

Engineering Cloud Financial Sovereignty in Libya: Towards a Self-Adaptive Immune System

Dr. Ismail Dawibi *

Department of Political Science, Faculty of Economics and Commerce, Alasmarya Islamic University, Zliten, Libya

هندسة السيادة المالية السحابية في ليبيا: نحو نظام مناعي ذاتي التكيف

د إسماعيل فرج الذويبي *

قسم العلوم السياسية، كلية الاقتصاد والتجارة، الجامعة الإسلامية الأسمرية، زليتن، ليبيا

*Corresponding author: ismail.sovereign@proton.me

Received: July 29, 2026	Accepted: September 25, 2026	Published: October 06, 2026
 Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).		

Abstract:

This study addresses the critical gap arising from the unprecedented surge in electronic payment transactions within the Libyan banking sector, which exceeded LYD 764.9 billion according to Central Bank of Libya data (September 2026), alongside associated operational vulnerabilities, cyber risks, and fragmented monitoring. The research aims to design an architectural model for a self-adaptive sovereign financial cloud powered by a cyber-immune system to ensure real-time response to operational shocks and anomalies. Utilizing a Design Science Research Methodology (DSRM) for the architectural build and a descriptive-analytical approach to evaluate central bank statistical data, the study demonstrates that implementing this model enhances financial inclusion and transparency. Furthermore, it empowers the central bank to detect and mitigate financial anomalies instantly. Additionally, results prove that integrating Zero-Knowledge Proofs (ZKP) ensures absolute privacy and regulatory compliance while reducing transaction settlement time to 3 instantaneous seconds. This ultimately establishes algorithmic governance that safeguards digital sovereignty and financial stability.

Keywords: Sovereign Financial Cloud, Self-Adaptive Cyber Immunity, Central Bank of Libya, Algorithmic Governance, Financial Inclusion.

الملخص

تسعى هذه الدراسة إلى معالجة الفجوة الناجمة عن التسارع الهائل في تعاملات الدفع الإلكتروني في القطاع المصرفي الليبي، والتي تجاوزت 764.9 مليار دينار وفقاً لبيانات مصرف ليبيا المركزي (سبتمبر 2026)، وما يرافقها من هشاشة تشغيلية ومخاطر سيبرانية وتشتت رقابي. تهدف الدراسة إلى بناء نموذج معماري هندسي لسحابة مالية سيادية ذاتية التكيف تعمل بنظام مناعي سيبراني يضمن الاستجابة اللحظية للصدمات والانحرافات التشغيلية. تعتمد الدراسة على منهج بحث علوم التصميم الهندسية لبناء المعمارية والنظام المناعي، والمنهج الوصفي التحليلي لتشخيص البيانات الإحصائية والمالية الصادرة عن البنك المركزي. توصلت الدراسة إلى أن تطبيق هذا النموذج يعزز الشمول المالي والشفافية، ويزيد من قدرة البنك المركزي على كشف وتطويق الشذوذ المالي والانحرافات لحظياً، كما أثبتت النتائج أن دمج تقنيات إثباتات المعرفة الصفرية (ZKP) يضمن الامتثال التنظيمي والخصوصية المطلقة مع تقليص زمن تسوية المعاملات إلى 3 ثوانٍ لحظية. أدى ذلك إلى تحقيق حوكمة خوارزمية تكفل السيادة الرقمية والاستقرار المالي.

الكلمات المفتاحية: السيادة المالية السحابية، المناعة السيبرانية ذاتية التكيف، مصرف ليبيا المركزي، الحوكمة الخوارزمية، الشمول المالي.

المقدمة

تشهد البيانات المالية العربية ولا سيما في الدول ذات الاقتصادات الانتقالية مثل ليبيا، تحولات رقمية متسارعة تفرض إعادة النظر في هياكل الأنظمة المالية التقليدية (Gomber et al., 2018) وفي البيئة الليبية تحديداً تجلى هذا التحول في قفزة استثنائية وغير مسبقة في الاعتماد على وسائل الدفع الإلكتروني والخدمات المصرفية الرقمية (Central Bank of Libya, 2025) حيث كشف التقرير الرسمي لمصرف ليبيا المركزي الصادر في سبتمبر 2026 عن وصول حجم معاملات الدفع الإلكتروني إلى 764.9 مليار دينار ليبي خلال ثمانية أشهر فقط مدفوعة بانتشار تطبيقات المحمول وخدمات التحويل الفوري (Central Bank of Libya, 2026a). رغم هذا النمو الرقمي المتسارع إلا أنه يصطدم ببنية تحتية تقنية تعاني من التشتت والهشاشة التشغيلية، والاعتماد على برمجيات وتقنيات قد تفتقر إلى الأطر السيادية الوطنية الكفيلة بحمايتها من الهجمات السيبرانية واختناقات الخدمة، يبرز هذا الواقع فجوة مناعة رقمية تعوق قدرة السلطات النقدية والمصارف عن الاكتشاف المبكر للانحرافات المالية وتتبع استخدامات النقد الأجنبي، وكشف أنماط الاحتيال وشبهات غسل الأموال بأسلوب لحظي وديناميكي.

تأتي هذه الدراسة لتقديم إطار تطبيقي هجين يربط بين الهندسة السيادية والسحابة المصرفية الوطنية، من خلال تطوير نموذج معماري لسحابة مالية سيادية تعمل بنظام مناعي سيبراني ذاتي التكيف، يستند النموذج إلى ميكانيزمات الحوكمة الخوارزمية وتقنيات التشفير الحديثة مثل إثباتات المعرفة الصفرية (ZKP) والعقود الذكية، بما يضمن المعالجة الآمنة للبيانات داخل الحدود الوطنية، ويوفر للسلطة النقدية أدوات رصد لحظية تعزز الشفافية والإفصاح المالي وتدعم الاستقرار الاقتصادي والسيادة الرقمية.

1. مشكلة البحث

يشهد القطاع المالي والمصرفي الليبي قفزة غير مسبقة في الاعتماد على معاملات الدفع الإلكتروني والخدمات المالية الرقمية، حيث أشارت بيانات مصرف ليبيا المركزي (Central Bank of Libya, 2026b) إلى تجاوز إجمالي معاملات وسائل الدفع الإلكتروني حاجز 764.9 مليار دينار خلال ثمانية أشهر فقط، يقودها التحويل الفوري وتطبيقات المحمول.

غير أن هذا التسارع الرقمي الهائل يجري فوق بنية تحتية تقنية ومصرفية لا تزال تعاني من هشاشة المكونات التشغيلية ومخاطر سيبرانية متزايدة وتشتت في الحوكمة والرقابة اللحظية، ناهيك عن الاعتماد على برمجيات وتقنيات خارجية تفتقر إلى الأطر السيادية الوطنية يترتب على هذا الوضع حدوث فجوة مناعة رقمية تتمثل في، العجز عن الاكتشاف المبكر للانحرافات المالية والاختناقات التشغيلية وهجمات حجب الخدمة وكشف أنماط الاحتيال وشبهات غسل الأموال في التدفقات الضخمة للنقد الأجنبي والمعاملات اليومية بأسلوب لحظي وديناميكي، وتتحدد مشكلة الدراسة في السؤال المحوري التالي:

كيف يمكن بناء نموذج معماري لسحابة مالية سيادية ذاتية التكيف تعمل بنظام مناعي سيبراني، لتعزيز الشمول المالي والشفافية وضمان الاستجابة اللحظية للصدمات والانحرافات في البيئة المصرفية الليبية؟

الأسئلة الفرعية

1. السؤال التشخيصي: ما طبيعة وحجم الهشاشة والمخاطر التشغيلية في معمارية المدفوعات الرقمية الحالية في ليبيا في ضوء التسارع الهائل لتعاملات الدفع الإلكتروني (البالغة 764.9 مليار دينار)؟
2. السؤال الهندسي: ما المعمارية التقنية والتصميم الهيكلي المناسب لبناء سحابة مالية سيادية تحقق معايير العزل التام للبيانات الوطنية مع ضمان المرونة والتكامل بين البنك المركزي والمصارف التجارية؟
3. السؤال الوظيفي (المناعي): كيف تساهم ميكانيزمات المناعة السيبرانية ذاتية التكيف وتقنيات الحوكمة الخوارزمية مثل (ZKP و Smart Contracts) في رصد وتطويق الانحرافات والأنشطة المشبوهة لحظياً؟

4. السؤال التطبيقي/التقني: ما خارطة الطريق والأطر التشريعية والتقنية الكفيلة بتحويل هذا النموذج إلى تطبيق عملي يخدم استراتيجية الشفافية والإفصاح لمصرف ليبيا المركزي ويقلل العجز والهدر المالي؟

2. فرضية الدراسة

يؤدي تطبيق نموذج السحابة المالية السيادية ذاتية التكيف إلى تعزيز السيادة الرقمية وحماية هذا الحجم الضخم من التداولات (764.9 مليار دينار) من المخاطر السيبرانية والانحرافات، مع رفع كفاءة الرقابة اللحظية لتشمل هذا التوسع الهائل في البنية التحتية.

