

الأمن السيبراني: ضرورة حتمية لتعزيز الشمول المالي الرقمي والاستقرار المالي

Cybersecurity: An imperative necessity to enhance digital financial inclusion and financial stability

بن عيني رحيمة¹، سلكة براهيم²

¹ المركز الجامعي مغنية(الجزائر)، r.benaini@cu-maghnia.dz

² المركز الجامعي مغنية(الجزائر)، b.selka@cu-maghnia.dz

تاريخ النشر: 2025/12/25

تاريخ القبول: 2025/12/17

تاريخ الاستلام: 2025/11/18

ملخص:

تهدف هذه الدراسة إلى إبراز أهمية تحقيق الأمن السيبراني بالقطاع المصرفي والمالي، ودوره في تعزيز الشمول المالي وتحقيق الاستقرار المالي، وتسلط الضوء على أهم التهديدات السيبرانية التي تستهدف هذا القطاع وتؤثر عليه، وسبل مواجهتها. وخلصت الدراسة إلى أن التطور التكنولوجي في القطاع المالي يصاحبه تطور في أنواع المخاطر والتهديدات السيبرانية، وأنه من أجل تحقيق الاستقرار والشمول المالي من الضروري التوفيق والموازنة بين فرص وإيجابيات التكنولوجيا المالية وبين تحدياتها ومخاطرها السيبرانية.

كلمات مفتاحية: كلمة الأمن السيبراني، الشمول المالي، الاستقرار المالي.

Abstract:

This study aims to highlight the importance of financial technology, Digitalization of the banking and financial sector, And their role in achieving financial inclusion, and Shedding light on the most important cyber threats targeting and affecting this sector, and ways to confront them.

The study concluded that the technological development in the financial sector is accompanied by a development in the types of cyber risks and threats, and that in order to achieve financial stability and inclusion, it is necessary to balance the opportunities and cyber risks of financial technology.

Keywords: financial inclusion ; cybersecurity ;financial stability

بن عيني رحيمة، r.benaini@cu-maghnia.dz

1. مقدمة:

تعتبر التكنولوجيا المالية آخر التطورات في القطاع المالي والمصرفي، إذ يمثل هذا الأخير مجال التركيز بالنسبة لشركات التكنولوجيا نظرا للطبيعة غير المادية للأنشطة المالية، وتمثل بدورها التكنولوجيا أحد البنود الضخمة في موازنات البنوك وشركات القطاع المالي الأخرى، وقد ساعدت تطبيقات التكنولوجيا المالية على تسهيل تقديم الخدمات المالية للعملاء، وإحلال الطرق التقليدية بطرق حديثة ومتطورة كأجهزة الصراف الآلي، بطاقات الائتمان والخصم، الصيرفة الإلكترونية وغيرها من الطرق.

ونجحت الشركات الناشئة في مجال التكنولوجيا المالية في تقديم حزمة متنوعة من الخدمات المالية تتضمن خدمات المدفوعات، والإقراض، والتوفير، وتحويل الأموال، والتمويل الجماعي، والعملات الرقمية، إضافة إلى إدارة الثروات وخدمات التأمين، وأصبحت بذلك منافسا قويا للبنوك والمؤسسات المالية، إلا أن مصلحة الطرفين دفعت بهما إلى التشارك والتعاون بدلا من التنافس، فالبنوك تمتلك ثقة العملاء والشركات الناشئة تمتلك الابتكار والتكنولوجيا الحديثة، والمكسب الأهم لهذا التفاعل بين التكنولوجيا والقطاع المالي يتمثل في زيادة نسبة المستخدمين الذين يصلون إلى الخدمات المالية ويستفيدون منها وبالتالي رفع نسب الشمول المالي.

رغم التقدم الكبير الذي حققته الخدمات المالية الرقمية في إرساء الشمول المالي، إلا أنها توفر أيضا للقراصنة بيئة غنية بالأهداف، إذ أن الهجمة السيبرانية تشكل تهديدا للنظام المالي وتعطيلا للخدمات المالية الضرورية، وتقويضا للأمن والثقة، وتعرض الاستقرار المالي للخطر، فعلى الرغم من تعدد فوائد التكنولوجيا المالية على المؤسسات المالية والعملاء فإنه لا يمكن التوسع في الابتكار على حساب الأمن، لذا من الضروري خلق توازن بين تجنب المخاطر والتوسع في ابتكارات التكنولوجيا المالية والرقمنة، والتأكد من عدم تحول الابتكارات التكنولوجية إلى أدوات للاحتيال والقرصنة وتهديدا للاستقرار المالي.

و تعتبر البنوك من أكثر المؤسسات المالية التي تولي عناية خاصة وكبيرة لإدارة مخاطر الأمن السيبراني؛ لأن الآثار المحتملة للاختراق السيبراني تنطوي على تعرض البنوك لخسائر مالية مباشرة وغير مباشرة ناجمة عن الهجمات السيبرانية، وتعطيل الأعمال، والضرر على السمعة، وغيرها، ولا يمكن بأي

حال من الأحوال إغفال المخاطر المتزايدة للهجمات السيبرانية التي تعتبر البنوك هدفا جذابا لها نظرا لدورها الحيوي في الوساطة المالية، ما قد يهدد الاستقرار والشمول المالي، ومن هذا المنطلق تمكن مشكلة الدراسة من خلال طرح التساؤل التالي:

وعلى ضوء ما تقدم نقوم بطرح الاشكالية التالية: ما مدى تأثير مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي الرقمي؟

هدف البحث:

نهدف من خلال هذه الورقة البحثية التعرض لأهم الهجمات والمخاطر السيبرانية التي تتعرض لها الأنظمة المالية والمصرفية، وكيف يمكن جني منافع الابتكار الرقمي من أجل تحقيق الشمول المالي في ظل المخاطر التي تحملها التكنولوجيا المالية والتي تهدد الاستقرار المالي والشمول المالي.

منهج البحث

لدراسة الاشكالية المطروحة تم اعتماد المنهج الوصفي التحليلي للتعرف على المخاطر السيبرانية التي تواجه القطاع المصرفي والمالي، وتحليل مدى تأثير هذه المخاطر على تعزيز الشمول المالي الرقمي والاستقرار المالي.

