International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
IJFAES
Vol. (5), No. (9) September 2026 الإصدار (5)، العدد (9)

التوقيع الإلكتروني كمدخل لتعزيز الأمن السيبراني وتطوير الأداء المصرفي

مروه عبدالرحمن عبدالله
م.م، قسم الإدارة العامة، كلية الإدارة والاقتصاد، جامعة بغداد، العراق
ORCID: https://orcid.org/0009-0006-1177-453X
marwah@coadec.uobaghdad.edu.iq

زيد عائد مردان
م.د، وزارة النفط، العراق
Zaid.aed@jisu.edu.iq

آلاء حسين هادي
م.م، ماجستير مالية مصرفية، جامعة الكوفة، العراق
alaa.hussain9093@gmial.com

المستخلص

يشهد القطاع المصرفي تحولات رقمية متسارعة جعلت من الاعتماد على الوسائل الإلكترونية في تقديم الخدمات المالية خيارًا استراتيجيًا لا غنى عنه، غير أن هذا التحول ترافق مع تحديات أمنية متزايدة مثل محاولات الاختراق، تزوير المعاملات، وانتهاك سرية البيانات، وهو ما قد يضعف ثقة العملاء بالمنظومة المصرفية. ومن هنا تبرز أهمية التوقيع الإلكتروني كأداة تقنية فاعلة لمعالجة هذه التحديات عبر ما يوفره من ضمانات التوثيق والمصداقية وعدم الإنكار في المعاملات، إلا أن محدودية تطبيقه في المصارف المحلية وضعف الوعي بأبعاده القانونية والفنية يشكلان إشكالية تستوجب البحث والدراسة.

تهدف الدراسة إلى تحليل مفهوم التوقيع الإلكتروني وأبعاده التقنية والقانونية في السياق المصرفي، وتوضيح دوره في تعزيز الأمن السيبراني وحماية البيانات والمعاملات، وبيان أثره في تطوير الأداء المصرفي من خلال الكفاءة والسرعة والموثوقية، فضلًا عن اقتراح آليات عملية لتبنيه وفق المعايير الدولية وبما يتناسب مع البيئة المصرفية العراقية. وقد اعتمدت الدراسة المنهج الوصفي التحليلي مدعومًا بالمنهج الاستقرائي من خلال تحليل التشريعات والتجارب الدولية الناجحة، كما اختبرت ثلاث فرضيات رئيسية تتعلق بوجود علاقة ارتباط بين التوقيع الإلكتروني والأداء المصرفي، وبين الأمن السيبراني والأداء المصرفي، فضلًا عن العلاقة بين التوقيع الإلكتروني والأمن السيبراني في تحسين الأداء المصرفي.

توصلت الدراسة إلى مجموعة من الاستنتاجات أبرزها: أن التوقيع الإلكتروني يسهم بفاعلية في تعزيز الثقة بالمعاملات المصرفية عبر ضمان التوثيق والمصداقية وعدم الإنكار، وأن الأمن السيبراني يمثل عنصرًا تكامليًا معه في حماية البنية التحتية المصرفية ضد الاختراقات والتزوير، فيما يشكل ضعف البنية التشريعية والتنظيمية في البيئة المحلية أحد أبرز معوقات التبني الفاعل لهذه التقنية. كما أظهرت النتائج أن المصارف التي تبنّت تطبيقات جزئية للتوقيع الإلكتروني حققت تحسنًا ملموسًا في كفاءة الخدمات وسرعة إنجاز المعاملات.

وانطلاقًا من هذه النتائج، أوصت الدراسة بضرورة إصدار تشريعات متكاملة تنظم استخدام التوقيع الإلكتروني وتحدد أبعاده القانونية لحماية جميع الأطراف، وتعزيز البنية التحتية للأمن السيبراني في المصارف، ونشر الوعي القانوني والتقني لدى العاملين والعملاء، إلى جانب الاستفادة من التجارب الدولية الناجحة وتكييفها مع البيئة العراقية، وتشجيع المصارف على الاستثمار في الأنظمة الرقمية الحديثة وربط التوقيع الإلكتروني بخطط التحول الرقمي الشامل.