3. أهداف البحث

تهدف هذه الدراسة إلى تحقيق ما يلي:

1. تأمين وحوكمة 764.9 مليار دينار من التداولات الإلكترونية، ورفع نسبة العمليات الخاضعة للرقابة اللحظية من 0% (في النظام التقليدي) إلى 100%.
2. تصميم نموذج معماري هندسي لسحابة مالية سيادية توفر البيئة الآمنة للخدمات المصرفية الوطنية.
3. تطوير ميكانيكية مناعية خوارزمية لتتبع وإدارة المخاطر والسيولة وكشف الاحتيال لحظياً.
4. اقتراح خارطة طريق تنفيذية تلبي متطلبات الحوكمة والتشريعات والبنية التحتية لضمان نجاح التطبيق.

4. أهمية البحث

تتجلى أهمية هذه الدراسة في جانبين رئيسيين:

الأهمية العلمية/الأكاديمية: تقديم إطار نظري وهندسي يربط بين الهندسة السيادية والسحابة المصرفية، والمناخ السيبرانية المعتمدة على الذكاء الاصطناعي.

الأهمية العملية/التطبيقية: تزامن هذه الدراسة مع قفزة التعاملات الرقمية في ليبيا (764.9 مليار دينار) ووجود حاجة ماسة لدى السلطات النقدية (مصرف ليبيا المركزي) لحلول سيادية لحماية هذه التدفقات، وتنفيذ الشفافية والإفصاح المالي ومكافحة غسل الأموال ومتابعة استخدامات النقد الأجنبي بفعالية.

5. منهجية البحث

. المنهج الهندسي/التصميمي لتصميم وبناء المعمارية التقنية والنظام المناخي السحابي.

. المنهج الوصفي التحليلي لتحليل البيانات والبيانات المالية والتشغيلية الواردة في تقارير مصرف ليبيا المركزي سبتمبر 2026 (تحليل أرقام المدفوعات، التحويلات الفورية، الصكوك، واستخدامات النقد الأجنبي).

6. الدراسات السابقة

تُعد الدراسات السابقة البوصلة التي تضمن أن البحث يسير في الاتجاه الصحيح، وتساعد في تحديد الفجوة المعرفية التي يسعى البحث الحالي لسدها، فيما يلي استعراض لبعض الدراسات ذات الصلة مع الإشارة إلى أوجه الاستفادة والفجوة التي يمثلها البحث الحالي:

استعرضت الدراسة عدة دراسات رئيسية: تناولت الأولى (IBM, 2025) مفهوم السحابة السيادية ودورها في الامتثال التنظيمي، وتقارير تقييم التقنيات السحابية المتقدمة للإدارة المالية السحابية التي أصبحت معياراً أساسياً للمؤسسات التنظيمية (Gartner, 2025) وركزت الثانية (Reply, 2025) على السيادة في الخدمات المالية الأوروبية مشيرة إلى أن 48% من المؤسسات تصنف السيادة ضمن أهم التحديات، أما الثالثة (IBM, 2025) فتناولت الإدارة المالية السحابية كاستراتيجية شاملة، بينما قدمت الرابعة (الراجحي) نموذجاً للادخار الذكي عبر المدفوعات اليومية، وجاءت الخامسة المبادرة الإماراتية (2024-2025) كنموذج إقليمي لتوطين البيانات المالية (Salaam Gateway, 2026) والسادسة تناولت دراسات التحول الرقمي في البنوك المركزية بالدول النامية أو الدول ذات البيانات الانتقالية/المحفوفة بالمخاطر.

إبراز الفجوة البحثية: حيث ركزت الدراسات السابقة إما على الأمن السيبراني التقليدي أو التحول الرقمي التجاري، بينما تفتقر الأدبيات إلى نموذج جمع بين السيادة السحابية الوطنية والمناخ ذاتية التكيف الخوارزمية المطبقة على بيئة مصرفية نامية تشهد طفرة تدفقات إلكترونية سريعة كما هو الحال في ليبيا.

ثانياً: الأطر المفاهيمية والأدبيات المرجعية

يشكّل هذا المحور الركيزة النظرية للنموذج الهندسي المقترح حيث يُحدد المفاهيم الأساسية الثلاثة المتقاطعة: السيادة المالية السحابية (الإطار القانوني والتشغيلي) الحوكمة الخوارزمية (آلية الأتمتة) وتقنيات المناعة السيبرانية (درع الحماية والتكيف) تمهيداً للتصميم الهندسي في المحور الثاني وتطبيقه على النظام الادخاري الرقمي في المحور الثالث.

1. السيادة المالية السحابية: المفاهيم والارتكازات

تُعرّف السحابة السيادية بأنها بيئة حوسبة تخضع بياناتها وعملياتها التشغيلية حصرياً لقوانين الدولة، بحيث لا يمكن لأي طرف خارجي الوصول إليها دون إذن قانوني (IBM, 2025) وفي السياق المالي تمتد السيادة المالية السحابية إلى ثلاث ركائز مترابطة:

1. سيادة البيانات: تخزين ومعالجة البيانات المالية الحساسة داخل الحدود الجغرافية للدولة وخضوعها للقوانين الوطنية في الخصوصية والإفصاح.
2. السيادة التشغيلية: قدرة الدولة على إدارة البنية التحتية السحابية بشكل مستقل مع خطط طوارئ محلية لضمان استمرارية الأعمال.
3. السيادة التقنية: امتلاك الكوادر والمعايير الوطنية لتطوير وصيانة البيئة السحابية وهو الأصعب في الدول الانتقالية لكنه الأهم للاستدامة.

تشير الأدبيات (Reply, 2025) إلى أن 48% من المؤسسات المالية الأوروبية تصنف السيادة الرقمية ضمن أهم التحديات، لكن هذه الأدبيات تركز على الدول المتقدمة، بينما تظل البيانات العربية الانتقالية – كليياً – بحاجة لنموذج يراعي البنية الهشة وضعف الكوادر.

تكتسب هذه الركائز أهمية قصوى في ضوء البيانات الرسمية لمصرف ليبيا المركزي (سبتمبر 2026) التي تكشف عن قفزة نوعية في حجم التداولات الإلكترونية بلغت 764.9 مليار دينار خلال ثمانية أشهر فقط، مدفوعة بـ 297.5 مليار دينار من التحويلات الفورية و 247.3 مليار دينار عبر تطبيقات الهاتف، هذا الحجم الكبير من التدفقات المالية الرقمية، الذي يمر عبر بنية تحتية موزعة على 220,954 نقطة بيع و 5.8 مليون بطاقة مفعلة يجعل من السيادة المالية السحابية ضرورة حتمية، ليس فقط لحماية البيانات بل لضمان استمرارية هذه التدفقات الحيوية ومنع أي انقطاع قد يشل الاقتصاد الوطني، وهو ما يتفق مع التوجهات العالمية الحديثة لتأمين القطاعات المالية الحساسة، مثل المبادرة الأوروبية لبناء سحابة سيادية مخصصة للقطاع المالي بتكلفة 7.8 مليار يورو (AWS & SAP, 2025).