محاور البحث

للإلمام بجوانب الموضوع والإجابة على الإشكالية تم تقسيم البحث إلى 3 محاور رئيسية:

1. المخاطر السيبرانية لرقمنة الجهاز المصرفي والمالي
2. تحليل أثر مخاطر الأمن السيبراني على الشمول المالي والاستقرار المالي
3. استراتيجيات تحقيق الأمن السيبراني في القطاع المالي.

2. المخاطر السيبرانية لرقمنة الجهاز المصرفي والمالي :

1.1 تعريف المخاطر الالكترونية:

تعتبر المخاطر الإلكترونية شكلا من أشكال المخاطر التشغيلية وتعرف على أنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن الحوادث الداخلية والخارجية. أو أطراف أخرى، بما في ذلك السرقة أو

النزاهة المعرضة للخطر أو تلف المعلومات ، والاحتيايل الداخلي والخارجي، وتعطيل الأعمال. وهذا التعريف يتوافق إلى حد كبير مع جهود القطاع الخاص المتزامنة المعروفة لتحديد المخاطر السيبرانية، على سبيل المثال. و قد تؤدي حوادث المخاطر السيبرانية إلى إضعاف سرية وسلامة وتوافر البيانات والمعلومات، والتشغيل السليم للبنية التحتية لتكنولوجيا المعلومات. وعليه فان المخاطر السيبرانية على مؤسسات القطاع المالي هي مخاطر تشغيلية على أصول المعلومات والتكنولوجيا.

2.2 أنواع التهديدات السيبرانية على القطاع المصرفي:

• البرمجيات الخبيثة: Malware

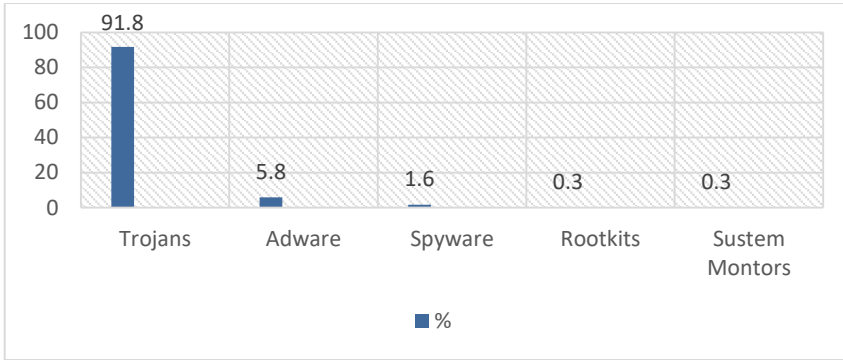
البرمجيات الخبيثة مصطلح عام يستعمل لوصف كل أنواع البرمجيات التي يمكن أن تجلب ضررا أو تسرق بيانات من جهاز الحوسبة المستهدف، والبرمجيات الخبيثة عديدة ومتعددة منها: الفيروسات، الديدان، هجمات الفدية، الاصطياد المشفر، برامج الخداع، برامج التجسس، أحصنة طروادة، الأبواب الخلفية، الجذور الخفية، الروبوتات.... (A.Hassan, 2019,, p. 09)، وسنقوم في هذا البحث بالتطرق لأشهر البرمجيات الخبيثة التي تتعرض لها الأنظمة المالية.

• البرمجيات الخبيثة عبر الهاتف المحمول Mobile Malware

يتزايد الاحتيايل في الخدمات المصرفية عبر الهاتف المحمول مع تزايد استخدام العملاء للتطبيقات المصرفية وأنظمة الدفع عبره، وسيصبح قريبا أكثر انتشارا من الاحتيايل التقليدي لبطاقات الائتمان، إذ بين 2016 و2018 تضاعفت هجمات البرمجيات الخبيثة عبر الهاتف المحمول إلى 3 أضعاف، ففي 2018 9.9 مليار مستخدم على الأقل تأثروا بالبرمجيات الخبيثة عبر الهاتف المحمول خصوصا الخاصة بالخدمات المصرفية. (Silvia Baur-yazbeck, 2019, p. 07)

ومن أكثر البرمجيات الخبيثة التي تتعرض لها الهواتف المحمولة بصفة عامة: أحصنة طروادة كما هو مبين في الشكل التالي:

الشكل رقم (2): تطبيقات الهاتف المحمول الضارة



Source : (Lonas, 2020, p. 20)

● أحصنة طروادة Trojan Horses

هو أكبر فئة من عائلة البرامج الضارة، هدفه سرقة المعلومات القيمة والتحكم في النظام، إذ يتم استخدام أحصنة طروادة للحصول على موطن قدم أولي وتنزيل برامج ضارة أخرى. (council, 2021, p. 16)

● أحصنة طروادة المصرفية

أثناء استخدام الخدمات المصرفية الإلكترونية أو عبر الهاتف المحمول، أحصنة طروادة المصرفية قادرة على اختطاف المتصفح والعبث بالمعاملات المالية أو سرقة بيانات اعتماد المستخدم أثناء استخدام خدمات بنكية، كما يمكن إرسال حصان طروادة المصرفي من خلال مرفقات في البريد الإلكتروني أو البرامج المصابة. (council, 2021, p. 16)

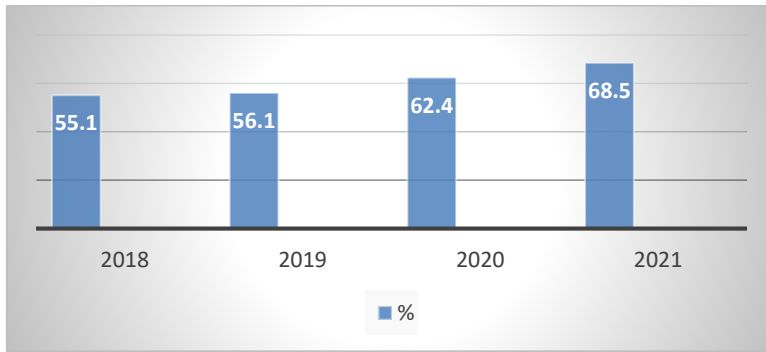
● هجمة الفدية Ransomware

من أحدث وأخطر البرمجيات الخبيثة "هجمة الفدية" أو ما يسمى بـ "الابتزاز الرقمي"، وهي نوع من البرامج الخبيثة يمنع أو يعيق وصول المستخدمين لموارد جهاز الحوسبة و/أو البيانات الشخصية (سواء كان كمبيوتر، خادم، لوحة إلكترونية، هاتف ذكي أو جهاز انترنت الأشياء) عن طريق تشفير الملفات.

