Comprehensive Journal of Science
Volume (10), Issue (39), (March, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) العدد 39 مارس 2026
ردمد: 3014-6266

تقييم أمن وكفاءة تطبيقات المصارف الليبية الإلكترونية وأثرها على جودة الخدمات المصرفية

الصادق عبد القادر الحمزاوي

كلية تقنية الحاسوب طرابلس – ليبيا

alhmzawey@gmail.com

Evaluating the Security and Efficiency of Libyan Banking Mobile Applications and Their Impact on the Quality of Banking Services

Sadeq Abdulkader Alhmzawey
Faculty of Computer Technology – Tripoli, Libya

تاريخ الاستلام: 2026/01/01 –تاريخ المراجعة: 2026/01/20 – تاريخ القبول: 2026/01/30 – تاريخ للنشر: 2026/02/23

الملخص

شهد القطاع المصرفي الليبي خلال السنوات الأخيرة تحولًا رقميًا ملحوظًا تمثل في إطلاق تطبيقات مصرفية إلكترونية تهدف إلى تسهيل تقديم الخدمات المالية وتحسين تجربة العملاء. إلا أن هذا التحول الرقمي يرافقه عدد من التحديات التقنية والأمنية التي قد تؤثر على جودة الخدمات المصرفية وثقة المستخدمين.

هدفت هذه الدراسة إلى تقييم مستوى الأمن السيبراني وكفاءة التطبيقات المصرفية الليبية، وتحليل أثرها على رضا العملاء وجودة الخدمات الرقمية. اعتمدت الدراسة على المنهج الوصفي التحليلي، وشملت عينة مكونة من 351 مشاركًا، تم اعتماد 313 استبانة صالحة للتحليل الإحصائي.

أظهرت النتائج وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين الرضا العام وكل من التجربة الرقمية وسهولة الاستخدام وسهولة التفعيل، بينما لم يظهر تأثير معنوي للرسوم المصرفية. كما كشفت الاختبارات التقنية عن غياب آليات فحص بيئة التشغيل في بعض التطبيقات، مثل عدم التحقق من تفعيل وضع المطور (Developer Mode) ، مما قد يمثل نقطة ضعف أمنية.

الكلمات المفتاحية: الأمن السيبراني، التطبيقات المصرفية، جودة الخدمة، الثقة الرقمية، المصارف الليبية.

Abstract

This study aimed to evaluate the cybersecurity level and functional efficiency of Libyan banking mobile applications and their impact on service quality and customer satisfaction. The study adopted a descriptive analytical approach and analyzed 313 valid survey responses.

The findings revealed statistically significant positive correlations between overall satisfaction and digital experience, ease of use, and ease of activation. However, service fees did not show a significant impact. Technical testing also revealed the absence of runtime environment checks in some applications, including Developer Mode detection, which may represent a potential security weakness.

Keywords: Cybersecurity, Mobile Banking Applications, Service Quality, Digital Trust, Libyan Banks.

1- المقدمة

أدى التطور السريع في تقنيات الاتصالات والهواتف الذكية إلى تحول جذري في أساليب تقديم الخدمات المصرفية عالميًا، حيث أصبحت التطبيقات المصرفية الإلكترونية إحدى أهم القنوات المعتمدة لتسهيل العمليات المالية وتحسين تجربة المستخدم.

وفي ليبيا، اتجهت المصارف خلال السنوات الأخيرة إلى إطلاق تطبيقات إلكترونية بهدف تقليل الاعتماد على المعاملات الورقية داخل الفروع، وتخفيف الضغط على البنية التحتية المصرفية. إلا أن هذا التحول الرقمي يواجه تحديات تتعلق بالأمن السيبراني، وكفاءة الأداء، وسهولة الاستخدام، ووضوح الرسوم.

ومن هنا تنبع أهمية تقييم واقع هذه التطبيقات، وقياس مدى انعكاسها على جودة الخدمات المصرفية وثقة العملاء.

2- مشكلة البحث

على الرغم من انتشار التطبيقات المصرفية في ليبيا، إلا أن هناك ملاحظات تتعلق بـ:

- تفاوت مستويات الأمان بين التطبيقات.
- تعقيد إجراءات التفعيل الأولي.
- ضعف في قنوات الدعم الفني.
- عدم وضوح الرسوم والخصومات.
- محدودية بعض الخدمات الرقمية.