2. الحوكمة الخوارزمية والذكاء الاصطناعي

إذا كانت السيادة هي الجسد التشغيلي فالحوكمة الخوارزمية تمثل العقل المُدبّر، أي تحويل القواعد والسياسات المالية إلى بروتوكولات برمجية ذكية تُنفّذ تلقائياً عند توفر الشروط، ويلعب الذكاء الاصطناعي دوراً في ثلاثة مستويات:

1. الرصد والتحليل اللحظي: استخدام خوارزميات التعلّم الآلي لتحليل تدفق السيولة وأنماط المعاملات آنياً.
2. اتخاذ القرار الآلي: تعديل الفوائد والحوافز تلقائياً دون انتظار دورات اللجان النقدية.
3. التعلّم والتطوّر الذاتي: تحسّن الخوارزميات بمرور الوقت عبر التعلّم من الأخطاء السابقة (Pinheiro & Pinheiro, 2025).

تُحذّر الأدبيات النقدية (Zuboff, 2019) & (O'Neil, 2016) من التحكّم الخوارزمي المطلق، لذا تؤكد الدراسة أن الحوكمة الخوارزمية لا تلغي الدور البشري، بل تُعيد توزيعه من التنفيذ الروتيني إلى الإشراف الاستراتيجي والتدخل الاستثنائي وفق آلية نافذة الطوارئ (المحور الثاني).

3. تقنيات المناعة السيبرانية والتكيف الذاتي

إذا كانت السيادة هي الجسد والحوكمة الخوارزمية هي العقل، فالمناعة السيبرانية تمثل الجهاز المناعي الذي يحمي النظام ويكيّفه، وهي تعني قدرة النظام على: اكتشاف التهديدات (التوقع) التكيف معها (الاستجابة الذاتية) التعافي السريع (المرونة) والتعلّم من الهجمات السابقة (التطوّر المناعي).

وتبرز تقنية إثباتات المعرفة الصفرية (ZKP) كأداة محورية تتيح التحقق من أهلية المواطن للحوافز دون الكشف عن رصيده أو تاريخ معاملاته محققة معادلة: الامتثال + الخصوصية + السرعة، كما تتطلب هذه المنة التأسيس لاستراتيجيات تشفير متقدمة مقاومة للحسابات الكمومية (Springer, 2025) لضمان استدامة التشفير والتعافي.

أما الأنظمة ذاتية التعديل فتقوم على خوارزميات تعيد تكوين نفسها تلقائياً عند تغير الظروف (كتعديل الفوائد عند ارتفاع التضخم) مع تحديد نقاط تحوّل واضحة سنصممها في المحور الثاني.

4. القراءة النقدية للدراسات السابقة والفجوة المعرفية

تُلخّص القراءة النقدية للأدبيات في ثلاثة مستويات:

المستوى الأول – الأدبيات العالمية: ركّزت على الأطر التنظيمية للسيادة (كدراسات IBM وReply) لكنها أغفلت الهندسة التطبيقية في البيانات محدودة الموارد والمناعة الذاتية دون تدخل بشري. المستوى الثاني – المبادرات الإقليمية: تُثمّن الدراسة المبادرة الإماراتية (2024-2025) كأول نموذج عربي (Salaam Gateway, 2026) لكنها ركّزت على توطين البيانات دون معمارية خوارزمية للتكيف وهي تجربة مؤسساتية كبرى لا تُعمّم بسهولة على دول انتقالية كليبيا. المستوى الثالث – تطبيقات الادخار الرقمي: قدّمت أتمتة جزئية (كالراجحي) لكنها تخلو من البعد السيادي والمناعي والخوارزمي المتطور.

خلاصة الفجوة: توزّعت الأدبيات بين تنظيم بلا هندسة (عالمياً) سيادة بلا تكيف (إقليمياً) وتطبيق بلا سيادة (محلياً) ومن هنا تنطلق الدراسة لتقديم إطار هندسي – خوارزمي – سيادي – مناعي، يُختبر في البيئة الادخارية الليبية وهو الإضافة المعرفية الجوهرية لهذه الورقة.

ثالثاً: المعمارية الهندسية للنموذج المقترح

بعد وضع الأطر المفاهيمية ينتقل هذا المحور إلى التصميم الهندسي التفصيلي للنظام القائم على ثلاث طبقات متكاملة: البنية التحتية السيادية والخوارزميات الذاتية والتدفقات التشغيلية لتحقيق أربع خصائص: السيادة الذكاء المناعة الشفافية.

1. مكونات البنية التحتية السيادية

صُمّمت البنية لتلبي متطلبات السيادة الثلاثية (البيانات، التشغيل، التقنية) مع مراعاة محدودية الموارد في البيانات الانتقالية وتتكون من عدة طبقات:

الطبقة الأولى: المعمارية السحابية الهجينة: تجمع بين سحابة خاصة وطنية للبيانات شديدة الحساسية (تُدار بكفاءات وطنية) وسحابة عامة مُدارة للعمليات الأقل حساسية (مع اشتراط تخزين البيانات داخل الدولة) يمنح هذا المزيج مرونة عالية مع سيادة كاملة على البيانات الأكثر حساسية ويُقلل التكاليف التشغيلية (IBM, 2025).

جدول (1) ملخص مكونات البنية التحتية السيادية في النموذج المقترح

الطبقة	المكون الرئيسي	الوظيفة الأساسية
الطبقة الأولى	المعمارية السحابية الهجينة	الجمع بين سحابة خاصة وطنية للبيانات الحساسة وسحابة عامة مُدارة للعمليات الأقل حساسية، لتحقيق التوازن بين السيادة والتكلفة
الطبقة الثانية	طبقات تشفير متعددة	تطبيق التشفير من النهاية إلى النهاية والتشفير المتجانس والتوقيع الرقمي لحماية البيانات في حالات السكون والنقل والمعالجة
الطبقة الثالثة	بروتوكولات الربط التنظيمي	ربط البنية التقنية بالإطار القانوني عبر واجهات الامتثال وسجل التدقيق الموزع وبروتوكول الإخطار التلقائي
الطبقة الرابعة	إثباتات المعرفة الصفرية (ZKP)	التحقق من أهلية المواطن للحوافز دون الكشف عن رصيده أو تاريخ معاملاته لتحقيق الخصوصية مع الامتثال

الطبقة الخامسة	إدارة الهوية والوصول (IAM)	اعتماد المصادقة متعددة العوامل والبيومترية لمنع انتحال الهوية مع الربط بالسجل المدني الوطني
الطبقة السادسة	نظام المقاصة الإلكترونية (1.6 مليون صك بقيمة 81 مليار دينار) ونظام التسوية اللحظية (RTGS)	ربط أنظمة المقاصة والتسوية القائمة بالنظام السيادي الجديد وضمان تدفق البيانات لحظياً لأغراض الرقابة والتحليل.

المصدر: إعداد الباحث بناءً على التصميم الهندسي للنموذج المقترح.

الطبقة الثانية: طبقات التشفير المتعددة: تُطبّق ثلاثة مستويات: التشفير من النهاية إلى النهاية (لحماية البيانات من أي طرف غير مخوّل) والتشفير المتجانس (لمعالجة البيانات المشفرة دون فكها - مرحلياً) والتوقيع الرقمي والطوابع الزمنية لتشفير المعاملات وجعلها مقاومة للتلاعب والهجمات الكمومية (Springer, 2025).

الطبقة الثالثة: بروتوكولات الربط التنظيمي: تربط البنية التقنية بالإطار القانوني عبر: واجهات برمجة تطبيقات الامتثال (تربط النظام بالبنك المركزي وهيئة الرقابة) وسجل تدقيق موزع غير قابل للتغيير (يسجل كل قرار خوارزمي) وبروتوكول إخطار تلقائي (يبلغ السلطات عند تجاوز المؤشرات حدودها الآمنة). الطبقة الرابعة: تطبيق إثباتات المعرفة الصفرية: (ZKP) وهي الطبقة الأكثر ابتكاراً حيث تتيح التحقق من أهلية المواطن للحوافز دون الكشف عن رصيده أو تاريخ معاملاته، عبر توليد إثبات رياضي يُرسل إلى الجهة المانحة التي تتحقق منه دون الاطلاع على البيانات الخام، وتُحقق معادلة: الامتثال + الخصوصية + السرعة.