الكلمات المفتاحية: التوقيع الإلكتروني، الأمن السيبراني، الأداء المصرفي.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
IJFAES
Vol. (5), No. (9) September 2026 الإصدار (5)، العدد (9)

Electronic Signature as an Approach to Enhancing Cybersecurity and Developing Banking Performance

Marwah Abdulrahman Abdullah
Department of Public Administration, College of Administration and Economics, University of Baghdad, Iraq
ORCID: https://orcid.org/0009-0006-1177-453X
marwah@coadec.uobaghdad.edu.iq

Zaid Aed Mardan
Ministry of Oil, Iraq
Zaid.aed@jisu.edu.iq

Alaa Hussain Hadi
Master's in Banking and Finance, University of Kufa, Iraq
alaa.hussain9093@gmail.com

Abstract

The banking sector is undergoing rapid digital transformation, making reliance on electronic means for delivering financial services an indispensable strategic choice. However, this shift has been accompanied by mounting security challenges—such as hacking attempts, transaction fraud, and breaches of data confidentiality—that threaten to undermine customer confidence in the banking system. Consequently, the electronic signature emerges as a vital technical tool for addressing these challenges by providing guarantees of authentication, credibility, and non-repudiation in transactions. Yet, its limited adoption by local banks and a lack of awareness regarding its legal and technical dimensions constitute an issue requiring further study.

This study aims to analyze the concept of electronic signatures and their technical and legal dimensions within the banking context. It seeks to clarify their role in enhancing cybersecurity and protecting data and transactions, as well as their impact on improving banking performance through increased efficiency, speed, and reliability. Furthermore, the study proposes practical mechanisms for adopting electronic signatures in alignment with international standards and the specificities of the Iraqi banking environment. The research employs a descriptive-analytical approach, supplemented by an inductive method involving the analysis of legislation and successful international experiences. It also tests three main hypotheses concerning the correlations between electronic signatures and banking performance, cybersecurity and banking performance, and the combined role of electronic signatures and cybersecurity in enhancing banking performance. The study reached several key conclusions: electronic signatures effectively foster trust in banking transactions by ensuring authentication, credibility, and non-repudiation; cybersecurity acts as a complementary element in protecting banking infrastructure against breaches and fraud; and weaknesses in the local legislative and regulatory framework constitute a major obstacle to the effective adoption of this technology. Furthermore, the results indicated that banks implementing partial electronic signature solutions achieved tangible improvements in service efficiency and transaction processing speed.

Based on these findings, the study recommends enacting comprehensive legislation to regulate the use of electronic signatures and define their legal parameters to protect all parties; strengthening banking cybersecurity infrastructure; raising legal and technical awareness among staff and customers; leveraging successful international experiences and adapting them to the Iraqi context; and encouraging banks to invest in modern digital systems and integrate electronic signatures into comprehensive digital transformation plans.

Keywords: Electronic Signature, Cybersecurity, Banking Performance.

المقدمة

يشهد القطاع المصرفي في العصر الرقمي تحولات نوعية متسارعة، فرضتها التطورات التكنولوجية والتحول نحو الخدمات المالية الإلكترونية. وقد أصبحت هذه التحولات ضرورة استراتيجية لا غنى عنها، حيث تسهم في رفع كفاءة العمليات المصرفية، تحسين تجربة العملاء، وتوسيع نطاق الخدمات المالية المقدمة بسرعة ودقة أكبر، بما يعزز القدرة التنافسية للمؤسسات المصرفية في بيئات العمل المحلية والعالمية. غير أن هذا التحول الرقمي المصاحب لتطور الخدمات المصرفية لم يأتِ بدون تحديات جوهرية، إذ يرافقه تصاعد في المخاطر الأمنية مثل محاولات الاختراق، تزوير المعاملات، وانتهاك سرية البيانات، وهو ما يهدد ثقة العملاء بالأنظمة المصرفية ويعرض المؤسسات لمخاطر مالية وتشغيلية كبيرة. في هذا السياق، برز التوقيع الإلكتروني كأحد الحلول التقنية الفعّالة لمواجهة هذه التحديات، لما يوفره من ضمانات للتوثيق والمصداقية وعدم الإنكار في المعاملات الرقمية، إضافة إلى دوره في تعزيز الشفافية وتقليل مخاطر التلاعب بالبيانات.