وعليه يتمثل السؤال الرئيس للبحث في:

ما مدى كفاءة وأمن تطبيقات المصارف الليبية الإلكترونية، وما أثر ذلك على جودة الخدمات المصرفية المقدمة للزبائن؟

3- أهداف البحث

1. تقييم مستوى الأمن السيبراني في التطبيقات المصرفية الليبية.
2. تحليل كفاءة الخدمات المصرفية المقدمة عبر التطبيقات.
3. دراسة تجربة المستخدم ومرحلة التفعيل.
4. تقييم خدمات الدفع عبر الهاتف المحمول.
5. تقديم توصيات عملية لتعزيز الأمن وتحسين الجودة.

4- أهمية البحث

- دعم المصارف الليبية في تطوير تطبيقاتها الرقمية.
- تعزيز الوعي بالأمن السيبراني في القطاع المصرفي.
- توفير دراسة تطبيقية حديثة تدعم المكتبة الأكاديمية الليبية.

- مساعدة متخذي القرار في تحسين الخدمات الرقمية.

5- الإطار النظري

يشهد القطاع المصرفي العالمي تحولًا رقميًا متسارعًا مدفوعًا بتطور تقنيات الاتصالات وانتشار الهواتف الذكية، مما أدى إلى بروز الخدمات المصرفية عبر الهاتف المحمول (Mobile Banking) كقناة رئيسية لتقديم الخدمات المالية. ويُعرّف الأمن السيبراني بأنه مجموعة السياسات والإجراءات والتقنيات المصممة لحماية الأنظمة والشبكات والبيانات من الهجمات الرقمية والاختراقات (بن حامد، 2022).

في السياق المصرفي، يمثل الأمن السيبراني عنصرًا حاسمًا في ضمان سرية المعلومات المصرفية وسلامة المعاملات المالية. وتشير معايير (2023) OWASP Mobile Top 10 إلى أن تطبيقات الهاتف المحمول قد تكون عرضة لمخاطر متعددة، مثل ضعف المصادقة، سوء إدارة الجلسات، وعدم التحقق من بيئة التشغيل. ويُعدّ فحص حالات مثل Rootأو Developer Mode من الممارسات الأمنية المهمة التي تمنع تشغيل التطبيق في بيئات غير آمنة قد تسمح بالهندسة العكسية أو تحليل حركة البيانات.

ومن منظور جودة الخدمة، يُعد مفهوم جودة الخدمة الإلكترونية (E-Service Quality) امتدادًا لنموذج SERVQUALالتقليدي، حيث يتم تقييم الخدمة بناءً على أبعاد مثل الاعتمادية، سهولة الاستخدام، الاستجابة، والأمان. وتشير الأدبيات إلى أن رضا العملاء في البيئة الرقمية يتأثر بشكل مباشر بتجربة المستخدم الرقمية (Digital Experience)، والتي تشمل سهولة التفاعل، سرعة الأداء، وضوح الإجراءات، ومستوى الأمان المدرك.

كما تؤكد دراسات Mobile Banking Adoption أن الثقة الرقمية (Digital Trust) تمثل عاملًا وسيطًا بين الأمان التقني ورضا العملاء .(Sahi et al., 2021) فكلما ارتفع مستوى الأمان المدرك وتحسنت تجربة الاستخدام، زادت ثقة العملاء في التطبيق، مما ينعكس إيجابًا على رضاهم واستمرار استخدامهم للخدمة.

وبناءً على ذلك، يمكن صياغة العلاقة النظرية بين متغيرات الدراسة على النحو التالي:

الأمان التقني + سهولة الاستخدام + جودة التجربة الرقمية

⬇

تعزيز الثقة الرقمية

⬇

زيادة رضا العملاء وجودة الخدمة المصرفية الإلكترونية

وعليه، فإن تقييم التطبيقات المصرفية لا يقتصر على فحص خصائصها الوظيفية، بل يمتد ليشمل تحليل بنيتها الأمنية ومدى توافقها مع المعايير الدولية، ومدى انعكاس ذلك على تجربة المستخدم ورضاه العام.