الطبقة الخامسة: إدارة الهوية والوصول: (IAM) تعتمد على مصادقة متعددة العوامل وبيومترية (بصمة، تعرّف على الوجه) لمنع انتحال الهوية مع ربطها بسجل مدني وطني وحفظ البيانات البيومترية مشفرة. الطبقة السادسة: ربط أنظمة المقاصة والتسوية اللحظية (RTGS) بالنظام السيادي الجديد لضمان تدفق بيانات التداولات المالية والإنفاق الحكومي لحظياً لأغراض الرقابة والتحليل (Central Bank of Libya, 2026b).

2. خوارزميات التكييف والمناعة الذاتية

تمثل الخوارزميات الجهاز العصبي للنظام وتعمل وفق مفهوم المناعة السيبرانية المتقدمة للأنظمة المالية ((Bulgakova et al., 2025 عبر ثلاثة مسارات متوازية: المسار الأول: الاستجابة اللحظية للصدمات المالية: تعتمد على التعلّم الآلي الإشرافي (للتدريب على بيانات الأزمات التاريخية) والتعلّم المعزّز (لمحاكاة سيناريوهات الاستجابة) ترصد مؤشرات أنية (التضخم، سعر الصرف، الودائع، طلبات السحب) وعند تجاوز عتبة الخطر، تتخذ إجراءات تلقائية: تعديل الفوائد، تفعيل حوافز إضافية، رفع حدود السحب مؤقتاً، مع إخطار البنك المركزي وتبرير القرار خوارزمياً، وترصد هذه المسارات أيضاً مؤشرات حجم التداولات اللحظية عبر نقاط البيع (POS) وتطبيقات الهاتف بما في ذلك 1.6 مليون صك بقيمة 81 مليار دينار تمر عبر نظام المقاصة الإلكترونية. المسار الثاني: الاستهداف الآلي لثغرات الاحتيال: باستخدام خوارزميات كشف الشذوذ القائمة على التعلّم العميق التي تتعلم النمط الطبيعي لسلوك المستخدم، وتكشف أي انحراف في أجزاء من الثانية بدقة عالية وإنذارات كاذبة منخفضة مع تعلّم مستمر من كل محاولة احتيال، وعند الاشتباه يتخذ إجراءات متدرجة: تعليق المعاملة، طلب مصادقة إضافية، وإبلاغ الجهات الأمنية في الحالات الخطيرة. المسار الثالث: التعديل الذاتي للسياسات: خوارزميات تعيد معايرة السياسات الادخارية تلقائياً عبر حلقات التغذية الراجعة: تقيس أثر السياسات الحالية وتُقرّن النتائج بالأهداف وتُعدّل الأدوات (الحوافز، الرسوم، القيود) لتقليص الفجوة.

آلية التدخل البشري المشروط (نافذة الطوارئ):

لتجنب التحكّم الخوارزمي المطلق في الأزمات غير المبرمجة تُدمج المعمارية بروتوكولاً استثنائياً بشروط صارمة:

- شروط التفعيل: حالات محدودة كالهجوم السيبراني الواسع، التغير الاقتصادي المفاجئ أو ظهور قرارات خوارزمية غير عادلة.
 - إجراءات التفعيل: قرار جماعي (لجنة ثلاثية: بنك مركزي، هيئة رقابية، خبير تقني) توثيق رقمي مشفّر في سجل موزع ومدة لا تتجاوز 72 ساعة (قابلة للتديد مرة واحدة).
 - إجراءات ما بعد التفعيل: تدقيق فوري من فريق مستقل ورفع التوصيات لهيئة رقابية عليا وتغذية نتائج التدقيق في منظومة التعلم الآلي لمنع تكرار الأخطاء.
- بهذه الآلية تُحقق المعادلة: مناعة ذاتية آنية + تدخل بشري مشروط = نظام هجين يجمع كفاءة الخوارزميات وحكمة البشر.

3. هندسة التدفقات التشغيلية

تهدف إلى رسم خريطة تفاعل الأطراف الفاعلة لتحقيق: الوضوح (تحديد الأدوار) السرعة (إزالة الاختناقات البيروقراطية) والمساءلة (توثيق كل إجراء)، لا يأتي النموذج المقترح ليحل محل البنية التحتية القائمة بل ليعمل كطبقة سيادية ذكية فوقها، فمع وجود 220,954 نقطة بيع و8.2 مليون مشترك في التحويل الفوري و5.5 مليون مشترك في تطبيقات المصارف، يصبح التحدي الأكبر هو ربط هذه الأنظمة المتباينة في نسج سيادي واحد، وهنا تبرز أهمية بروتوكولات الربط التنظيمي (الطبقة الثالثة) التي ستعمل كواجهة برمجية موحدة (API) تربط بين هذه الأنظمة وتضمن تدفق البيانات بشكل آمن ولحظي إلى الخوارزميات المركزية في مصرف ليبيا المركزي لمتابعة مؤشرات الإيراد والإنفاق (Central Bank of Libya, 2026b).

أ. الأطراف الفاعلة الرئيسية

يحدد النموذج ستة أطراف فاعلة رئيسية لكل منها دور محدد في التدفق التشغيلي

الطرف	الدور الرئيسي
المواطن	صاحب الحساب الادخاري مقدّم الطلبات
المؤسسة المالية	الوسيط التنفيذي للمعاملات والسياسات
البنك المركزي	مصدر السياسات النقدية المشرف على الاستقرار
ديوان المحاسبة	الجهة الرقابية المستقلة للامتثال والتدقيق
الخوارزمي المركزي	قلب النظام ينفذ القرارات الآلية ويؤدّ التوصيات
مزود السحابة السيادية	المشغل التقني للبنية التحتية والأمن السيبراني

التدفق التشغيلي النموذجي (فتح حساب وحافز شهري):
 المرحلة الأولى - التسجيل والتحقق: يُقدّم المواطن طلباً عبر التطبيق → تتحقق المؤسسة من هويته → (IAM) تُرسل البيانات مشفّرة للخوارزمي المركزي → يُفتح حساب في السحابة الخاصة.
 المرحلة الثانية - تنفيذ السياسات: يُحدد الخوارزمي الحوافز (وفق سياسات البنك المركزي) → تُرسل للمؤسسة للتطبيق → يُراقب السلوك ويُعدّل الحوافز ديناميكياً.
 المرحلة الثالثة - الرصد والتصدي للاحتيال: عند كل معاملة يفحصها الخوارزمي أنياً → إذا طبيعية تُنفذ وتُسجّل → إذا مشبوهة تُعلّق ويرسل إشعار → بعد تأكيد المواطن (MFA) تُعاد تنشيطها.
 المرحلة الرابعة - التقارير والتدقيق: يُؤدّ الخوارزمي تقارير دورية (يومية، أسبوعية، شهرية) للبنك المركزي وهيئة الرقابة → تُستخدم لتحديث السياسات الكلية → في حال تفعيل نافذة الطوارئ، يُؤدّ تقرير استثنائي فوري.

ب. رسم تخطيطي لسير العمليات

ولتخيل هذه التدفقات بصرياً يمكن تمثيلها في دورة تشغيلية مغلقة (Closed Loop) على النحو التالي:

رابعاً: الحالة التطبيقية – هندسة النظام الادخاري الرقمي

بعد تصميم المعمارية الهندسية ينتقل هذا المحور إلى التطبيق العملي على النظام الادخاري الرقمي في البيئة الليبية (قيمة المدفوعات الرقمية 764.9) للإجابة عن: كيف يُحفّز النظام الادخاري الرقمي المبني على السيادة والمناعة الذاتية الادخار ويُعزز الشمول المالي ويُرسّي الثقة الرقمية في بيئة انتقالية هشة؟

1. إسقاط النموذج على البيئة الادخارية الليبية

يتطلب الإسقاط أربع آليات تشغيلية رئيسية.

أ. الآلية الأولى: حساب الادخار الذكي:

ربط تلقائي بالمعاملات اليومية: تحديد نسبة مئوية (مثلاً 5%) من كل معاملة شراء تُخصم تلقائياً وتُودع في حساب الادخار.