(A.Hassan, 2019,, p. 09) ، هجمة الفدية لا تهدف لاحداث أضرار على نظام الملفات وإنما هدفها الدائم هو النكود، وعلى غير أنواع الهجمات الأخرى، يتم إخطار الضحية بشكل تقليدي بحدوث استغلال، ويطلب المجرم خلف البرنامج فدية، ويقوم بإعطاء تعليمات الدفع للضحية من أجل فك التشفير وإعادة البيانات لوضعها الطبيعي. (Mark Stamp, 2021, p. 166)

برامج الفدية هي أخطر البرامج اليوم وأسرعها انتشارا، فحسب دراسة أجرتها Kaspersky أن هذا البرنامج في تزايد مستمر ومن المقدر أن الأعمال ستعرض لهذه الهجمة كل 11 ثانية، والشكل الموالي يبين مدى استمرارية تزايد نسبة تعرض المؤسسات لها.

الشكل رقم (3): نسبة المؤسسات التي تعرضت لهجمة الفدية في العالم بين 2018 و2021

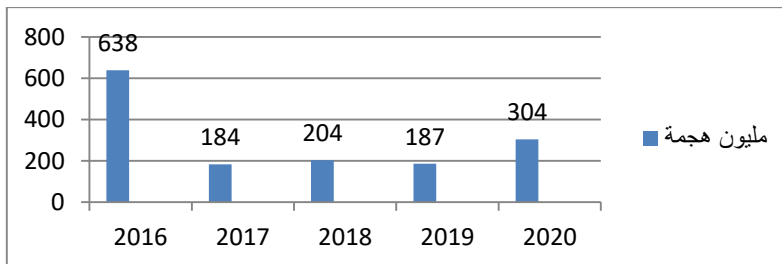


المصدر: من إعداد الباحثة إعتقادا على بيانات موقع STATISTA

<https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/>

أما بالنسبة لعدد الهجمات فقد ارتفعت ارتفاعا مهولا في سنة 2020

الشكل رقم (4): عدد هجمات برنامج الفدية من 2016-2020



المصدر: من إعداد الباحثة إعتقادا على بيانات موقع STATISTA

<https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/>

سجلت سنة 2020 304 مليون هجمة فدية في العالم، إذ ارتفع عدد الهجمات ب 62% عن 2019 وسجلت ثاني أعلى معدل بعد 2016.

• الروبوتات Botnet

الروبوتات عبارة عن مجموعة من الأجهزة المتصلة بالانترنت تم اختراقها بواسطة مهاجم دون علم الضحية، تعمل شبكات الروبوت كمضاعف قوة للنشاط الضار، في الوقت الحاضر يبدو أن الروبوتات تركز عليها أكثر فأكثر برامج الفدية الضارة وليس الأنشطة المتعلقة بالاحتيال. (council, 2021, p. 30) ويتمثل خطر البوت نت في سيطرة شخص أو مجموعة يعرف بالمتحكم (Master) على شبكات ضخمة من الأجهزة الحاسوبية ربما يبلغ عددها الآلاف بل حتى الملايين، ويمكن لذلك المتحكم أن يطلب من تلك الأجهزة القيام في توقيت محدد عن طريق برنامج تحكم يطلق عليه برنامج السيطرة والتحكم بتنفيذ أوامر معينة لأغراض تجارية أو تخريبية، وتتم كل هذه الأمور بشكل خفي عن مستخدمي الأجهزة. (العزب، 2018).

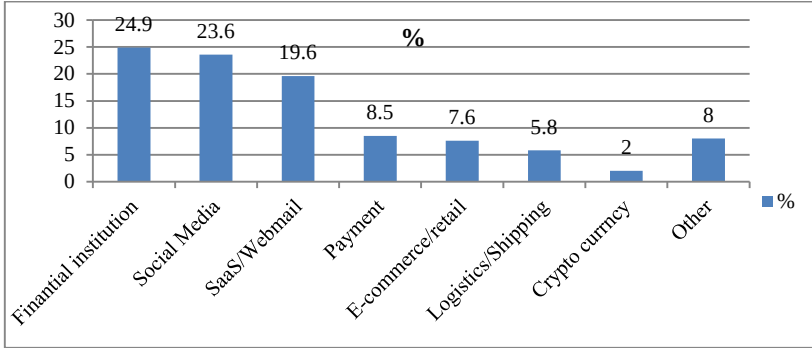
• التصيد Phishing

هي ممارسة احتيالية يستخدم فيها المحتالون طعم البريد الإلكتروني "للاحتيال" عن طريق التكرار في شكل كيان جدير بالثقة، فيقومون بإرسال رسائل بريد إلكتروني إلى أشخاص أبرياء، يدعون أنها من مصادر شرعية لحث الضحايا على الكشف عن معلومات حساسة، شخصية ومالية ككلمات المرور، معلومات بطاقة الائتمان/الخصم على الانترنت. (Vallabhaneni, 2021, p. 579)

وتحتل المؤسسات المالية المرتبة الأولى في القطاعات التي تعرضت لهجمة التصيد سنة 2021 حسب

المنصة الإحصائية Statista

الشكل رقم (5): الصناعات الأكثر استهدافا من قبل هجمة التصيد الاحتيالي عبر الانترنت في الربع الأول Q1 من 2021



المصدر: من إعداد الباحثة اعتمادا على بيانات موقع STATISTA

<https://www.statista.com/statistics/266161/websites-most-affected-by-physhing/>

وثبت مؤخرا الاحتيال والسرقة باستخدام **SWIFT** (نظام رسائل الدفع الالكترونية الرئيسي للنظام المالي العالمي) فيتم الوصول إلى المعلومات السرية بما في ذلك بيانات اعتماد العملاء وعليه استخدام الدفع عبر الانترنت، وتمثل خسائر الاحتيال الالكتروني 90% من الخسائر المبلغ عنها. وأشهر حادثة باستخدام نظام **SWIFT** ما حدث في فبراير 2016 حين استهدف القراصنة بنك بنغلادش المركزي واستغلوا مواطن ضعف في نظام **SWIFT** في محاولة لسرقة مليار دولار، ورغم حظر معظم المعاملات اختفى مبلغ قدره 101 مليون دولار. (Antoine Bouveret, 2018, p. 11)