6- الدراسات السابقة

تناولت العديد من الدراسات موضوع الأمن السيبراني والخدمات المصرفية الرقمية من زوايا مختلفة، سواء من حيث حماية البيانات أو جودة الخدمة أو أثر التحول الرقمي على أداء المؤسسات المالية.

فقد هدفت دراسة **بن حامد (2022)** إلى تحليل دور الأمن السيبراني في حماية الأنظمة والبيانات في المؤسسات الحديثة، واعتمدت على المنهج الوصفي التحليلي، حيث توصلت إلى أن غياب السياسات الأمنية الواضحة يؤدي إلى زيادة احتمالية الاختراقات وتسرب البيانات، وأكدت على ضرورة تبني معايير دولية لحماية الأنظمة الرقمية. وتستفيد الدراسة الحالية من هذه النتائج في تعزيز البعد الأمني عند تقييم التطبيقات المصرفية الليبية.

كما تناولت دراسة **عزام (2019)** أثر الأنظمة الرقمية في تحسين حماية البيانات المصرفية في البنوك التجارية بعمان، واعتمدت على تحليل استبيانات موجهة للعاملين في القطاع المصرفي، وأظهرت النتائج وجود علاقة إيجابية بين مستوى التطور التقني وحماية البيانات المصرفية. إلا أن الدراسة ركزت على البيئة المؤسسية الداخلية ولم تتناول تقييم التطبيقات من منظور المستخدم النهائي، وهو ما تسعى الدراسة الحالية إلى معالجته.

أما دراسة **ناشف (2018)** فقد بحثت في وسائل الدفع الإلكتروني في المؤسسات المالية الجزائرية، وأشارت إلى أن تطوير البنية التحتية الرقمية يسهم في رفع كفاءة العمليات المالية، لكنها حذرت من أن ضعف الثقافة الأمنية يمثل تحديًا أمام التوسع في الخدمات الإلكترونية. وتبرز أهمية هذه الدراسة في تسليط الضوء على العلاقة بين التطور التقني ومستوى الأمان.

وعلى المستوى المحلي، هدفت دراسة **غلاء وآخرون (2022)** إلى تحليل أثر نظم الدفع الإلكتروني في تحسين أداء المصارف التجارية الليبية، حيث أظهرت النتائج أن التحول نحو الدفع الإلكتروني يسهم في تقليل التكاليف التشغيلية وتحسين مستوى الخدمة. إلا أن الدراسة لم تتناول الجوانب الأمنية التقنية للتطبيقات المصرفية بصورة مباشرة، مما يترك مجالًا لدراسات تركز على التقييم الأمني الفني.

أظهرت دراسة **Alalwan et al. (2017)** أن تبني العملاء للخدمات المصرفية عبر الهاتف المحمول يتأثر بعوامل متعددة، أبرزها الثقة المدركة وسهولة الاستخدام وجودة النظام. وأكدت الدراسة أن الأمان يعد من أهم المحددات في قرار الاستخدام.

كما بينت دراسة **Sahi et al. (2021)** أن الثقة الرقمية تمثل متغيرًا وسيطًا بين جودة الخدمة الإلكترونية ورضا العملاء، وأن أي خلل أمني محسوس يؤدي إلى تراجع الثقة وبالتالي انخفاض مستوى الرضا.

من خلال استعراض الدراسات السابقة يتضح أن معظمها ركز على العلاقة بين التحول الرقمي وجودة الخدمة أو حماية البيانات، إلا أنها لم تتناول اختبارًا أمنيًا تطبيقيًا مباشرًا للتطبيقات المصرفية الليبية، خاصة فيما يتعلق بفحص بيئة التشغيل والكشف عن تفعيل وضع المطور (Developer Mode) ، وهو ما تمثل فجوة بحثية تسعى الدراسة الحالية إلى معالجتها.

7- الفجوة البحثية

لم تتناول الدراسات السابقة اختبارًا أمنيًا مباشرًا لتطبيقات المصارف الليبية فيما يتعلق بفحص تفعيل وضع المطور، وهو ما تسعى هذه الدراسة إلى معالجته.

8- الفرضيات

- توجد علاقة ذات دلالة إحصائية بين جودة التجربة الرقمية والرضا العام.
- توجد علاقة ذات دلالة إحصائية بين سهولة الاستخدام والرضا العام.
- توجد علاقة ذات دلالة إحصائية بين سهولة التفعيل والرضا العام.
- لا توجد علاقة ذات دلالة إحصائية بين الرسوم والرضا العام.

