطلقة والنسبية بين $\alpha = 1.25$ و"$\alpha = 2.00$

القطاع	الفارق بين القسط عند $\alpha =$ 2.00 و $\alpha = 1.25$ (جنيه مصري)	نسبة الزيادة
البنوك	45,000	≈ 5.95%
التأمين	60,000	≈ 7.32%
الشركات الصغيرة والمتوسطة	90,000	≈ 8.96%
الاتصالات والتكنولوجيا	75,000	≈ 8.43%

المصدر: من إعداد الباحثتين

- يرجع هذا التفاوت في الأقساط بين القطاعات إلى اختلاف كل من القيمة المتوقعة للخسارة والانحراف المعياري لها. فالشركات الصغيرة والمتوسطة تُظهر تقلباً أكبر في حجم الخسائر، وهو ما يجعل تأثير معامل التحفظ أكثر وضوحاً عند حساب القسط ، مقارنة بالقطاعات الأخرى ذات المخاطر الأقل تقلباً.

٢/١/٤ تحليل تأثير التغير في القيمة المتوقعة للخسارة ($E(L)$)

في إطار اختبار مرونة النموذج وتحديد مدى تأثر القسط بالتغيرات المحتملة في القيمة المتوقعة للخسارة $E(L)$ ، تم إجراء تحليل حساسية يقوم على تعديل هذه القيمة بنسبة محددة مع الحفاظ على ثبات كل من معامل التحفظ α والانحراف المعياري للخسارة $\sigma(L)$ وقد تم اختيار نسبتي زيادة تمثلان سيناريوهين معقولين لارتفاع التكاليف المتوقعة أو زيادة حجم المطالبات، وهما ١٠٪ و٢٠٪، وذلك من أجل محاكاة تأثير تقلبات السوق أو تطورات المخاطر المرتبطة بكل قطاع (الجدول – ٧) ، ومنه تبين ما يلي:

جدول(٧) تأثير زيادة $E(L)$ على القسط

* القسط بالجنيه المصري

القطاع	بعد زيادة $E(L)$ 10%	القسط بعد زيادة $E(L)$ %10	بعد زيادة $E(L)$ 20%	القسط بعد زيادة $E(L)$ %20
البنوك	15,206	782,206	16,588	793,588
التأمين	19,958	859,958	21,772	879,772
الشركات الصغيرة والمتوسطة	31,944	1,056,944	34,848	1,079,848
الاتصالات والتكنولوجيا	26,400	938,400	28,800	961,800

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

- زيادة القيمة المتوقعة للخسارة بنسبة ١٠٪ و٢٠٪ انعكست مباشرة على القسط ، حيث ارتفعت قيمة القسط بنفس الاتجاه، وهو ما يعكس العلاقة الخطية بين $E(L)$ والقسط عند ثبات كل من α و$\sigma(L)$ هذه النتيجة تتسق مع النموذج الرياضي المستخدم.
- أظهر قطاع الاتصالات والتكنولوجيا أعلى نسبة زيادة في القسط (٢.٤٩٪) نتيجة لزيادة $E(L)$ ، مما يشير إلى تأثر كبير لحجم الخسارة المتوقعة على تسعير القسط في هذا القطاع (الجدزل– ٨) حيث أن جزءاً كبيراً من القسط يستمد من مؤشرات أخرى مثل التشتت (σ) أو الحدود القصوى للخسارة.
- في المقابل يشهد ، قطاع البنوك أقل نسبة زيادة في القسط (١.٤٦٪) بين القطاعات، مما يعكس درجة تحفظ أقل أو استقرار أعلى في توزيع الخسائر المتوقعة مقارنة بالقطاعات الأخرى.