مع ذلك، فإن تبني التوقيع الإلكتروني في البيئة المصرفية المحلية لا يزال محدودًا، ويرجع ذلك إلى ضعف الوعي القانوني والفني لدى العاملين والعملاء، فضلاً عن قصور البنية التشريعية والتنظيمية التي تحدد إطار استخدامه. وهذا يبرز الحاجة إلى دراسة معمقة لدور التوقيع الإلكتروني كمدخل لتعزيز الأمن السيبراني وتطوير الأداء المصرفي، مع التركيز على كيفية التوافق بين الأمان الرقمي وكفاءة العمليات المصرفية.

تكتسب هذه الدراسة أهميتها من كونها تسلط الضوء على العلاقة التكاملية بين التوقيع الإلكتروني والأمن السيبراني، حيث يمثل دمج هذين المتغيرين أداة فعّالة لتحسين جودة الخدمات المصرفية وحماية البنية التحتية الرقمية. كما تهدف إلى تقديم إطار علمي وتطبيقي يمكّن المصارف من اعتماد التوقيع الإلكتروني وفق المعايير الدولية، بما يسهم في تعزيز ثقة العملاء وضمان موثوقية المعاملات الرقمية. من الناحية النظرية، تسهم الدراسة في إثراء الأدبيات العلمية حول التوقيع الإلكتروني ودوره في حماية الأنظمة المصرفية من المخاطر الرقمية والهجمات السيبرانية، بينما يتمثل الجانب العملي في تقديم دليل استرشادي يوضح كيفية تبني هذه التقنية في المصارف المحلية لتحقيق الفائدة القصوى. كما تدعم الدراسة التوجهات الاستراتيجية للتحول الرقمي والابتكار في القطاع المصرفي، وتعزز التنافسية في الأسواق المالية.

تتناول الدراسة موضوعها من خلال تحليل شامل لمفهوم التوقيع الإلكتروني وأبعاده التقنية والقانونية، واستعراض دوره في تعزيز الأمن السيبراني وحماية البيانات والمعاملات، إضافة إلى بيان أثره في تحسين الأداء المصرفي من حيث الكفاءة والسرعة والموثوقية. كما تستفيد من التجارب الدولية الناجحة في تطبيق التوقيع الإلكتروني، مع استخدام المنهج الوصفي التحليلي مدعومًا بالمنهج الاستقرائي لبناء إطار نظري وتطبيقي قادر على الاستجابة لمتطلبات البيئة المصرفية العراقية.

مراجعة الأدبيات: منهجية الدراسة

أولاً: مشكلة الدراسة:

يشهد القطاع المصرفي تحولات رقمية متسارعة جعلت من الاعتماد على الوسائل الإلكترونية في تقديم الخدمات المالية خيارًا استراتيجيًا لا يمكن الاستغناء عنه. غير أن هذا التوجه يرافقه تصاعد في التحديات الأمنية، التي تتمثل في محاولات الاختراق، تزوير المعاملات، وانتهاك سرية البيانات، وهي مشكلات من شأنها إضعاف ثقة العملاء بالمنظومة المصرفية. وفي هذا السياق، يبرز التوقيع الإلكتروني كأحد الحلول التقنية الفعّالة لمواجهة هذه التحديات، لما يوفره من ضمانات تتعلق بالتوثيق، المصداقية، وعدم الإنكار في المعاملات الإلكترونية. إلا أن محدودية تطبيقه بالشكل الأمثل في المصارف المحلية، إلى جانب

ضعف الوعي بجوانبه القانونية والفنية، يطرح إشكالية تستدعي دراسة معمقة لدور التوقيع الإلكتروني كمدخل لتعزيز الأمن السيبراني وتطوير الأداء المصرفي.