• سرقة الهوية Identity Theft

تتمثل في نقل هوية شخص آخر أو استخدامها دون سلطة قانونية بقصد ارتكاب أو المساعدة أو التحريض على أي نشاط غير قانوني، والبيانات الشخصية التي تتعرض لسرقة الهوية تتمثل في العناوين، أرقام الضمان الاجتماعي، أرقام البنك أو بطاقات الائتمان، وبالتسلح بهذه البيانات يحاول اللصوص الحصول على أموال من حساب مصرفي، أو فرض رسوم على حسابات بطاقة ائتمان قائمة أو فتح حسابات جديدة، أو تقديم مطالبات تأمين كاذبة، أو إتلاف التصنيف الائتماني لشخص آخر عن طريق تقديم طلب زائف للحماية من الإتلاف. (Dana C.McWay, 2021, p. 209)

آثار هذه الهجمة كبيرة جدا فقد كشف معهد معلومات التأمين في سنة 2016 أن 16 مليار دولار تمت سرقتها من 15.4 مليون عميل عن طريق سرقة الهوية. (Jo Ann Barefoot, 2020, p. 04)*

• هجمة رفض الخدمة Denial of Service DoS

هدفها منع إتاحة خدمات وموارد المؤسسة لمدة معينة، عن طريق إصابة آلات وخوادم ومداخل المؤسسة لمنع وصول العملاء إليها، هدفها ليس تخريب أو سرقة المعلومات بل فقط إتلاف وإضرار سمعة المؤسسة بإعاقة السير الحسن لأنشطتها عبر الانترنت. (Jo Ann Barefoot, 2020, p. 04)

وتعتبر مؤسسات القطاع المالي أكثر المؤسسات تعرضا لرفض الخدمة وأكثرها تضررا خصوصا مع اعتماد هذه المؤسسات للتكنولوجيات المالية واعتمادها في تقديم خدماتها المالية على الانترنت والهواتف المحمولة.

ومن أشهر الحوادث في رفض الخدمة ما حدث في جمهورية التشيك في مارس 2013، حيث تعطلت المواقع الإلكترونية للبنك المركزي وثلاثة بنوك كبيرة وتعطلت البورصة مع أضرار قدرت بنحو 0.5 مليون دولار، وفي جويلية 2014 تعرضت 7 مؤسسات مالية كبرى في النرويج للهجوم، ما أدى إلى تعطل الخدمات خلال اليوم، وفي نهاية 2014 عانت 3 بنوك في فنلندا من هجمة رفض الخدمة جعلت خدماتها عبر الانترنت غير متاحة، ومنعت عملاء أحد البنوك من السحب النقدي وسداد المدفوعات بالبطاقات. (Jo Ann Barefoot, 2020, p. 11)

3 تحليل أثر مخاطر الأمن السيبراني على الشمول المالي والاستقرار المالي

1.3 مخاطر الأمن السيبراني في الخدمات المالية عبر الحدود :

تثير الابتكارات الرقمية لخدمات الدفع عبر الحدود باستخدام FinTechs مخاطر جديدة، لا سيما فيما يتعلق بالأمن السيبراني. إن الطبيعة المتغيرة للهجمات الإلكترونية ونمو المخاطر السيبرانية مدفوعة بعوامل تشمل التقنيات المتقدمة، وزيادة الترابط بين المؤسسات المالية والأطراف الخارجية، والحوافز الأكثر أهمية لمجرمي الانترنت لاستهداف الهيئات المالية (Huang, K., & Madnick, (2020)) S., سبيل المثال، أدى الهجوم الإلكتروني على بنك (Chile de Banco) في عام

2018 إلى تدمير 9000 محطة عمل و500 خادم، بالإضافة إلى تعرض نقاط النهاية للتعامل مع المعاملات على شبكة **SWIFT** للخطر، كما يتم استخدام الخوارزميات التي تعمل خلف الشاشة لأتمتة الموافقات أو الاستشارات الائتمانية، وتسهيل الامتثال التنظيمي واكتشاف الاحتيال وأتمتة تداول الأصول المالية، وتلعب أدوار أساسية لخدمات الدفع عبر الحدود. ومع ذلك، فإن سلامة الخوارزميات، والضعف المتأصل في 12 الخوارزميات المعتمدة، والمسائل الأخلاقية للحكم الذاتي، وما إلى ذلك، تزيد من المخاطر النظامية داخل الاعتماد الواسع النطاق للتداول الخوارزمي هذه الأيام، يمكن أن تؤدي هذه نظام الدفع عبر الحدود. نظر التقلبات إلى مزيد من الانهيارات السريعة (Pupentsova, S., & Livintsova, M, 2022)

و يعتبر النظام المالي بنية تحتية مهمة ويتم تعريف أمنه السيبراني على أنه جزء من الأمن السيبراني الوطني. الاستثناء الأمني هو مبدأ مهم في بيئة التجارة الدولية، والذي يسمح للحكومات باتخاذ الإجراءات عند الضرورة في حالات المصلحة الأمنية الأساسية. ومع ذلك، يعتبر هذا الاستثناء الأمني محددا ذاتيا أو ما يسمى الحكم الذاتي أو التفسير الذاتي ومن المتوقع أن يظل غير واضح في المستقبل القريب. حيث يثير العديد من النزاعات في مجال الأمن السيبراني بين الدول (Tzoneva, A., Momcheva, Stoyanov, B. & G., 2022) وللتغلب على خسائر الأمن السيبراني لابد من وجود مبادئ أساسية مهمة لإنشاء مخطط لتصنيف تأثير الخسائر السيبرانية في إنشاء فئات تجمع تأثيرات الخسارة المتشابهة نسبيا في طبيعتها وتحتوي على دوافع مماثلة من أجل تسهيل الخطوات القابلة للتنفيذ من منظور إدارة المخاطر، خاصة فيما يلي: (Curti, F., Gerlach, J., Kazinnik, S., Lee, Mihov, A. & M. J., 2019)

- تحديد تأثير الخسائر السيبرانية بشكل فريد للانتماء إلى فئة تصنيف معينة .
 - أن يكون لفئة تصنيف الخسائر السيبرانية تأثيرات ذات دوافع أساسية مماثلة .
- يستخلص الباحثان أنه قد يكون لمخاطر الأمن السيبراني تأثيرات و خسائر متعددة، وقد يرتبط هجوم إلكتروني واحد بتعطيل عدة خدمات في الشركة التي تعرضت للهجوم، وخرق البيانات، وسرقة أموال

العملاء. لأن الخطر السيبراني يشمل على جميع الحوادث المرتبطة بالحوادث الإلكترونية باستثناء تكاليف الفرصة والإيرادات الضائعة والتكاليف المتعلقة بإدارة المخاطر وتحسينات الرقابة المنفذة لمنع الخسائر السيبرانية المستقبلية .