جدول(٨) التحليل الكمي للفروق في الأقساط عند زيادة قيمة $E(L)$

القطاع	القسط عند زيادة ١٠٪ (جنيه)	القسط عند زيادة ٢٠٪ (جنيه)	الفرق المطلق في القسط (جنيه)	النسبة المئوية للزيادة (%)
قطاع البنوك	782,206	793,588	11,382	1.46%
قطاع التأمين	859,958	879,772	19,814	2.30%
قطاع الشركات الصغيرة والمتوسطة	1,056,944	1,079,848	22,904	2.17%
قطاع الاتصالات والتكنولوجيا	938,400	961,800	23,400	2.49%

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

٣/١/٤ تحليل تأثير التغير في الانحراف المعياري للخسارة σ(L)

تم إجراء تحليل كمي يظهر تأثير تعديل الانحراف المعياري بنسبة ±٢٠٪ على القسط في القطاعات الرئيسية بهدف قياس مدى استجابة القسط لهذه التغيرات، وتحديد القطاعات الأكثر حساسية للتقلبات في التشتت الإحصائي للخسائر(الجدول – ٩ و ١٠) ، ومنه تبين ما يلي:

جدول (٩) تحليل أثر التغير في الانحراف المعياري σ(L) بنسبة ±٢٠٪ على القسط.

* القسط بالجنيه المصري

القطاع	σ(L)	σ(L) -20%	القسط	σ(L) +20%	القسط
البنوك	~2,236	~1,789	748,824	~2,683	792,824
التأمين	~2,345	~1,876	818,144	~2,814	862,144
الشركات الصغيرة والمتوسطة	~2,449	~1,959	1,004,040	~2,939	1,064,040
الاتصالات والتكنولوجيا	~2,280	~1,824	895,000	~2,736	935,000

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

جدول (١٠) الفروقات الناتجة عن التغير في σ(L)

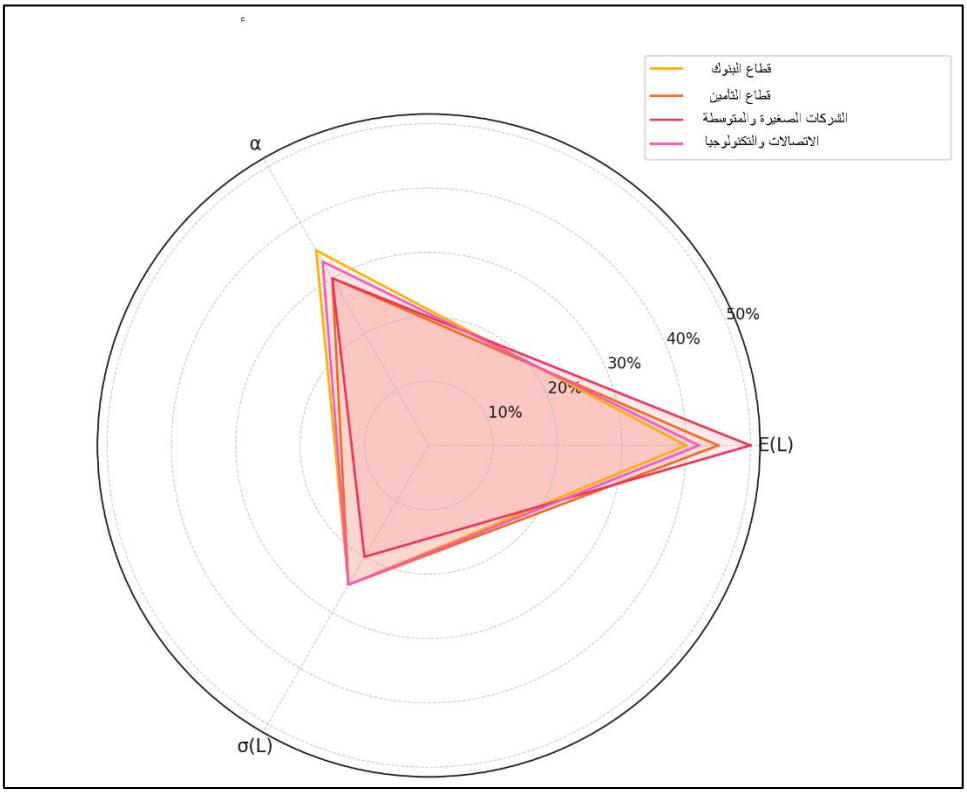
* القسط بالجنيه المصري

القطاع	القسط عند -٢٠٪	القسط عند +٢٠٪	الفرق المطلق	الفرق النسبي (%)
قطاع البنوك	748,824	792,824	44,000	5.88%
قطاع التأمين	818,144	862,144	44,000	5.38%
قطاع الشركات الصغيرة والمتوسطة	1,004,040	1,064,040	60,000	5.97%
قطاع الاتصالات والتكنولوجيا	895,000	935,000	40,000	4.47%