حوافز آتية متغيرة: عائد يتغير تلقائياً حسب مدة الاحتفاظ، انتظام الإيداع، والظروف الاقتصادية (رفع الفائدة عند التضخم).

لوحة تحكم شفافة: تعرض المدخرات، العوائد، التوقعات، وتوصيات تحسين السلوك الادخاري (Desai, 2025).

ب. الآلية الثانية: تطبيق إثباتات المعرفة الصفرية (ZKP) في منح الحوافز:

التحقق من الأهلية: يتحقق النظام عبر ZKP من استيفاء المواطن لشروط الحافز دون كشف رصيده أو معاملاته.

منح الحافز: يُصرّف تلقائياً مع إشعار المواطن بالقيمة والمدة.

الامتثال التنظيمي: تُتاح لهيئة الرقابة التحقق من إجمالي الحوافز إحصائياً دون الاطلاع على بيانات الأفراد (zkVerify, 2025).

ج. الآلية الثالثة: التكيف الذاتي للسياسات الادخارية:

معدل التضخم: إذا تجاوز 5% تُرفع الفائدة تلقائياً لتعويض التضخم.

نسبة الادخار الوطني: إذا انخفضت عن المستهدف تُفعّل حوافز إضافية.

مؤشرات السيولة: إذا لاحظ النظام زيادة غير طبيعية في طلبات السحب يُفعّل إجراءات احترازية مع إشعار البنك المركزي (Perdana et al., 2025).

د. الآلية الرابعة: تعزيز الثقافة المالية الرقمية:

إشعارات توعوية آتية: تُرسل عند كل معاملة لشرح أثرها على المدخرات مستقبلاً.

محاكي الادخار: أداة تفاعلية لمحاكاة سيناريوهات ادخارية مختلفة.

تقييم المعرفة المالية: اختبارات دورية مع توصيات مخصصة للتحسين (World Bank, 2024).

2. تشخيص البيئة المالية الليبية ومعالجة المحددات

لم يعد التحدي في ليبيا هو تحفيز المواطن على استخدام المدفوعات الرقمية بل حماية هذا التحول الكبير، فمع وصول حجم التداول الإلكتروني إلى 764.9 مليار دينار ووجود أكثر من 8.2 مليون مشترك في خدمات التحويل الفوري، أصبح المواطن الليبي مندمجاً فعلياً في الاقتصاد الرقمي، بالتالي يتحول دور حساس الادخار الذكي من مجرد أداة جذب المدخرات إلى أداة تأمين هذه المدخرات وحمايتها من التضخم والمخاطر السيبرانية، عبر تعديل الفوائد تلقائياً وتوفير حوافز للاحتفاظ بالمدخرات في النظام الرسمي بدلاً من تحويلها إلى النقد الأجنبي أو خارج النظام المصرفي.

تحديد مستهدف كمي للنموذج:

الهدف الأول: تأمين وحوكمة 100% من التداولات الإلكترونية (764.9 مليار دينار) عبر النظام المناعي السيبراني، مع رفع نسبة العمليات الخاضعة للتحليل اللحظي من 0% إلى 100% خلال 12 شهراً.

الهدف الثاني: تقليص زمن تسوية المعاملات الادخارية من متوسط 3 أيام عمل إلى 3 ثوان لحظية، مع ضمان عدم تأخير هذا التسريع على أمن 45.9 مليون عملية تحويل فوري و302 مليون عملية POS.

الهدف الثالث: تقليل زمن اكتشاف ومعالجة أي انحراف في أنظمة الدفع الإلكتروني من ساعات (في النظام الحالي) إلى أجزاء من الثانية، مع تغطية 220,954 نقطة بيع و5.8 مليون بطاقة.

3. تقييم الكفاءة المتوقعة

لا يقتصر تقييم النموذج على المؤشرات التشغيلية الكمية فحسب بل يتعداها إلى ثلاثة أبعاد استراتيجية تُحدد نجاحه على المدى المتوسط والبعيد.

أ. البعد الأول: الاستقرار النقدي

نُقاس مساهمة النظام في الاستقرار النقدي من خلال أربعة مؤشرات رئيسية:

- مؤشر التضخم الادخاري: وهو قدرة النظام على حماية قيمة المدخرات من التضخم عبر تعديل الفوائد تلقائياً، يُتوقع أن يُحقق النظام حماية لا تقل عن 80% من قيمة المدخرات من التضخم، مقارنة بـ 40% في النظام التقليدي (حيث تُتخذ القرارات ببطء) (International Monetary Fund, 2025).
- مؤشر السيولة المصرفية: يُقاس عبر حجم الودائع الادخارية الجديدة التي يجذبها النظام، يُتوقع زيادة الودائع الادخارية بنسبة 25% على الأقل خلال 18 شهراً، مما يُعزز سيولة البنوك وقدرتها على الإقراض.
- مؤشر تقلب المعاملات: يُقاس عبر الانحراف المعياري لطلبات السحب والإيداع، يُتوقع أن يُقلل النظام من التقلبات الحادة (التي قد تشير إلى ذعر مصرفي) بنسبة 30% بفضل قدرته على الكشف المبكر عن الأنماط غير الطبيعية واتخاذ إجراءات احترازية تلقائية.
- مؤشر حماية التدفقات الرقمية: يقيس قدرة النظام على حماية 764.9 مليار دينار من التداولات من الاختراق أو التلاعب ويُستهدف تحقيق حماية بنسبة 99.99%.

ب. البعد الثاني: الشفافية المالية والرقابة

يُقاس هذا البعد عبر:

- مؤشر الامتثال التنظيمي: نسبة القرارات الخوارزمية المتوافقة مع اللوائح المالية الوطنية، والمُتوقع أن تتجاوز 99% مقارنة بـ 85% في النظم التقليدية (بسبب الأخطاء البشرية والتأخير) (European Banking Authority, 2025).
- مؤشر قابلية التدقيق: يُقاس عبر مدى سرعة وسهولة توفير سجلات التدقيق للهيئات الرقابية، يُتوقع أن يُقلص النظام زمن التدقيق من أسابيع إلى ساعات بفضل سجل التدقيق الموزع الآلي.
- مؤشر الفساد المالي المُكتشف: يُقاس عبر عدد حالات الاحتيال أو التلاعب المُكتشفة آلياً، يُتوقع أن يزيد النظام من نسبة اكتشاف الاحتيال بنسبة 200% على الأقل مقارنة بالأنظمة التقليدية التي تعتمد على البلاغات البشرية والتدقيق العشوائي.
- مؤشر تغطية الرقابة اللحظية: نسبة نقاط البيع (220,954) وعمليات التحويل الفوري (45.9 مليون) الخاضعة للرقابة اللحظية. يُستهدف 100%.

ج. البعد الثالث: ترسيخ الثقافة المالية الرقمية

وهو البعد الأكثر ابتكاراً في التقييم ويُستهدف رفع وعي 8.2 مليون مشترك في التحويل الفوري و5.5 مليون مشترك في تطبيقات المصارف بكيفية حماية بياناتهم وأموالهم في هذا الفضاء الرقمي الجديد، ويُقاس عبر مؤشرين:

- مؤشر المعرفة المالية الرقمية: يُقاس عبر اختبارات معرفية مدمجة في التطبيق (كما في الآلية الرابعة 3.1) ويُستهدف رفع متوسط درجة المعرفة المالية للمواطنين المستخدمين من 40% (تقدير مبدئي) إلى 60% خلال 18 شهراً.
- معدل تفاعل المستخدمين مع أدوات التوعية: يُقاس عبر عدد مرات فتح أدوات المحاكاة، الإشعارات التوعوية ومشاهدة المحتوى التعليمي، يُستهدف أن يتفاعل 50% على الأقل من المستخدمين مع هذه الأدوات شهرياً، مما يعكس تحولاً في السلوك من مجرد استخدام الخدمة إلى فهمها والتعلم منها.