3-2/ أثر استخدام التكنولوجيا المالية على الاستقرار والشمول المالي في قطاع البنوك :

تلعب التكنولوجيا المالية دورا متزايدا لتعزيز نظام الدفع عبر الحدود بينما تظهر مخاطر التهديد السيبراني. ومع ذلك، ينبغي أن يقترن الاستخدام المتزايد لهذه التقنيات بتعزيز الرقابة التنظيمية على الأنشطة المالية لحماية الاستقرار المالي، حيث قد تظهر مخاطر جديدة تزيد اتجاهات الرقمنة المالية من الحاجة إلى الأمن السيبراني لحماية المستهلكين والمنتجين الماليين. ومن ثم، إلى جانب تنفيذ اللوائح ذات الصلة لحماية الأنظمة المالية والتخفيف من مخاطر الأمن السيبراني المحتملة، حيث فرضت العديد من الدول قيودا على حواجز التجارة الإلكترونية، بهدف تصنيفها في الفئات التالية، التوطين، و يتكون أول تقييد للتجارة من متطلبات التوطين، بما في ذلك البيانات أو توطين النظام ذي الصلة. على سبيل المثال، تتطلب الهند أن يتم وضع جميع بيانات الدفع التي تحتفظ بها شركات الدفع في منشآت محلية داخل الدولة ولا يسمح بتصديرها خارج البلاد، ولا حتى للمعالجة. إلى جانب متطلبات البيانات (Huang, Madnick, S. & K., 2020)) و على الرغم من أن FinTech تخلق فوائد الاستقرار المالي، إلا أنه من المحتمل أن يكون لها تأثير نظامي سلبي على الأخير ويمكن أن تنتج آثار سلبية خطيرة يمكن أن تعرض الاقتصاد الحقيقي للخطر، وتعتبر التكنولوجيا المالية إحدى التقنيات الهامة التي يمكن أن تقود الاستقرار المالي من خلال قنوات التمويل الأصغر والقنوات المالية الكلية. لذلك يمكن أن تخلق التكنولوجيا المالية مخاطر مالية صغيرة وكبيرة على الاستقرار المالي. بينما يعمل رأس المال والسيولة من جانب على تعزيز المرونة المالية، من ناحية أخرى، وتدعم الحوكمة والضوابط القوية المرونة التشغيلية. و تنبع مصادر المخاطر التشغيلية من الحوكمة ومراقبة العمليات، و المخاطر الإلكترونية، والاعتماد على الأطراف الثالثة، والمخاطر القانونية ومخاطر الأعمال المتعلقة بالبنية التحتية الحيوية

للأسواق المالية (Vučinić, M., 2020)

و يشير الشمول المالي إلى عدد المستفيدين الذين يمكنهم الوصول إلى الخدمات المصرفية أو المالية، حيث أن الخطوة الأولى نحو الشمول المالي هي امتلاك حساب على نحو متزايد، يتم استخدام المدفوعات الرقمية في المعاملات المالية. كما يعد إجراء المدفوعات الرقمية أو تلقيها أحد الاستخدامات المهمة لحساب الادخار. مع ذلك، أفاد عدد قليل من الأشخاص باستخدام حساباتهم للادخار و لكن ليس أيضا لإجراء مدفوعات رقمية أو تلقيها في العام الماضي، كما ساعدت التكنولوجيا في تحقيق التكافؤ بين الجنسين وقلصت الفجوة بين البالغين الأكثر ثراء و الفقراء (Saon Raya, S. P., & Miglanic, S., 2019).

وان أحد المنتجات التي تم إنشاؤها من نموذج **Fintech** هو منصة الإقراض من شخص إلى شخص (P2P) على الرغم من أن إقراض **P2P** يقدم خدمات أفضل بتكاليف منخفضة، إلا أنه زاد أيضا من مخاطر الائتمان . وبالتالي ظهور المخاطر النظامية، ومما لا شك فيه أن الوسائط الرقمية قد زادت من مستوى الشمول المالي عالميا من 51 بالمائة عام 2011 إلى 69 بالمائة في 2017 والتحدي الذي يواجه البنوك هو تحديد أنسب نموذج للاتصال للتفاعل مع شرائح مختلفة من العملاء من أجل إقناعهم بتبني قنوات مصرفية رقمية ونظرا للاضطرابات غير النقدية، لا تستطيع المؤسسات المالية التحكم في تجربة العملاء في المعاملات بسبب التكامل وتفقّد المؤسسات المالية الرؤية وسيتعين عليها أن تهدف إلى تأمين مكان البطاقة الافتراضية في السوق (Shanmugam, S. & Yadav, M., 2022).

ويستنتج الباحثان أن التطورات السريعة في التكنولوجيا المالية على الأسواق المالية ونماذج الأعمال للمؤسسات المالية التقليدية من أجل متابعة الاتجاهات الحالية والمنافسة في منافستها سريعة النمو، للوصول إلى الشمول المالي. حيث تتبنى المؤسسات المالية التقليدية التغييرات من أجل تلبية احتياجات السوق. و يمكن أن تكون عوامل جانب العرض والطلب بمثابة محركات الابتكارات المالية، و تبحث للأجيال الجديدة بشكل خاص عن خدمة مالية سريعة وسهلة الوصول يمكن الوصول إليها في أي وقت وفي أي مكان. و فيما يتعلق بذلك، من المرجح أن يستخدموا المدفوعات الإلكترونية أو

الخدمات المصرفية عبر الهاتف المحمول أو ائتمانات **FinTech** أو غيرها من المنتجات بدلا من استخدام أساليب الخدمات المالية التقليدية. و الشاغل الرئيسي هو التأثير الرقمي على استقرار وسلامة الأسواق والأنظمة المالية الأوسع.