المصدر: مخرجات تطبيق النموذج باستخدام لغة البرمجة Python

- وجود علاقة طردية بين قيمة الانحراف المعياري للخسارة والقسط ، فكلما زاد الانحراف المعياري بنسبة ٢٠٪ ارتفع القسط ، والعكس صحيح.
- قطاع الشركات الصغيرة والمتوسطة هو الأكثر تأثراً بتغير الانحراف المعياري، حيث بلغ الفرق المطلق في القسط نتيجة التغير ±٢٠٪ نحو ٦٠٠٠٠ جنيه، بنسبة تغير تقدر بـ ٥,٩٧٪، مما يشير إلى حساسية هذا القطاع العالية تجاه تقلبات الخسارة.
- قطاع الاتصالات والتكنولوجيا هو الأقل تأثراً، حيث بلغ الفرق المطلق في القسط الناتج عن تغير الانحراف المعياري ±٢٠٪ نحو ٤٠٠٠٠ جنيه فقط، وبنسبة تغير ٤.٤٧٪.
- قطاعات البنوك والتأمين تأثرت بدرجة متقاربة، إذ سجل كل منهما فرقًا مطلقًا في القسط بمقدار ٤٤٠٠٠ جنيه، إلا أن نسبة التغير في قطاع البنوك كانت أعلى قليلاً ٥.٨٨٪ مقارنة بقطاع التأمين ٥.٣٨٪.

ويوضح الشكل (٢) تمثيلاً بصريا لمدى حساسية القسط وتوزيع مستويات الحساسية النسبية للأقساط تجاه التغير في كل من المعاملات الثلاثة الأساسية :القيمة المتوقعة للخسارة$E(L)$ ، ومعامل الحذرα ، والانحراف المعياري للخسارة$\sigma(L)$ ، وذلك عبر القطاعات الأربعة محل الدراسة.



المصدر: من إعداد الباحثتين.

شكل (٢) مخطط رادار Radar Chart يوضح مستوى حساسية الأقساط لتغي كل من α و $E(L)$ و σ(L)

٢/٤ بناء النموذج المؤسسي لتسعير التأمين السيبراني

على الرغم من أهمية احتساب الأقساط التأمينية على مستوى القطاع في تقديم صورة عامة عن توزيع المخاطر، إلا أن التركيز الأكبر من جانب شـــركات التأمين ينصـــب في الغالب على حساب قسط التأمين السيبراني للوحدة الاقتصادية، بوصفه الأداة الأكثر دقة لتسعير الخطر وتحديد شروط التغطية على نحو مخصص. ويعد هذا الانتقال من التحليل الكلي إلى التحليل الجزئي عند مســـتوى الوحدة الاقتصـــادية نقلة منهجية تعكس التوجه نحو التخصـــيص في إدارة المخاطر، خصوصاً في بيئات تتسم بتنوع مستويات الحماية التقنية، والبنى التحتية، ونوع البيانات المتداولة. وبذلك، يتيح حساب القسط على مستوى المؤسسة تمثيلاً أكثر صدقاً لعوامل الخطر، مما يساهم في تحسين دقة التسعير، وتقديم عروض تأمينية أكثر اتساقاً مع احتياجات كل عميل على حدة، سواء من حيث التكلفة أو نطاق التغطية.

فعلى عكس النمذجة القطاعية التي تفترض تجانساً نسبياً بين الوحدات الاقتصادية داخل القطاع الواحد، فإن تحليل القسط على مستوى المؤسسة يتيح نمذجة دقيقة لمكونات الخطر الفعلية، ما يعزز من دقة التسعير واستهدافه.