ثانياً: أهمية الدراسة:

تتجلى أهمية الدراسة في النقاط التالية:

1. يساهم في إثراء الأدبيات العلمية المتعلقة بالتوقيع الإلكتروني وأثره في تعزيز الأمن السيبراني داخل المؤسسات المصرفية، بما يسد فجوة معرفية قائمة في هذا المجال.
2. يوفّر إطارًا عمليًا يساعد المصارف على تبني التوقيع الإلكتروني كأداة لضمان موثوقية المعاملات وتعزيز مستوى الأمان.
3. يعزز ثقة العملاء بالخدمات المصرفية الرقمية، ويدعم مسارات التحول الرقمي والابتكار في القطاع المالي.
4. يقلل من مخاطر الاحتيال والخسائر الناجمة عن الاختراقات والتلاعب بالبيانات، مما يسهم في رفع كفاءة الأداء المالي للمصارف.

ثالثاً: أهداف الدراسة:

في ضوء ما سبق، تهدف الدراسة إلى تحقيق ما يلي:

1. تحليل مفهوم التوقيع الإلكتروني واستعراض أبعاده التقنية والقانونية في السياق المصرفي.
2. توضيح دور التوقيع الإلكتروني في تعزيز الأمن السيبراني وحماية المعاملات من التلاعب أو الانتحال.
3. بيان أثر التوقيع الإلكتروني في تطوير الأداء المصرفي من خلال تحسين الكفاءة، تسريع إنجاز المعاملات، وزيادة موثوقية الخدمات.
4. اقتراح آليات عملية وتوصيات لتبني التوقيع الإلكتروني في المصارف بما يتوافق مع المعايير الدولية للأمن السيبراني.

رابعاً: فرضيات الدراسة:

في ضوء تحديد مشكلة الدراسة وأهميتها وأهدافها، تختبر الدراسة الحالية الفرضيات الآتية:

- الفرضية الأولى: للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.
- الفرضية الثانية: للأمن السيبراني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.
- الفرضية الثالثة: للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي.

المبحث الثاني: الإطار النظري للدراسة

أولاً: التوقيع الإلكتروني:

1. مفهوم التوقيع الإلكتروني (المفهوم والتعريف):

يُعد التوقيع الالكتروني أحد نتائج تطور التكنولوجيا واتساع نطاق المعاملات القانونية. ويُعدّ التوقيع الإلكتروني نتيجة حتمية لدخول تكنولوجيا المعلومات في مجال المعاملات القانونية والتسجيلية. (Pourteymour & Shams, 2024: 85)

التوقيع هو علامة شخصية مكتوبة بخط اليد على الوثيقة تشير إلى موافقته على محتواها، بالإضافة إلى ذلك، يسمح التوقيع بتحديد هوية المُوقّع، في عالم الإنترنت، تخدم التوقيعات الرقمية نفس غرض نظيراتها التقليدية (Karonen, 2025: 9)

التوقيع الإلكتروني هو نهج رياضي يُثبت صحة وسلامة الرسالة أو البرنامج أو المستند الرقمي. وهو المعادل الرقمي للتوقيع اليدوي أو الختم المختوم (Djouadi, 2024: 5).

تضمن خوارزميات التوقيع الإلكتروني صحة المستندات الرقمية وسلامتها وعدم إنكارها، ومن خلال استخدام أساليب التشفير لإنشاء التوقيعات والتحقق منها، تُسهّل هذه الخوارزميات تبادل المستندات الرقمية وتوقيعها بشكل آمن عبر منصات متنوعة، كما توفر ميزات فريدة ومميزة، مما يضمن اتصالات رقمية آمنة وفعالة. (Stanešić et al., 2025: 406)

بالنسبة للجانب المالي لهذه المشكلة، حيث تنتقل المعاملات المالية بشكل متزايد إلى المنصات الرقمية، يواجه القطاع المصرفي، على وجه الخصوص، تحدي تأمين التوقيعات الرقمية ضد محاولات التزوير المعقدة. يُعدّ تنفيذ وتطبيق أنظمة قوية للتحقق من التوقيعات أمرًا ضروريًا لحماية سلامة المعاملات المالية، ومنع سرقة الهوية، وضمان موثوقية المستندات الرقمية (Christianto et al., 2024: 267).