جدول (2): ملخص مؤشرات تقييم كفاءة النظام المقترح

المستهدف (18 شهراً)	القيمة الحالية	المؤشر	القياس	البعد الاستراتيجي
$\geq 80\%$	(40%~ في الأنظمة التقليدية)	مؤشر التضخم الادخاري	قدرة النظام على حماية قيمة المدخرات من التضخم	الاستقرار النقدي
+25%	-	مؤشر السيولة المصرفية	زيادة حجم الودائع الادخارية الجديدة	الاستقرار النقدي
-30%	-	مؤشر تقلب المعاملات	الانحراف المعياري لطلبات السحب والإيداع	الاستقرار النقدي
$\geq 99.99\%$	0%	مؤشر حماية التدفقات الرقمية	قدرة النظام على حماية 764.9 مليار دينار من الاختراق أو التلاعب	الاستقرار النقدي
$\geq 99\%$	~85%	مؤشر الامتثال التنظيمي	نسبة القرارات الخوارزمية المتوافقة مع اللوائح	الشفافية والرقابة
ساعات	أسابيع	مؤشر قابلية التدقيق	سرعة توفير سجلات التدقيق للهيئات الرقابية	الشفافية والرقابة
+200%	-	مؤشر اكتشاف الفساد	زيادة نسبة اكتشاف حالات الاحتيال آلياً	الشفافية والرقابة
100%	0%	مؤشر تغطية الرقابة اللحظية	نسبة نقاط البيع (220,954) وعمليات التحويل الفوري (45.9 مليون) الخاضعة للرقابة اللحظية	الشفافية والرقابة
$\geq 60\%$	~40%	مؤشر المعرفة المالية الرقمية	متوسط درجة المعرفة المالية للمستخدمين	الثقافة المالية الرقمية
$\geq 50\%$	-	معدل تفاعل المستخدمين مع التوعية	نسبة المستخدمين الذين يستخدمون أدوات التوعية شهرياً	الثقافة المالية الرقمية
$\geq 70\%$	-	مؤشر الثقة الرقمية (DTI)	نسبة رضا المستخدمين وثقتهم بالنظام (استبيان)	الثقة الرقمية

المصدر: إعداد الباحث بناءً على مؤشرات التقييم المقترحة في المحور 3.3، والمراجع الداعمة (World Bank, 2024) (European Banking Authority, (International Monetary Fund, 2025) Bank, 2024) (2025)

4. مؤشر الثقة الرقمية كمعيار نجاح أساسي

لن يُكتفى بالمؤشرات المالية التقليدية (كالسيولة والشفافية) والمؤشرات التشغيلية (كالنسبة المئوية للمدفوعات وزمن التسوية) في تقييم النموذج، بل يُستحدث مؤشر نوعي أساسي يُسمى مؤشر الثقة الرقمية (Digital Trust Index - DTI)، يُعتبر شرطاً ضرورياً (لكن غير كافٍ) لاعتبار النموذج ناجحاً، ويُقاس هذا المؤشر عبر استبيانات رقمية دورية لعينة ممثلة من المستخدمين (يُحدد حجمها إحصائياً بما يضمن تمثيل الفئات العمرية والجغرافية والدخلية المختلفة) ويستهدف ثلاثة محاور رئيسية:

1. شعور المواطن بالأمان تجاه حفظ مدخراته في بيئة سحابية سيادية:
- يُقاس عبر أسئلة مثل: إلى أي مدى تثق بأن مدخراتك آمنة من الاختراق أو السرقة في هذا النظام؟ (مقياس من 1 إلى 5).

يُستهدف تحقيق متوسط درجة لا يقل عن 4 من 5 (أي 80% رضا) في جميع شرائح المستخدمين.

2. درجة فهم المواطن لآلية عمل الخوارزميات التي تدير مدخراته:

يُقاس عبر أسئلة معرفية بسيطة مثل: هل تفهم كيف يُحتسب العائد على مدخراتك؟ وهل تعرف متى وكيف تُتخذ قرارات تعديل الفوائد؟

يُستهدف أن يجيب 60% على الأقل من المستخدمين بنعم أو فهم متوسط على هذه الأسئلة، مما يعكس أن النظام ليس صندوقاً أسود (Black Box) بل مفهوماً وشفافاً.

3. رصد أي تردد في استخدام النظام نتيجة مخاوف سيبرانية أو تنظيمية:

يُقاس عبر أسئلة مثل: هل ترددت في استخدام النظام بسبب مخاوف من اختراق البيانات؟ وهل تشعر بالقلق من أن بياناتك قد تُستخدم لأغراض غير التي صُمم من أجلها؟

يُستهدف ألا تتجاوز نسبة المستخدمين الذين يُبدون تردداً كبيراً 15% من العينة، مما يشير إلى تغلب الثقة على الخوف.

5. معيار النجاح النهائي

يُعتبر تجاوز هذا المؤشر لنسبة 70% من رضا المستخدمين وثقهم بالنظام شرطاً أساسياً لاعتبار النموذج ناجحاً، إلى جانب تحقيق المؤشرات الكمية (نسبة المدفوعات الرقمية وزمن التسوية) فإذا حقق النظام المؤشرات الكمية لكن فشل في بناء الثقة الرقمية يُعد فشله استراتيجياً، لأن الادخار الرقمي في جوهره ينهض على الثقة قبل التقنية، فالمواطن لن يُودع مدخراته في نظام لا يثق به مهما كانت سرعته أو دقته التقنية، وبالمقابل إذا حقق الثقة لكنه فشل في المؤشرات الكمية يُعد ذلك نجاحاً جزئياً يحتاج إلى تحسين تشغيلي وليس فشلاً كلياً.

بهذا التطبيق المتكامل يكون النموذج قد اختُبر في سياق واقعي انتقالي، مع تحديد أهداف كمية ونوعية واضحة وآليات قياس دقيقة، وفي الخاتمة سنستخلص النتائج الأساسية للدراسة ونقدّم توصيات إجرائية لبناء نظام مناعة مالية سيبراني سيادي شامل، مع تحديد آفاق الدراسات المستقبلية التي يمكن أن تُوسع نطاق هذا النموذج أو تُعمّقه.

خامساً: خاتمة

تُختتم هذه الدراسة بعرض موجز لأهم النتائج التي توصل إليها النموذج الهندسي المقترح، ثم تُقدّم توصيات إجرائية عملية على شكل خارطة طريق مرحلية، يليها استشراف لآفاق بحثية مستقبلية يمكن أن تُوسع نطاق التطبيق أو تُعمّق أبعاده النظرية والتقنية، ولقد حقّقت الدراسة الأهداف الأربعة التي رسمتها في مستهلها: فقد قدّمت إطاراً نظرياً متكاملاً لهندسة السيادة المالية السحابية، وصمّمت معمارية تقنية قائمة على ثلاث طبقات، وطبّقت هذا الإطار على النظام الادخاري الرقمي في البيئة الليبية، واختبرت كفاءته عبر مؤشرات كمية ونوعية، وانتهت إلى أن تبني السحابة المالية السيادية يُسهم في تحسين الأداء المالي وتعزيز الشفافية، مع تقديم توصيات إجرائية عملية قابلة للتنفيذ.

1. النتائج الأساسية

توصلت هذه الدراسة إلى مجموعة من النتائج الأساسية التي يمكن إيجازها على النحو التالي:

1. فيما يتعلق بالإطار المفاهيمي: أثبتت الدراسة أن مفهوم هندسة السيادة المالية السحابية يمثل نقلة نوعية في فهم العلاقة بين السيادة الرقمية والأنظمة المالية، حيث يتجاوز مجرد توطين البيانات ليشمل ثلاثة أبعاد متكاملة: السيادة القانونية (الامتثال والتشريع) والسيادة التشغيلية (الاستقلالية واستمرارية الأعمال) والسيادة التقنية (امتلاك الكوادر والمعايير الوطنية) كما بيّنت الدراسة أن التكامل بين هذه الأبعاد الثلاثة يُشكل الأساس المتين لأي نظام مالي رقمي سيادي في البيئات الانتقالية.
2. فيما يتعلق بالمعمارية الهندسية: قدّمت الدراسة نموذجاً هندسياً مبتكراً يقوم على ثلاث طبقات متكاملة: البنية التحتية السيادية (المعمارية الهجينة، التشفير المتعدد، بروتوكولات الربط التنظيمي، إثباتات المعرفة الصفرية، وإدارة الهوية) والخوارزميات الذاتية (الاستجابة اللحظية للصدمات، الاستهداف الآلي للاحتيال، والتعديل الذاتي للسياسات) والتدفقات التشغيلية (تحديد الأدوار، رسم خريطة التفاعل،

وضمن المساواة) كما أثبتت الدراسة أن دمج تقنية إثباتات المعرفة الصفريّة في النظام الادخاري يُحقق معادلة صعبة: الامتثال التنظيمي + الخصوصية المطلقة + السرعة اللحظية.