وفي هذا السياق، يستخدم النموذج المقترح لتقدير الخسارة الكلية المتوقعة L_i للمؤسسة بناء على معطيات خاصة بها، تشمل:

- **تكرار الحوادث السيبرانية** : F_i والذي يمكن تقديره من خلال سجل الحوادث التاريخي للمؤسسة أو متوسطات مشابهة لمؤسسات مماثلة في الحجم والنشاط. وإن لم تكن هناك بيانات داخلية من المؤسسة، يمكن استخدام نسب التهديد على عدد الأجهزة المتصلة بالشبكة كبديل تقريبي
- **شدة الخسارة** : S_i وتستخلص إما من بيانات محاسبية أو تقديرات معيارية تأخذ في الاعتبار تكلفة التعطل، استرداد الأنظمة، وفقدان السمعة. وكذلك يمكن استخدام متوسط الشدة في القطاع المنتمي إليه المؤسسة.
- **قابلية التعرض** :D_i والتي تعكس هشاشة البنية التحتية الرقمية ووجود أو غياب إجراءات الأمن السيبراني. ويمكن حسابها من خلال تقارير تقييم داخلية تقارير مثل تقارير Kaspersky.
- **نوع التغطية التأمينية** : C_i والتي تحدد نطاق الحماية التأمينية، سواء كانت محدودة أو شاملة أو متوسطة، بما يؤثر على حجم التكاليف التي تقع على عاتق شركة التأمين.

ويمكن بناء نموذج التسعير باستخدام لغة Python وفق الكود البرمجي التالي

```
# [1] Inputs
F_i = ...    # Frequency of cyber incidents per year
S_i = ...    # Expected loss severity per incident (EGP)
D_i = ...    # Vulnerability coefficient (0 to 1)
C_i = ...    # Coverage type (1 = Limited, 2 = Moderate, 3 = Comprehensive)
# [2] Weight function w(C_i, D_i)
def weight_function(C, D):
    if C == 1:
        return 0.9 + D
    elif C == 2:
        return 0.8 + D
    elif C == 3:
        return 0.6 + D
    else:
        return 1.0
w_i = weight_function(C_i, D_i)
# [3] Expected annual loss
E_L = F_i * S_i * w_i
# [4] Risk loading parameters
alpha = ...
beta = ...
gamma = ...
# [5] Risk measures
Var_L = ...
CVaR_L = ...
# [6] Annual premium calculation
P = E_L + alpha * Var_L + beta * CVaR_L
# [7] Output
print("Expected annual loss E[L]:", round(E_L, 2), "EGP")
print("Final premium P:", round(P, 2), "EGP")
```

المصدر: بناء النموذج باستخدام لغة البرمجة Python

٥- النتائج والتوصيات

٥/١ النتائج

توصلت الدراسة إلى عدد من النتائج التي تسلط الضوء على واقع تسعير التأمين السيبراني في السوق المصرية، لا سيما في ظل بيئة تتسم بعدم اكتمال المعلومات وتعدد مصادر المخاطر. وقد أظهرت النتائج ما يلي:

- أن النماذج التي دمجت الجبر الاحتمالي (مثل فضاءات الاحتمالات المرتبطة بالمصفوفات والتحولات الخطية) مع النماذج الاكتوارية عن نتائج أكثر دقة ومرونة في تقدير القسط السيبراني. إذ استطاعت هذه النماذج تقديم تسعير يعتمد على توزيع المخاطر الهيكلية بدلًا من التوزيع الكلاسيكي، ما أتاح تمثيلاً أفضل للواقع السيبراني المعقد.
- وجود معلومات غير مكتملة حول حوادث الاختراق السيبرانية السابقة، وشدة التأثير المالي، ونقاط الضعف في أنظمة العملاء، يؤدي إلى تباين كبير في تسعير الأقساط. وتبين أن تجاهل هذا التباين يؤدي إلى إما تسعير مفرط يزيد العبء على الشركات، أو تسعير ناقص يعرض شركات التأمين للخسارة.
- أن محاكاة الأحداث المستقبلية باستخدام سلاسل ماركوف أو النماذج الاحتمالية المركبة يمكن شركات التأمين من اختبار مدى حساسية الأقساط لأي تغيّر في تواتر أو شدة الهجمات، وبالتالي اتخاذ قرارات تسعيرية أكثر مرونة واستباقية.
- السوق المصري يعاني من نقص في البيانات السيبرانية المنظمة كنتيجة لضعف البنية التحتية المعلوماتية فيما يخص تجميع البيانات المتعلقة بالحوادث السيبرانية، سواء على مستوى الشركات أو على مستوى الهيئات التنظيمية، مما يعد من أكبر التحديات أمام تفعيل نماذج تسعير دقيقة وموثوقة.
- يتسم النموذج المقترح ببنية رياضية تمزج بين نظرية الاحتمالات والجبر الخطي، حيث تم استخدام المصفوفات لتمثيل حالات عدم اليقين، وتطبيق دوال التوزيع الاحتمالي لقياس المخاطر، مما مكن من بناء نموذج مرن قادر على التكيف مع بيئات معلوماتية غير مكتملة أو متقلبة.