9- منهجية البحث

9.1 منهج الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، لملاءمته لطبيعة البحث الذي يهدف إلى تقييم مستوى الأمن السيبراني وكفاءة التطبيقات المصرفية الليبية، وتحليل أثرها على جودة الخدمات المصرفية ورضا العملاء.

9.2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من مستخدمي التطبيقات المصرفية الليبية عبر الهواتف الذكية. وتم توزيع الاستبيان إلكترونيًا عبر منصات التواصل الاجتماعي، حيث بلغ عدد المشاركين (351) مشاركًا، تم اعتماد (313) استبانة صالحة للتحليل الإحصائي بعد استبعاد الردود غير المكتملة.

9.3 أداة الدراسة

تم تصميم استبيان إلكتروني لقياس متغيرات الدراسة، وتضمن عدة محاور رئيسية:

- مستوى الرضا العام
- سهولة تفعيل التطبيق
- سهولة الاستخدام
- تقييم الرسوم والخصومات
- تقييم التجربة العامة
- مدى توفر الدعم الفني
- الشعور بالأمان

واعتمد الاستبيان على مقياس ليكرت الخماسي (Likert Scale) وفق التدرج التالي:

1 = ضعيف جدًا
2 = ضعيف
3 = متوسط
4 = جيد
5 = ممتاز

9.4 صدق وثبات الأداة

تم عرض الاستبيان على عدد من المختصين في مجال تقنية المعلومات للتحقق من صدقه الظاهري ومناسبته لأهداف الدراسة. وأظهرت النتائج قبول الأداة للتحليل الإحصائي.

9.5 أساليب التحليل الإحصائي

تم تحليل البيانات باستخدام برنامج SPSS ، حيث تم اعتماد مستوى دلالة إحصائية.($\alpha = 0.05$)

وشملت أساليب التحليل ما يلي:

1. الإحصاءات الوصفية (المتوسط الحسابي، الانحراف المعياري، النسب المئوية).
2. معامل ارتباط بيرسون (Pearson Correlation) لقياس العلاقة بين المتغيرات.
3. تحليل الانحدار الخطي المتعدد (Multiple Regression) لتحديد المتغيرات الأكثر تأثيرًا في الرضا العام.

10- نتائج الدراسة

10.1 النتائج الوصفية

أظهرت نتائج التحليل الوصفي أن متوسط الرضا العام عن التطبيقات المصرفية بلغ (3.28 من 5)، مما يشير إلى مستوى رضا متوسط يميل إلى الإيجابي. كما بلغ متوسط سهولة التفعيل (3.59)، ومتوسط سهولة الاستخدام (3.98)، وهو ما يعكس قبولًا جيدًا من المستخدمين بعد مرحلة التفعيل الأولي.

في المقابل، جاء متوسط تقييم الرسوم والخصومات منخفضًا نسبيًا (2.23)، مما يدل على وجود عدم رضا واضح فيما يتعلق بالرسوم المصرفية المرتبطة بالخدمات الإلكترونية.

أما متوسط تقييم التجربة العامة فقد بلغ (3.50)، مما يعكس تجربة مقبولة إجمالًا، مع وجود مجال للتحسين.

10.2نتائج اختبار الفرضيات (معامل بيرسون)

أظهرت نتائج اختبار معامل ارتباط بيرسون وجود علاقات ارتباط إيجابية ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) كما يلي:

- العلاقة بين الرضا العام والتجربة الرقمية:

  $r = 0.568$ ، $p \le 0.001$

  علاقة إيجابية متوسطة إلى قوية.
- العلاقة بين الرضا وسهولة التفعيل:

  $r = 0.489$ ، $p \le 0.001$

  علاقة إيجابية متوسطة.
- العلاقة بين الرضا وسهولة الاستخدام:

  $r = 0.462$ ، $p \le 0.001$

  علاقة إيجابية متوسطة.
- العلاقة بين الرضا وتقييم الرسوم:

  $r = 0.287$ ، $p \le 0.001$

  علاقة إيجابية ضعيفة نسبيًا.