3. فيما يتعلق بآليات المنة والتكيف الذاتي: خلصت الدراسة إلى أن بناء نظام مالي مناعي ذاتي التكيف يتطلب ثلاث آليات متوازنة: التوقع (الكشف المبكر عن التهديدات) الاستجابة الذاتية (التكيف اللحظي مع الصدمات دون تدخل بشري) والتعلم المستمر (التطور المناعي من خلال تحليل الهجمات السابقة) وأن آلية التدخل البشري المشروط (نافذة الطوارئ) تُعد ضرورة حتمية لتجنب مخاطر التحكم الخوارزمي المطلق خاصة في الأزمات غير المبرمجة، مع اشتراط اتخاذ القرار بتمثيل جماعي وتوثيق رقمي مشفر ومدة زمنية محدودة.

4. أظهر تطبيق النموذج على البيئة الليبية في ضوء بيانات مصرف ليبيا المركزي (سبتمبر 2026) أن التحدي لم يعد في رفع نسبة استخدام المدفوعات الرقمية، بل في تأمين وحوكمة حجم هائل من التداولات بلغ 764.9 مليار دينار، تمر عبر 220,954 نقطة بيع و5.8 مليون بطاقة و45.9 مليون عملية تحويل فوري، وأن النموذج المقترح قادر على تحويل هذه البنية التحتية الضخمة من مجرد وسيلة دفع إلى نظام مالي سيادي مناعي، مع تقليص زمن التسوية إلى 3 ثوانٍ وضمن أمن 302 مليون عملية POS. 5. فيما يتعلق بتقييم الكفاءة المتوقعة: خلصت الدراسة إلى إمكانية تحقيق تحسينات ملموسة في ثلاثة أبعاد استراتيجية: الاستقرار النقدي (حماية المدخرات من التضخم بنسبة لا تقل عن 80%)، زيادة الودائع الادخارية بنسبة 25%، وتقليل تقلب المعاملات بنسبة 30% والشفافية المالية والرقابة (رفع الامتثال التنظيمي إلى 99%، تقليص زمن التدقيق من أسابيع إلى ساعات، وزيادة اكتشاف الاحتيال بنسبة 200%) وترسيخ الثقافة المالية الرقمية (رفع المعرفة المالية من 40% إلى 60%)، وتحقيق تفاعل 50% من المستخدمين مع أدوات التوعية).

2. التوصيات الإجرائية: خارطة طريق

انطلاقاً من النتائج التي خلصت إليها الدراسة تُقدّم التوصيات الإجرائية التالية على شكل خارطة طريق مرحلية، تستهدف صنّاع السياسات والمؤسسات المالية والجهات التنظيمية في الدول العربية الانتقالية وبخاصة في ليبيا:

المرحلة الأولى: التأسيس والتشريع (0-6 أشهر)

- إصدار تشريع وطني للسيادة المالية السحابية: يتضمن تعريفاً واضحاً لمفهوم السيادة الرقمية في القطاع المالي ويحدد آليات حماية البيانات وشروط توطيئها وعقوبات الاختراق، مع الاستناد إلى المعايير الدولية (كتوجيهات DORA الأوروبية) مع تكييفها مع السياق المحلي.
- إنشاء هيئة وطنية للسيادة المالية الرقمية: تكون مسؤولة عن الإشراف على تطبيق معايير السيادة وإصدار التراخيص لمزودي الخدمات السحابية وضمن الامتثال التنظيمي، مع تمثيل ثلاثي (البنك المركزي، هيئة الرقابة المالية، وخبراء تقنيون مستقلون).
- تقييم البنية التحتية الرقمية الحالية: إجراء تدقيق أمني شامل لـ 220,954 نقطة بيع و5.8 مليون بطاقة و8.2 مليون مشترك في التحويل الفوري، وتحديد الفجوات في الأمن السيبراني وسعات التخزين وقدرات المعالجة والشبكات، كخطوة تمهيدية لبناء السحابة الوطنية.
- تحديد الفجوات في أنظمة المقاصة الإلكترونية (1.6 مليون صك) وربطها بالنظام السيادي الجديد.

المرحلة الثانية: البناء والتطوير (6-12 شهراً)

- بناء السحابة الوطنية المالية الهجينة: اعتماد نموذج السحابة الهجينة الذي يجمع بين سحابة خاصة وطنية (للبائعات الحساسة) وسحابة عامة مُدارة (للعمليات الأقل حساسية) مع اشتراط تخزين البيانات داخل الحدود الجغرافية للدولة وتوفير خطط طوارئ محلية لضمان استمرارية الأعمال.
- بناء الخوارزميات القادرة على معالجة 45.9 مليون عملية تحويل فوري و302 مليون عملية POS بشكل لحظي.
- تطوير واجهات برمجة التطبيقات (APIs) للربط مع 220,954 نقطة بيع.

- تطوير الخوارزميات الذاتية التكيف: بناء وتدريب خوارزميات التعلم الآلي على البيانات التاريخية للأزمات المالية المحلية والإقليمية، مع تصميم نظام كشف الشذوذ القائم على التعلم العميق للتصدي للاحتيال، وتطوير آلية التعديل الذاتي للسياسات الادخارية استجابة للتغيرات الاقتصادية الكلية.
- تدريب الكوادر الوطنية ونقل المعرفة: إطلاق برامج تدريبية مكثفة للموارد البشرية المحلية (مهندسي برمجيات، مختصي أمن سيبراني، محلي بيانات) بالتعاون مع الجامعات ومراكز البحث الإقليمية، مع تصميم وثائق تقنية مبسطة باللغة العربية لضمان قابلية التشغيل والصيانة محلياً على المدى الطويل.

المرحلة الثالثة: التشغيل التجريبي والتقييم (12-18 شهراً)

- إطلاق النظام الادخاري الرقمي الذكي كمرحلة تجريبية: تطبيق النموذج على شريحة محدودة من المستخدمين (مثلاً: موظفو القطاع العام أو عملاء بنك واحد) بهدف اختبار كفاءة الخوارزميات، وسلاسة التدفقات التشغيلية، وفعالية آليات الأمن السيبراني، مع جمع التغذية الراجعة لتحسين الأداء.
- قياس مؤشرات الأداء الرئيسية: متابعة المؤشرات الكمية (نسبة المدفوعات الرقمية، زمن التسوية، حجم الودائع الادخارية، اكتشاف الاحتيال) والمؤشرات النوعية (مؤشر الثقة الرقمية، مؤشر المعرفة المالية، معدل التفاعل مع أدوات التوعية) بشكل دوري (شهري وربع سنوي) مع مقارنتها بالأهداف المرسومة وإجراء التعديلات اللازمة.
- يجب أن يكون التشغيل التجريبي على شريحة من المستخدمين تمثل 5.8 مليون بطاقة مفعلة، مع التركيز على 45.9 مليون عملية تحويل فوري كحالة اختبار حقيقية لضمان توسيع قاعدة الشمول المالي باستغلال تقنيات السجلات الموزعة والسحابة الوطنية (Parthiban et al., 2025).
- تفعيل آلية نافذة الطوارئ: تجربة آلية التدخل البشري المشروط في سيناريوهات محاكاة للأزمات (كالهجوم السيبراني أو التغير الاقتصادي المفاجئ) للتحقق من فعاليتها وسرعة استجابتها، وتوثيق الدروس المستفادة لتحديث البروتوكولات.