- قابلية النموذج للتوسع والتعديل البنيوي، حيث أن تصميمه المعتمد على وحدات رياضية مستقلة Modules يسمح بتوسيع النموذج ليشمل أنواعاً مختلفة من المخاطر، مثل مخاطر السوق أو مخاطر التشغيل، وذلك دون الحاجة إلى إعادة بناء النموذج من الأساس، مما يعزز من قابلية التكيف والتطوير المستقبلي.
- سمحت البنية الطبقية للنموذج المقترح بدمج سيناريوهات متعددة عبر طبقات تحليلية مختلفة، وهو ما أتاح تمثيل ديناميكي لتطور المخاطر بمرور الوقت. وقد تم دعم هذه البنية عبر معاملات مرجحة Weighted Parameters تتغير بحسب شدة التهديد وتكراره، وهو ما يشير إلى كفاءة التصميم البنيوي في احتواء التعقيد.
- أثبت النموذج فعالية ملحوظة في حالات محدودية البيانات، حيث تم تعويض نقص البيانات من خلال تطبيق تقنيات استدلال بايزي (Bayesian Inference) داخل بنيته الرياضية، مما مكن النموذج من توليد توزيع احتمالي محدث باستمرار بناء على البيانات المتاحة، وهو ما يعكس كفاءة التصميم البنيوي في العمل تحت ظروف عدم يقين عالية.
- تستجيب الأقساط بشكل طردي وواضح لزيادة $E(L)$ فمع زيادة متوقعة بنسبة ١٠٪ و٢٠٪ في الخسائر، زادت الأقساط في جميع القطاعات بنسبة قريبة من نسب الزيادة، ما يعكس حساسية النموذج العالية لهذا المتغير. حيث كانت أعلى استجابة مسجلة في قطاع البنوك، بينما سجل قطاع الشركات الصغيرة والمتوسطة أقل استجابة، ما يشير إلى تفاوت في البنية المخاطرية لهذه القطاعات.
- استجابة الأقساط لتغير الانحراف المعياري $\sigma(L)$ حيث انه عند تعديل $\sigma(L)$بنسبة ±٢٠٪، مع تثبيت باقي المتغيرات، أظهرت النتائج تغيرات ملحوظة في القسط ، لكنها أقل حدة من تلك الناتجة عن تعديل $E(L)$ ، وتعكس هذه النتيجة تأثيراً غير مباشر للتقلبات، إذ يلعب معامل α دوراً مضاعفاً في تضخيم أثر هذه التغيرات، خصوصاً في القطاعات ذات الحساسية المرتفعة مثل التأمين والتكنولوجيا.
- يظهر التحليل المقارن عبر القطاعات الاختلافات النسبية في استجابات الأقساط. حيث يحتل قطاع الشركات الصغيرة والمتوسطة وقطاع الاتصالات والتكنولوجيا القيم الأعلى

للقسط في معظم السيناريوهات، مما يشير إلى تقييم أكبر لمستوى المخاطر فيهما، بينما يظهر قطاع البنوك بانتظام عند القيم الأدنى، نظراً لخفض قيمة $E(L)$ و$\sigma(L)$ نسبياً.