2-3/ أثر مخاطر الأمن السيبراني على الاستقرار والشمول المالي للبنوك :

تبنت البنوك بشكل متزايد دورها في تعزيز الشمول المالي إلى جانب أهدافها التقليدية المتمثلة في الحفاظ على استقرار الأسعار والاستقرار المالي. ولتحقيق هذه الغاية، لا تستخدم بعض البنوك المركزية القواعد واللوائح فحسب، بل تستخدم أيضا الابتكار من خلال التدخل المباشر في نظام المدفوعات الفورية المدعوم من البنك المركزي. والذي يمكن أن يحدثه البنك المركزي على تحقيق الاندماج والمنافسة في صناعة المدفوعات. وأن دور البنك في المدفوعات يمكن أن يكون أداة فعالة لتعزيز الإدماج وتعزيز المنافسة، لا سيما عندما يبدو الفاعلون الخاصون غير راغبين أو غير قادرين على القيام بذلك بأنفسهم . ومع ذلك، فإن شرعية التدخلات المبتكرة للبنك المركزي في المدفوعات والذي يمكن للبنوك أن تمضي فيه في إجراءاتها المبتكرة دون المبالغة في تقدير أيدئها أو إزاحة المبادرة والبراعة الخاصة (Bolzani, J، 2022) و تغطي البنوك خمس وظائف واسعة. وهي من أجل اجراء المدفوعات واستلامها، بما في ذلك عبر الحدود (Miglanic, S., & Saon Raya, S. P., 2019)

• الادخار لتتمكن من الاستهلاك أو الاستثمار لاحقا .

• الاقتراض لتتمكن من الاستهلاك أو الاستثمار الآن

• إدارة المخاطر على الدخل والمدخرات والمعاملات

قد تحفز **Fintech** مكاسب الكفاءة في البنوك، وتقدم منتجات وخدمات أفضل وأكثر استهدافا وتعمق الشمول المالي. ومع ذلك، قد يشكل أيضا مخاطر إذا كان تطبيقه يقوض المنافسة والثقة ونقل السياسة النقدية والاستقرار المالي. على الرغم من الاعتراف بأن المخاطر السيبرانية تشكل تهديدا للاستقرار

المالي، إلا أن قياس وتحليل المخاطر الإلكترونية في البنوك لم ينضج إلى الحد الذي يمكن فيه قياسها وإدارتها باستمرار مقابل تقبل المخاطر المؤسسية والنظر إليها من منظور النظام من خلال المنظّمون والمشرفون. وهذا يعيق الجهود المبذولة لقياس وإدارة هذه المخاطر بشكل فعال، مما يقلل من استعداد المؤسسات الفردية والجماعية للتعامل مع التهديدات الإلكترونية على مستوى النظام ومعالجة تكنولوجيا المعلومات أو أبعاد هندسة النظام للمخاطر السيبرانية، بل التركيز على جوانب إدارة المخاطر المالية للمخاطر السيبرانية (Tzoneva, A., Momcheva, G., & Stoyanov, B.,

2022)

و يستنتج الباحثان أن المخاطر السيبرانية تمتد إلى جميع المجالات الرئيسية لعمليات البنوك، والاستقرار المالي، والنزاهة المالية، والشمول المالي، وأنظمة الدفع، وإدارة العملات النقدية. على الرغم من أن هذه المخاطر المتعلقة بالأمن السيبراني تؤثر في المقام الأول على المؤسسات الخاضعة للإشراف على التعرض للمخاطر التي يواجهها البنك نفسه. والمشاركين في الأسواق المالية، إلا أنها تؤثر أيضا على التعرض للمخاطر التي يواجهها البنك نفسه بالإضافة إلى ذلك، يمكن أن تتفاقم المخاطر التشغيلية المتعلقة بالنظام الداخلي، بما في ذلك تكنولوجيا المعلومات والأمن السيبراني والموارد البشرية وإدارة استمرارية الأعمال، من خلال زيادة استخدام أدوات التكنولوجيا المالية أيضا. لذلك، تحتاج إدارة المخاطر السيبرانية للبنك إلى تشكيل خط دفاع مناسب للمخاطر المتعلقة بالتكنولوجيا المالية

.و على الرغم من أن مخاطر الأمن السيبراني ليست جديدة على الإطلاق، فإن السرعة والميل الذي تحدث به تطورات في البنوك إلا أن إدارات تكنولوجيا المعلومات والمشرفين الماليين هم أول وحدات عمل داخل العديد من البنوك لتحديد مخاطر الأمن السيبراني. لذلك تحتاج البنوك إلى تعزيز إدارتها الداخلية للمخاطر لتشمل مساعدة شاملة على مستوى البنك في تحديد المخاطر المتعلقة بالتكنولوجيا ومخاطر الأمن السيبراني وتخفيفها والإبلاغ عنها ومراقبتها بالنسبة للبنك، حيث أن حوكمة المخاطر وثقافة المخاطر القوية أمران حاسمان. هذه تتطلب توعية قوية من البنك. وأن يكون المحافظين وأعضاء مجلس الإدارة على دراية بالمخاطر المتعلقة بالأمن السيبراني التي تديرها البنك، وكيف أن هناك حاجة

واضحة لوضع إطار عمل لإدارة المخاطر السيبرانية. وسيشمل ذلك الوصول إلى موظفي البنك المركزي وتدريبهم (لا يقتصر على المشرفين ومتخصصي تكنولوجيا المعلومات - على الرغم من أن برنامج التدريب على التكنولوجيا المالية وإدارة المخاطر وتدريب موحد ومتسق ومركز على التكنولوجيا الإلكترونية)، بالإضافة إلى تعزيز فهم أعضاء مجلس الإدارة أنفسهم لتطورات التكنولوجيا المالية على مستوى أكثر دقة، حيث أن إدارة المخاطر يجب أن تأخذ في الحسبان دمج العاملين السيبرانيين في فرق إدارة الأزمات.