المرحلة الرابعة: التوسع والاستدامة (18-24 شهراً)

- التعميم على جميع المؤسسات المالية: توسيع النظام ليشمل جميع نقاط البيع (220,954) وجميع مشترك التحويل الفوري (8.2 مليون).
- إطلاق حملات وطنية للثقافة المالية الرقمية: تصميم وتنفيذ حملات توعية عبر وسائل التواصل الاجتماعي والإذاعة والتلفزيون والمنصات التعليمية، لتعزيز الوعي بأهمية الادخار الرقمي وأمان النظام السحابي السيادي، مع التعاون مع وزارة التربية والتعليم لإدراج مفاهيم الثقافة المالية في المناهج المدرسية.
- إنشاء منصة إقليمية لتبادل الخبرات: اقتراح إنشاء منصة عربية للتعاون في مجال السيادة المالية السحابية، تهدف إلى تبادل التجارب وتوحيد المعايير وتطوير الحلول التقنية المشتركة وتعزيز القدرات الجماعية للدول العربية في مواجهة التحديات السيبرانية والرقمية، على أن تكون ليبيا - بفضل ريادتها في هذا المجال - أحد الأعضاء المؤسسين لهذه المنصة.

3. آفاق الدراسات المستقبلية

- على الرغم من النتائج المهمة التي توصلت إليها هذه الدراسة إلا أنها تفتح آفاقاً بحثية واسعة يمكن للباحثين والممارسين استكشافها مستقبلاً ومن أبرزها:
- دراسة تأثير النمو الحاد في التداولات الإلكترونية على السياسة النقدية: مع وصول حجم التداول إلى 764.9 مليار دينار يصبح من الضروري دراسة كيف يمكن للبنك المركزي استخدام هذه البيانات الضخمة في رسم السياسة النقدية وتأثير ذلك على عرض النقود والتضخم.

- دراسة التطبيق العملي للنموذج في بيانات عربية أخرى: اختبار فعالية الإطار المقترح في دول عربية انتقالية أخرى (كالسودان، اليمن، تونس أو مصر) ذات ظروف اقتصادية وتنظيمية مختلفة بهدف تعميم النموذج وتطويره بما يتناسب مع خصوصية كل بيئة.
- تقنيات التشفير المتجانس: دراسة إمكانية تعميم استخدام التشفير المتجانس في النظام المالي السحابي، مع تحليل التحديات التقنية المرتبطة بالكفاءة الحسابية، والتكاليف التشغيلية وتقديم حلول مبتكرة لتجاوزها، مما يُعزز الخصوصية طوال دورة حياة المعاملة.
- دمج العملات الرقمية للبنوك المركزية: (CBDC) استكشاف كيفية تكامل النظام الادخاري الرقمي المقترح مع مشاريع العملات الرقمية للبنوك المركزية العربية، وتأثير ذلك على السياسات النقدية والسيولة المصرفية وسلوك الادخار الوطني.
- تطبيقات الذكاء الاصطناعي التوليدي: (Generative AI) دراسة استخدام نماذج الذكاء الاصطناعي التوليدي في تعزيز التوعية المالية، عبر تقديم توصيات ادخارية مخصصة وإنتاج محتوى توعوي تفاعلي ومحاكاة سيناريوهات مالية مستقبلية، مع تحليل المخاطر الأخلاقية والتشغيلية لهذه التقنيات.
- الأطر الأخلاقية للحوكمة الخوارزمية: وضع إطار أخلاقي شامل لحوكمة الخوارزميات في القطاع المالي يتضمن معايير العدالة، الشفافية، قابلية التفسير (Explainability) وآليات المساءلة لضمان أن القرارات الخوارزمية لا تُنتج تحيزاً أو تمييزاً ضد أي فئة من المواطنين، بما يتماشى مع مبادئ الشمول المالي والعدالة الاجتماعية.
- دراسة الجدوى الاقتصادية: إجراء تحليل كمي لتكلفة الفائدة (Cost-Benefit Analysis) لتطبيق النظام السحابي السيادي على المستوى الوطني، يشمل التكاليف الاستثمارية والتشغيلية مقابل العوائد المتوقعة من تحسين الكفاءة، تقليل الاحتيالات وزيادة الشمول المالي، لتوفير مبررات اقتصادية واضحة لصناع القرار.
- تحليل المخاطر السيبرانية الكمومية: مع التطور المتسارع في الحوسبة الكمومية، يصبح من الضروري دراسة تأثير هذه التقنيات على أمن التشفير في الأنظمة المالية السحابية، وتطوير استراتيجيات انتقالية نحو التشفير المقاوم للحوسبة الكمومية (Quantum-Safe Cryptography) لضمان استدامة الأمن السيبراني في العقود القادمة.
- تقييم أثر النموذج على الاستقرار المالي الكلي: دراسة تأثير تبني النظام السحابي السيادي على المؤشرات الكلية للاقتصاد الوطني كالتضخم ومعدلات الادخار الوطني والاستثمار والنمو الاقتصادي، باستخدام نماذج الاقتصاد القياسي الديناميكي لتوفير رؤية شاملة لتأثير التحول الرقمي على التنمية المستدامة.

بهذه الخاتمة تأمل الدراسة أن يكون هذا العمل مساهمة متواضعة في بناء منظومة مالية رقمية سيادية ومناعية، تُعزز المرونة الوطنية وتُرسّي دعائم الشمول المالي الآمن في العصر الرقمي.

قائمة المراجع

- [1] AWS & SAP. (2025, May). AWS-SAP launch €7.8bn sovereign cloud for EU finance. FinTech Magazine.
- [2] Bulgakova, E., Kubankov, A., Gudkova, K., & Bulgakov, V. (2025). Ensuring information security of Russian financial institutions: The concept of cyber immunity. Digital Law Journal.
- [3] Central Bank of Libya. (2025, December). CBL discusses with telecommunications companies the development of electronic payment services. Libyan News Agency (LANA).

- [4] Central Bank of Libya. (2026a, January). Governor of the Central Bank of Libya inaugurates the Libya international electronic payments exhibition (EPEX 2026). Central Bank of Libya Publications.
- [5] Central Bank of Libya. (2026b, September). Statement of revenue and expenditure for August 2026. Central Bank of Libya.
- [6] Desai, S. (2025). Agentic AI frameworks: Building autonomous, self-healing systems for financial infrastructure. *International Journal of Computational and Experimental Science and Engineering*, 11(4).
- [7] European Banking Authority. (2025). Digital Operational Resilience Act (DORA) – Regulatory technical standards. European Union.
- [8] Gartner. (2025). Magic quadrant for cloud financial management tools. Gartner Research.
- [9] Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220–265.
- [10] IBM. (2025). What is cloud financial management? IBM Think.
- [11] International Monetary Fund. (2025). Digital financial services and financial inclusion in fragile states (IMF Working Paper). International Monetary Fund.
- [12] O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
- [13] Parthiban, U., Pannerselvam, V. D., Murugesan, A., & Ramasamy, K. (2025). ShePowerChain: A blockchain-based platform for women's financial inclusion and empowerment. *Asian Women*, 41(3), 82–97.
- [14] Perdana, A., Arifin, S., & Quadrianto, N. (2025). Algorithmic trust and regulation: Governance, ethics, legal, and social implications blueprint for Indonesia's central banking. *Futures*, 158, Article 103456.
- [15] Pinheiro, M. R., & Pinheiro, M. J. (2025). Money as a tensor (arXiv Preprint arXiv:2504.06286). arXiv.
- [16] Reply. (2025). AI & sovereign cloud: Innovation and compliance for regulated industries. Reply Networks.
- [17] Salaam Gateway. (2026, January). UAE's sovereign financial cloud aims to safeguard more than just data. Global Islamic Economy Gateway.
- [18] Springer. (2025). Cybersecurity in the financial sector and the quantum-safe cryptography transition. *International Cybersecurity Law Review*, 6, 145–154.
- [19] World Bank. (2024). Financial inclusion and digital payments in the Middle East and North Africa (World Bank Group Report). The World Bank.
- [20] zkVerify. (2025, February). Advancing privacy-preserving lending through scalable ZK proof verification. zkVerify Blog.
- [21] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **JSHD** and/or the editor(s). **JSHD** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.