- قد يؤدي ارتفاع الأقساط بسبب تحفظ النموذج في قطاع مثل الشركات الصغيرة والمتوسطة إلى عزوف العملاء، لذا ينصح باستخدام أدوات موازية مثل إعادة التأمين أو استخدام توزيعات خسارة بديلة لتقليل الحساسية دون المساس بالحماية المالية. كما يمكن استخدام هذه النتائج من قِبل الجهات الرقابية لفرض ضوابط على سياسة التسعير في السوق، بما يضمن عدم استغلال معاملات التحفظ لرفع الأقساط بشكل غير مبرر في قطاعات ذات قدرات دفع محدودة.
- أظهر النموذج إمكانات عالية للمواءمة مع نماذج الذكاء الاصطناعي حيث يمكن أن يشكل بنية رياضية تمهيدية جيدة لإدماجه مع خوارزميات تعلم الآلة، خاصة خوارزميات الانحدار الاحتمالي العميق(Deep Probabilistic Regression) ، مما يفتح آفاقاً مستقبلية لتوسيع البنية نحو بناء نموذج ديناميكي ذاتي التعلم يعتمد على البيانات الحية من السوق.

٢/٥ التوصيات

انطلاقاً من النتائج التي توصل إليها هذا البحث، والتي كشفت عن أهمية بناء نموذج رياضي مرن وذكي لتسعير التأمين السيبراني في بيئة تتسم بعدم اليقين وتقلب معايير الخطر، تبرز الحاجة إلى تقديم توصيات علمية وعملية تساعد صناع القرار في شركات التأمين، والباحثين في مجالات العلوم الاكتوارية، في تطوير أدوات تسعير قادرة على التكيف مع التحديات الديناميكية المعاصرة. وتعزز هذه التوصيات من كفاءة النماذج الرياضية القائمة، وتفتح آفاقاً لتكامل الجبر الاحتمالي مع تقنيات الذكاء الاصطناعي والتحليل السيناريوي من أجل نمذجة المخاطر السيبرانية بصورة أكثر دقة وتكيفاً. وعلي ذلك فإن الدراسة توصي بما يلي:

- إنشاء قاعدة بيانات متخصصة بالحوادث السيبرانية تعنى بتجميع وتحديث البيانات المتعلقة بالحوادث السيبرانية في مصر، بما يشمل تكرار الهجمات، أنواعها، الخسائر المترتبة عليها، وطرق المعالجة. وذلك لضمان توفر مدخلات موثوقة لبناء نماذج تسعير دقيقة.

- اعتماد النماذج الاكتوارية المستندة إلى الجبر الاحتمالي وتحليل المصفوفات، بما يضمن نمذجة أكثر دقة للعلاقات بين مكونات الخطر السيبراني، لا سيما في البيئات التي تتسم بعدم اليقين وعدم اكتمال المعلومات.
- إلزام الشركات الراغبة في الحصول على تأمين سيبراني بالإفصاح عن خريطة بنيتها التحتية السيبرانية، ومستوى الأمان، والإجراءات الاحترازية المطبقة، بما يسهم في بناء نموذج تسعيري يعتمد على مخاطرة حقيقية وليس مفترضة كشرط للتأمين
- تحفيز الاستثمار في التأمين السيبراني من خلال الحوافز التنظيمية، بأن تقوم الهيئات الرقابية، مثل الهيئة العامة للرقابة المالية، بمنح حوافز تنظيمية أو ضريبية للشركات التي تشتري وثائق تأمين سيبراني، مما يشجع انتشار هذه الثقافة في السوق المحلي.
- تطوير وثائق تأمين سيبراني تأخذ في الحسبان اختلاف القطاعات الاقتصادية، وطبيعة البيانات المخزنة، وآليات إدارة المخاطر الرقمية لدى كل شركة، بحيث لا يكون القسط نمطياً بل مبنياً على خصائص العميل بشكل دقيق.
- تفعيل دور الذكاء الاصطناعي في دعم القرار التسعيري من خلال استخدام تقنيات التعلم الآلي Machine Learning لتحليل السلوك السيبراني، والتنبؤ بأنماط الهجمات، مما يساهم في تعزيز القدرة على التسعير الديناميكي، والتكيف الفوري مع تغير المخاطر.
- نظراً للطبيعة المتغيرة والمركبة للتحديات السيبرانية، وتطور أساليب النمذجة الكمية والاحتمالية، فإن هذا البحث يفتح المجال أمام الباحثين في المستقبل لتوسيع نطاق الدراسة من خلال استكشاف اتجاهات أكثر تعقيداً في تصميم نماذج تسعير التأمين السيبراني وتعميق الفهم النظري والتطبيقي لمنهجيات تسعير المخاطر، وبخاصة في بيئات يغلب عليها عدم التماثل المعلوماتي والتقلب الشديد، مع إمكانية توظيف أدوات رياضية وهندسية متقدمة، ودمجها بتقنيات الذكاء الاصطناعي وتحليل البيانات الكبيرة . وذلك من خلال توسيع النموذج ليشمل التأمين ضد المخاطر الرقمية غير التقليدية مثل مخاطر الذكاء الاصطناعي التوليدي، والهجمات العشوائية الناتجة عن نماذج لغوية