المحور الثالث: استراتيجية تحقيق الأمن السيبراني في القطاع المالي

1.3/ حساسية القطاع المالي تجاه المخاطر السيبرانية

إن التطورات التكنولوجية التي عرفها القطاع المالي، والتي عززت من إمكانية الوصول للخدمات المالية الرقمية بسرعة وسهولة، لها جانب مظلم يعتبر تحدياً لمؤسسات هذا القطاع، إذ زادت هذه التطورات من إمكانية تعرض المؤسسات لمخاطر من نوع جديد وهي المخاطر السيبرانية التي قد تعرض الاستقرار المالي للخطر، إذ يعتبر قطاع الخدمات المالية وخصوصاً القطاع المصرفي الأكثر حساسية للهجمات السيبرانية بنسبة تفوق القطاعات الأخرى بنسبة 65% وفق تقديرات البنك الدولي. (دائرة الاستقرار المالي ، 2019) وتعود هذه الحساسية لمجموعة من الأسباب أهمها:

- اعتماد القطاع على البنى التحتية الحرجة: والتي تشمل أنظمة الدفع والتسوية ومنصات التداول المركزية، ودافع الأوراق المالية، وتمثل البنية التحتية الحرجة نقطة ضعف واحدة، وأي هجمة ناجحة يمكن أن يكون لها عواقب واسعة النطاق. (Antoine Bouveret, 2018)

p. 11)

- التحول المتزايد إلى البنية التحتية السحابية: والذي نتج عنه المزيد من عقد البيانات المركزة، بتنوع أقل في البرامج وتدابير أمنية أعلى. (Ross Buckley, Douglas Arner, Dirk Zetsche and Eriks Selga, 2019)

- ظهور التكنولوجيات الجديدة: حيث أدى ظهور التكنولوجيا المالية وتطوير النظم الرقمية في التمويل إلى زيادة نسبة التعرض للهجمات السيبرانية، إذ أن التكنولوجيا تؤدي إلى توسيع نطاق

وأعداد نقاط الدخول في المالية الذي يمكن أن يستهدفه المتسللون، كما تزيد أنشطة التكنولوجيا المالية أيضا من اعتماد الأطراف الثالثة، حيث تقوم الشركات بتعهيد الأنشطة إلى عدد قليل من مقدمي الخدمات، في هذه الحالة التعطيل يزيد من المخاطر بسبب مركزية المزود في المالية.

- **الاعتماد على شبكات شديدة الترابط:** الأمر الذي يزيد من نطاق وسرعة العدوى، فهجوم ناجح على شبكة يمكن أن ينتشر بسرعة إلى شبكات أخرى، فبالنسبة للمؤسسات المالية، تعطل أحد البنوك الكبيرة يمكن أن يؤثر على الأطراف المقابلة والبنى التحتية للأسواق المالية.

(Antoine Bouveret, 2018, p. 11)

- **اعتماد أغلب المؤسسات المالية على الأنظمة القديمة:** والتي قد لا تكون مقاومة للهجمات السيبرانية، ففي الوقت الحالي يتوافر عدد قليل من الحلول التقنية لهذه الهجمات القادرة على زعزعة الثقة على نطاق واسع. (Tim Maurer, Arthur Nelson, 2021)

- **الانفصال بين مجتمع التمويل ومجتمع الأمن القومي:** فرغم أن السلطات المالية تواجه مخاطر متفردة من التهديدات السيبرانية، فإن علاقاتها لا تزال هشّة مع هيئات الأمن القومي التي تعتبر مشاركتها ضرورية للتصدي لتلك التهديدات، وتتفاقم المخاطر بسبب فجوة المسؤولية هذه واستمرار حالة عدم اليقين بشأن الأدوار المطلوبة لحماية النظام المالي العالمي. هذه الأسباب التي تجعل من القطاع المالي حساسا للمخاطر السيبرانية هي الدافع القوي لتكثيف الجهود في مجال تطوير أساليب الحماية والأمن السيبراني.

2.3/ الأمن السيبراني على مستوى المؤسسات:

الحماية البرمجية تتمثل في استخدام كل البرامج المتاحة و التي توفر حماية للمعلومات المنتقلة عبر الشبكات أو المخزنة في الحواسيب، ومن أهم طرق الحماية السيبرانية ما يلي:

- **برامج مكافحة الفيروسات:** لحماية الأنظمة من البرمجيات الخبيثة كالفيروسات والديدان وأحصنة طروادة....، وإجراء عملية المسح التلقائي.

- **الجدران النارية:** يقوم الجدار الناري بغريلة التوصلات الداخلة و الخارجة ومراقبة العمليات التي تمر بالشبكة.

- **التشفير:** هو الاعتماد على خوارزمية من أجل تحويل المعطيات الواضحة إلى معطيات مشفرة من أجل جعلها غير واضحة لشخص دخيل"، و الهدف من التشفير هو جعل كل الملفات الرقمية الموجودة على التحاميل غير صالحة الاستعمال لمن لا يملك مفتاح الرمز (Cuenot, Arnaud Pelletier et Patrick, 2003)

ويعتبر نظام التشفير الآلية الأساسية التي تتبعها جهات التوثيق الإلكتروني لضمان سلامة البيانات الإلكترونية المتبادلة بين البنك وعملائه، وتعتبرها الشركات المالية والمصرفية الوسيلة الأكثر فعالية لتأمين الرسائل والبيانات، والتشفير يكون بطريقتين: التشفير المتماثل الذي يتم استعمال فيه مفتاح عام واحد، التشفير غير المتماثل باستخدام مفتاحين عام وخاص، واختيار نوع من أنواع التشفير يكون حسب حساسية المعلومات وحجم الملفات المراد تشفيرها، وتعتمد قوة التشفير على عاملين: الخوارزمية، وطول المفتاح مقدرا ب **Bit**، وكلما زاد **Bit** زادت نسبة الأمان وصعوبة فك الشيفرة.

- **التوقيع الإلكتروني:** باعتبار أن التعرف على شخصية العميل والتأكد من هويته له بالغ الأهمية في مجال الأعمال المصرفية، فإن التوقيع الإلكتروني يعد من أبرز الوسائل المستخدمة من قبل البنوك لذلك.

- **مراقبة الدخول:** يتطلب الدخول للأنظمة التعريف بالهوية عن طريق معرفة عنوان **IP**، والتحقق من الهوية والذي يكون بعدة طرق ككلمة المرور، الإيماء، أو التحقق البيومتري اعتمادا على ملامح الوجه، أو قذحية العين...

- **أنظمة كشف التدخل:** عبارة عن أدوات مراقبة مستمرة موضوعة في نقاط الدخول الأكثر حساسية لشبكات المؤسسة لكشف التدخلات، و من ثم يطلق النظام إنذار في وقت حقيقي في حال

حدث مريب أو غير عادي. , (Kenneth Laudon et Jane Laudon, 2006)

- التحديثات واختبار الثغرات بشكل دوري: تقوم استراتيجية حماية البيانات في البيئة المصرفية على تحصين النظام داخليا عن طريق اختبارات فعالة للثغرات الأمنية في النظام والقيام بسدها، والتأكد من تحديث الأنظمة المستخدمة.
- توفير الكفاءات البشرية في مجال التقنية والأمن السيبراني ورفع الثقافة الأمنية الداخلية.