وعليه، تم قبول الفرضيات الثلاث الأولى، بينما أظهر متغير الرسوم تأثيرًا ضعيفًا مقارنة بالعوامل التقنية.

10.3 نتائج تحليل الانحدار المتعدد

أظهر تحليل الانحدار أن نموذج الدراسة دال إحصائيًا عند مستوى($p \le 0.001$) ، حيث بلغ معامل التحديد ($R^2 = 0.408$)، مما يعني أن المتغيرات المستقلة تفسر حوالي 40.8% من التغير في مستوى الرضا العام.

وقد تبين أن:

- التجربة العامة تمثل المتغير الأكثر تأثيرًا($\beta = 0.448$)
- تليها سهولة التفعيل($\beta = 0.228$)
- ثم سهولة الاستخدام($\beta = 0.148$)
- بينما لم يظهر متغير الرسوم تأثيرًا معنويًا في النموذج.

11- مناقشة النتائج

تشير نتائج الدراسة إلى أن جودة التجربة الرقمية تمثل العامل الأبرز في تشكيل رضا العملاء، وهو ما يتفق مع ما توصلت إليه دراسة Sahi et al. (2021) التي أكدت أن الثقة الرقمية ترتبط ارتباطًا وثيقًا بجودة التفاعل الرقمي.

كما تدعم النتائج ما أشار إليه Alalwan et al. (2017) بأن سهولة الاستخدام والأمان المدرك يمثلان من العوامل الأساسية في تبني الخدمات المصرفية عبر الهاتف المحمول.

ومن الملاحظ أن الرسوم المصرفية لم تكن العامل الأكثر تأثيرًا في الرضا العام، مما يشير إلى أن العملاء قد يعطون الأولوية للاستقرار التقني وسهولة الاستخدام على حساب التكلفة المالية، وهو ما يعكس تحولًا في سلوك المستخدمين نحو تقدير جودة الخدمة الرقمية.

أما فيما يتعلق بالتقييم الأمني الفني، فإن عدم وجود آلية لاكتشاف تفعيل وضع المطور في بعض التطبيقات قد يؤثر على الثقة الرقمية على المدى الطويل، خاصة في ظل تزايد التهديدات السيبرانية. ويتوافق ذلك مع توصيات OWASP (2023)التي تؤكد أهمية فحص بيئة التشغيل كجزء من ممارسات الأمن القياسية.

وبناءً على ذلك، يمكن القول إن تحسين البنية التقنية للتطبيقات المصرفية الليبية يمثل أولوية استراتيجية لتعزيز جودة الخدمة وزيادة رضا العملاء.

12- نتائج التقييم الأمني الفني

أظهرت الاختبارات التطبيقية ما يلي:

1. تفاوت في آليات التحقق من الهوية.
2. غياب آليات متقدمة لاكتشاف بيئة التشغيل غير الآمنة في بعض التطبيقات.

ملاحظة مهمة :عند تفعيل "وضع المطور (Developer Mode) "وميزة "تصحيح أخطاء"USB ، لم تقم بعض التطبيقات بإجراء فحص أو تقييد لعمل التطبيق في هذه البيئة.

ورغم أن تفعيل وضع المطور لا يُعد اختراقًا بحد ذاته، إلا أن عدم التحقق من هذه البيئة قد يسمح باستخدام أدوات تحليل أو مراقبة في حال استغلال الجهاز في بيئة غير آمنة، خاصة في غياب آليات مثل:

- اكتشاف الروت (Root Detection)
- التحقق من سلامة بيئة التشغيل (Runtime Integrity Check)

وهو ما يشير إلى الحاجة لتعزيز آليات الحماية الوقائية

13- أبرز التحديات المكتشفة

- تعقيدات في مرحلة التفعيل
- ضعف واضح في خدمات الدعم الفني
- عدم وضوح الرسوم
- مشاكل في استقرار بعض التطبيقات
- تفاوت في مستوى الحماية الوقائية

14- الدراسات المستقبلية

في ضوء نتائج الدراسة الحالية، تقترح الباحث إجراء عدد من الدراسات المستقبلية التي من شأنها تعميق الفهم حول أمن وكفاءة التطبيقات المصرفية الليبية، ومن أبرزها:

1. إجراء اختبارات اختراق تقنية معمقة (Penetration Testing) على التطبيقات المصرفية باستخدام أدوات متخصصة لتحليل مستوى الحماية الفعلي.
2. دراسة أثر تطبيق المصادقة متعددة العوامل (Multi–Factor Authentication) على مستوى الثقة الرقمية لدى العملاء.
3. تحليل الكود المصدري للتطبيقات المصرفية – إن أمكن – لتقييم مدى توافقها مع معايير OWASP Mobile Security.
4. توسيع نطاق الدراسة ليشمل مقارنة بين المصارف الليبية والمصارف في دول عربية أخرى.
5. دراسة العلاقة بين الأمن السيبراني وسلوكيات الاستمرار في استخدام التطبيقات المصرفية (Usage Continuance Behavior).

ومن شأن هذه الدراسات أن تسهم في تطوير إطار وطني لتعزيز أمن الخدمات المصرفية الرقمية في ليبيا.

15- التوصيات

1. اعتماد معايير أمن سيبراني موحدة على مستوى القطاع المصرفي الليبي.
2. تضمين آليات فحص بيئة التشغيل (التحقق من وضع المطور، كشف الروت، التحقق من سلامة الجهاز).
3. تحسين تجربة المستخدم في مرحلة التفعيل.
4. تطوير أنظمة دعم فني سريعة وفعالة Live Chat أو مركز دعم مباشر.
5. تعزيز الشفافية في عرض الرسوم والخصومات.
6. إجراء اختبارات الاختراق بشكل دوري بواسطة جهات متخصصة.
7. توفير حملات توعية رقمية للمستخدمين حول الاستخدام الآمن للتطبيقات.

16- الخاتمة

توصلت الدراسة إلى أن التطبيقات المصرفية الليبية تمثل خطوة إيجابية نحو التحول الرقمي، إلا أنها ما زالت تحتاج إلى تطوير على مستوى الأمان التقني، والدعم الفني، ووضوح السياسات المالية. كما أظهرت النتائج أن رضا المستخدمين يقع ضمن المستوى المتوسط الجيد، مما يعكس وجود قاعدة يمكن البناء عليها وتحسينها.

إن تعزيز الأمن السيبراني وتطوير تجربة المستخدم يمثلان عاملين حاسمين في رفع جودة الخدمات المصرفية الرقمية وزيادة ثقة العملاء في البيئة المصرفية الإلكترونية داخل ليبيا.

17 المراجع

1. بن حامد، زهرة محمود .(2022) .دور الأمن السيبراني في حماية الأنظمة والبيانات .رسالة ماجستير غير منشورة، جامعة عمان، عمان، الأردن.
2. الحسن، محمد حسين .(2011) .الإدارة الإلكترونية .عمان: مؤسسة الوراق للنشر والتوزيع.

3. الطائي، محمد عبدالحسين .(2010) .التجارة الإلكترونية: المستقبل الواعد للأجيال القادمة .عمان: دار الثقافة للنشر.
4. عزام، عبد الرحيم طارق .(2019) .أثر الأنظمة الرقمية في تحسين حماية البيانات المصرفية: دراسة على البنوك التجارية في عمان .رسالة ماجستير غير منشورة، جامعة عمان، عمان، الأردن.
5. غلاء، أبو بكر محمد، الدالي، محمود محمد، وأعليجة، معمر جمال. (2022). نظم الدفع الإلكتروني وأثرها في تحسين الأداء للمصارف التجارية الليبية: دراسة حالة .مجلة المنتدى الأكاديمي، 6(1)، الجامعة الأسمرية الإسلامية، زليتن.
6. ناشف، فاطمة .(2018) .وسائل الدفع الإلكتروني في المؤسسات المالية الجزائرية .رسالة ماجستير، جامعة مستغانم، الجزائر.

المراجع الأجنبية

1. Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2017). Examining factors influencing customers' intentions and adoption of mobile banking. *International Journal of Bank Marketing*, 35(3), 404–423.
2. OWASP. (2023). *OWASP Mobile Top 10 Security Risks*. Open Web Application Security Project. Retrieved from https://owasp.org
3. Sahi, G. K., Deng, Z., & Cheng, Y. (2021). Trust in digital banking and its impact on customer satisfaction and loyalty. *Journal of Retailing and Consumer Services*, 62, 102110.