المراجع

1- Allianz Global Corporate & Specialty. (2023). *Allianz Risk Barometer 2023*. Retrieved from https://www.agcs.allianz.com

2- Allianz Global Corporate & Specialty. (2023). *Cyber Risk Trends: The Cloud Wildcard*. Retrieved from www.agcs.allianz.com

3- Allianz Global Corporate & Specialty. (2024). *Allianz Risk Barometer 2024*. Retrieved from https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

4- Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modeling and pricing cyber insurance. *European Actuarial Journal, 13*, 1–53.

5- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice, 40*(1), 131–158.

6- Blanchet, J., Kang, Y., & Murthy, K. (2019). Robust Wasserstein profile inference and applications to machine learning. *Journal of Applied Probability, 56*(3), 830–857.

7- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. *Workshop on the Economics of Information Security (WEIS)*.

8- Central Bank of Egypt. (2024). *Official Exchange Rates*. Retrieved from https://www.cbe.org.eg

9- DataReportal. (2022). *Digital 2022: Egypt*. Retrieved from https://datareportal.com/reports/digital-2022-egypt

10- Delage, E., & Ye, Y. (2010). Distributionally robust optimization under moment uncertainty with application to data-driven problems. *Operations Research, 58*(3), 595–612.

11- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

12- Eling, M., & Wirfs, J. H. (2019). What are the actual costs of cyber risk events? *The Geneva Papers on Risk and Insurance – Issues and Practice, 44*(4), 499–524.

13- ENISA. (2023). *Threat Landscape for Supply Chain Attacks*. European Union Agency for Cybersecurity.

14- IBM Security. (2023). *Cost of a Data Breach Report 2023*. Ponemon Institute. Retrieved from https://www.ibm.com/reports/data-breach

15- Information technology — Security techniques — Guidelines for cybersecurity. International Organization for Standardization. Retrieved from https://www.iso.org/standard/44375.html

16- Kaas, R., Goovaerts, M. J., Dhaene, J., & Denuit, M. (2008). *Modern Actuarial Risk Theory: Using R*. Springer.

17- Kaspersky Lab. (2022–2023). *Kaspersky Security Bulletin*. Retrieved from https://www.kaspersky.com/blog/tag/security-bulletin

18- Kott, A. (2020). *Toward a Science of Cybersecurity*. Springer.

19- Liu, Y., Maillart, L., & Sicker, D. (2020). The impact of security investment on cyber insurance markets. *Risk Analysis, 40*(5), 1044–1062.

20- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity, 5*(1).

21- The World Bank. (2018–2023). Individuals using the Internet (% of population) – Egypt. Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EG

22- Trend Micro. (2018, 2020, 2022, 2023). *Trend Micro Annual Cybersecurity Threat Reports*. Retrieved from https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports

23- Wüthrich, M. V., & Merz, M. (2008). *Stochastic Claims Reserving Methods in Insurance*. Wiley.