4.3.3. خاتمة:

- رغم المزايا التي تقدمها التكنولوجيا المالية في تقديم الخدمات المالية، إلا أن المخاطر التي تنتج عنها قد تغير الصورة تماما، وتلعب بذلك التكنولوجيا دورا معاكسا، فبدل أن تساهم في تحقيق الشمول المالي تصبح هي المعرقل له، ولمعرفة حيثيات الموضوع قمنا من خلال هذا البحث بدراسة الاشكالية وتوصلنا إلى النتائج التالية:
- تساهم رقمنة القطاع المالي واعتماده على التكنولوجيا المالية في زيادة نسب الشمول المالي خصوصا في المناطق النائية المحرومة.
- إعداد خطط ووضع السياسات لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الاستقرار والشمول المالي.
- الاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبراني.
- توفير بيئة مناسبة للأمن السيبراني يهدف لدعم الشمول المالي.
- تزداد نسبة الهجمات السيبرانية على القطاع المالي كلما زاد اعتماده على التكنولوجيا المالية.
- تتطور الهجمات السيبرانية بتطور التكنولوجيا المالية، فبازدياد الاعتماد على الهاتف النقال في التعاملات المالية ظهرت برمجيات خبيثة خاصة بالمحمول، كحصان طروادة المصرفي و الروبوت المصرفي.

- تعتبر التهديدات التي تمس سرية المعلومات وتُعرضها للكشف (كالاختراق) الأخطر من بين التهديدات السيبرانية لتأثيرها الكبير على سمعة المؤسسة المالية وفقد الثقة فيها باعتبار أن الأساس في التعاملات المالية هو السرية والثقة.
- يعتبر القطاع المالي الأكثر حساسية من بين القطاعات للهجمات السيبرانية بسبب طبيعة البنية التحتية الحساسة، والترابط الشديد للشبكات بحيث إصابة شبكة واحدة ينتقل ويؤثر على البقية، لذا فإن التكلفة المالية للهجمات تكون عالية جدا.

5. قائمة المراجع:

- .Pupentsova, S., & Livintsova, M. (2022) The Enterprises Risk Management in the Context of Digital Transformation. . In *International Scientific Siberian Transport Forum*.1167-1159 ،
- A.Hassan, N. (2019,). , Ransomware revealed- A beginner's guide to protecting and recovering from ransomware attacks-,. (Apress, Éd.) pp. , p9.
- Antoine Bouveret. (2018). *Cyber risk for the financial sector : A framework for quantitative assessment-IMF working paper-*,. International Monetary Fund.
- Bolzani, J. (2022) Leading the Way in Payments: How Central Banks Are Using Innovation to Promote Financial Inclusion and Reshape Competition. Forthcoming, . *Journal of Law and Commerce of the University of Pittsburgh School of Law*,.41 ،
- Christine Lagarde.) June, (2018). Estimating cyber risk for the financial sector, . *IMF Blog*,.
- Cuenot, Arnaud Pelletier et Patrick. » (2003) *Intelligence Economique ,mode d'emploi –Maitrisez l'information stratégique de votre entreprise »*. France,: édition Pearson.
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. () August, , (2019). Cyber risk definition and classification for financial risk management. *Federal Reserve Bank of St Louis*.
- Dana C.McWay. (2021). Legal and Ethical Aspects of health information management. (f. edition, Éd.) 209.
- dfgf.) fgf). gdf. fdg: df.
- European Payments Council. 2021. (2021) *payment threats and fraud trends report*, . version 1.0, 2023, 03 18 تاريخ الاسترداد
- Hal Lonas. . (2020) Webroot threat report, webroot Inc..20 صفحة

- Huang, K., & Madnick, S. . .(2020)) *Cyber securing cross-border financial services:* .
- Jo Ann Barefoot. (2020, june). Digital Technology risks for finance : dangers embedded in fintech and regtech. (M.-R. A. series, Éd.) (No151), 04.
- Kenneth Laudon et Jane Laudon,. (2006) *Management des systèmes d'information*9 (المجلدات) éme édition,,). France: édition Pearson.
- Mamoun Alazab, Andrii Shalaginov Mark Stamp. ، (2021) *Malware Analysis Using Artificial Intelligence and Deep Learning*, ..166 صفحة
- Ponemon Institute, *The cost of cybercrime, ninth annual cost of cybercrime study*, Accenture. (2018).
- Ross Buckley, Douglas Arner, Dirk Zetsche and Eriks Selga. .(2019) The dark side of digital financial transformation: the new risks of fintech and the rise of techrisk,. *UNSW*.
- Saon Raya, S. P., & Miglanic, S.,. (2019) Use of Blockchain and Aritificial Intelligence to promote financial inclusion in India. *TECH MONITOR* • Jan-Mar.
- Silvia Baur-yazbeck, J. F. (2019, november). Cyber security in financial sector development-challenges and potential solutions for financial inclusion-,. p. 7.
- Tim Maurer, Arthur Nelson.) March, 2021). The global cyber threat,.) IFM (المحرر ، *finance & development revue*,.
- Tzoneva, A., Momcheva, G., & Stoyanov, B.) May, 2022). Vendor Cybersecurity Risk Assessment in an Autonomous Mobility Ecosystem. *n 2022 10th International Scientific Conference on Computer Science (COMSCI)*.
- Tzoneva, A., Momcheva, G., & Stoyanov, B.) may, 2022). Vendor Cybersecurity Risk Assessment in an Autonomous Mobility Ecosystem. . تأليف In 2022 10th International Scientific Conference on Computer Science (COMSCI) (المحرر).
- Vallabhaneni, S. (2021). business knowledge for Internet Auditing,. *Wiley CIA exam review focus notes 2021 part 3*, 579.
- Vučinić, M. .(2020) Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and*.66-43 ،(2)9 ،
- Yadav, M., & Shanmugam, S. .(2022) Fintech Lending in India: the Changing Paradigm of Banking.) UGC Care list no. 135، (المحرر) ،*Journal of the Oriental Institute*, ISSN: 0030-5324,.232-225 ،(5)71 ،
- تقرير الاستقرار المالي . (2019). دائرة الاستقرار المالي . البنك المركزي الأردني،.
- مأمون العزب. (أكتوبر ، 2018). أمن المعلومات في فضاءات انترنت الأشياء. (مؤسسة الكويت للتقدم العلمي، المحرر) مجلة التقدم العلمي، 99، 14.