تُصنف التوقيعات الرقمية على النحو التالي (Ege et al., 2025: 2):

- التوقيع الإلكتروني البسيط (SES): طرق تحقق أساسية مرتبطة بالمستندات الرقمية (مثل التوقيعات الممسوحة ضوئيًا، وتأكيدات البريد الرقمي).
- التوقيع الإلكتروني المتقدم (AES): توقيع مرتبط بشكل فريد بالموقّع، مما يضمن التحقق من الهوية وسلامة المستند.
- التوقيع الإلكتروني المؤهل (QES): أعلى توقيع إلكتروني معترف به قانونًا، صادر عن مزود خدمة موثوق (TSP) بناءً على شهادات مؤهلة.

2. خصائص التوقيع الإلكتروني:

هناك عدة تعريفات لخصائص التوقيع الإلكتروني، ومنها (Liu et al., 2024: 18):

- عدم قابلية التزوير (Unforgeability): لا يمكن لأي شخص، باستثناء المشاركين المحددين (الموقّع بالوكالة، عضو المجموعة)، إنشاء توقيع صالح.
- إمكانية التحقق (Verifiability): يمكن للمتحقق التحقق من توقيع الوكيل باستخدام مفتاح التحقق الخاص بموقّع الوكيل. ويمكنه معرفة ما إذا كان توقيع الوكيل مقبولًا من قِبل الموقّع الأصلي.
- عدم التنصل (Nonrepudiation): لا يمكن لموقّع الوكيل رفض توقيع الوكيل الصالح الذي وقّعه.
- إمكانية التمييز(Distinguishability): يجب أن يكون توقيع الوكيل قابلاً للتمييز عن التوقيع العادي.
- عدم قابلية التأطير(Non-frameability): لا يمكن للمهاجم إنشاء التوقيع الذي يستخدمه فاتح التوقيع من توقيع صالح للكشف عن هوية عضو صادق في مجموعة التوقيع.
- سلامة التتبع (Tracing soundness): يكشف فاتح التوقيع عن مُوقّع التوقيع، ولا يمكن للمهاجم إنشاء توقيع ينتمي إلى عضوين مختلفين في المجموعة.
- إمكانية التعرف (Identifiability): يمكن لأي شخص التعرف على المُوقّع بالوكالة من المغني الأصلي من خلال توقيع بالوكالة.
- إمكانية الربط (Linkability): إمكانية التحقق بشكل مجهول مما إذا كان قد تم توقيع توقيعين من قِبل نفس المُوقّع، وهذا أحد أكثر تطبيقات توقيعات الحلقات استخدامًا.

3. عملية إنشاء التوقيع الإلكتروني:

تُعد التوقيعات الرقمية حلاً تكنولوجيًا يتيح التحقق من هوية المُوقّع ويضمن سلامة المستندات الرقمية وصحتها، باستخدام التوقيع الإلكتروني، يُمكن تحديد هوية المستخدم، وتأكيد عملية توقيع المستند، وحمايته من التغييرات بعد توقيعه، أحد الجوانب

الرئيسية للتوقيع الرقمي هو أساسه التشفيري، الذي يوفر مستوى عالٍ من الأمان ويلعب دورًا حيويًا في الحماية من الاحتيال والتزوير، والشكل (1) يوضح عملية إنشاء التوقيع الإلكتروني. (Oleksiv & Nazarkevych, 2025: 41)

شكل (1): عملية إنشاء التوقيع الإلكتروني (المصدر: من إعداد الباحثين بالاعتماد على المصادر الواردة أعلاه)

4. أبعاد التوقيع الإلكتروني:

لفهم دور التوقيع الإلكتروني بشكل شامل، من المهم استعراض أبعاده الرئيسية التي تحدد فعاليته في المعاملات الإلكترونية. هذه الأبعاد توضح الجوانب التقنية، القانونية، والأمنية التي تساهم في تعزيز الموثوقية، حماية البيانات، وضمان سلامة العمليات الرقمية. ويمكن توضيحها كما يأتي:

أ. الإطار القانوني Legal Framework: يُوفر الإطار القانوني للمعاملات الرقمية الأساس، مُرسيًا الشروط التي تُعترف بموجبها بالتوقيعات الرقمية على أنها مُلزمة قانونًا، بدون هذا الأساس القانوني، حتى أكثر التوقيعات الرقمية أماناً لا يُمكنها سوى توفير ضمان فني دون القدرة على الإنفاذ القانوني اللازم في المعاملات التجارية والحكومية، ينبغي أن تكون الأطر القانونية للممارسات الجيدة محايدة من الناحية التكنولوجية، وتعترف بالتوقيعات الرقمية بأنواعها، وذلك في إطار نهج قائم على المخاطر، مما يسمح بحجز التوقيعات للتطبيقات عالية المخاطر (Tullis, 2024: 16). ويشمل الإطار القانوني:

- الإطار القانوني الوطني: يشمل الإطار القانوني مجموعة القوانين واللوائح التي تحكم المعاملات الإلكترونية والتواقيع الإلكترونية. ويحدد هذا الإطار الصلاحية القانونية وقابلية التنفيذ لإطار الثقة، ويوضح الآثار القانونية، وخاصة الشروط التي تعتبر بموجبها التواقيع الإلكترونية مكافئة للتواقيع اليدوية.
- إطار الاعتراف المتبادل: لضمان أساس مشترك للثقة والاعتراف المتبادل عبر الحدود وقابلية التشغيل البيني للتواقيع الإلكترونية، يمكن تنسيق الأطر القانونية وأطر الثقة على المستوى الدولي، مما يوسع نطاق الثقة عبر الدول (Tullis, 2024: 16).

ب. إطار الثقة (Trust Framework): إطار الثقة هو الهيكل التنظيمي الذي يحدد الحد الأدنى من المتطلبات للعناصر البشرية والعملياتية والتقنية المتعلقة بالتوقيع الإلكتروني، ويهدف إلى توفير أدلة موثوقة على مصداقية التوقيع الإلكتروني. يعمل

إطار الثقة على تعزيز الثقة من خلال المعايير والشفافية، ويشمل غالبًا مستويات متعددة للضمان (Levels of Assurance) تسمح بمطابقة قوة التوقيع مع مستوى المخاطر المرتبط بالمعاملة.

- متطلبات الأدلة والضمانات: يتم بعد ذلك تشكيل مصادر الثقة وتوسيعها من خلال إطار الثقة، الذي يحدد الحد الأدنى من المتطلبات للعناصر البشرية والعملياتية والتقنية المتعلقة بالتوقيع، والتي توفر أدلة على موثوقيته. يعمل إطار الثقة على تمديد الثقة من خلال المعايير والشفافية.
- مستويات الضمان (Levels of Assurance): قد يشمل إطار الثقة أيضًا مستويات متعددة من الضمان أو مستويات الثقة. تساعد هذه المتطلبات المتدرجة على دعم احتياجات المعاملات ذات مستويات المخاطر المختلفة، مما يسمح بمطابقة توقيع ذي قوة مناسبة مع المعاملة التي تتوافق مع مستوى المخاطر الخاص بها.

ت. مصادر الثقة (Sources of Trust): هي العناصر الأساسية التي تُبنى عليها الثقة في التوقيع الإلكتروني، وتشمل جميع العوامل البشرية والتقنية والإجرائية التي تتيح التحقق من مصداقية التوقيع الإلكتروني.

- الثقة السابقة القائمة: (Pre-existing Trust) يمكن أن تنشأ الثقة من مصادر موجودة مسبقًا، مثل الأطراف التي تعرف بعضها البعض بالفعل، بالإضافة إلى مصادر الثقة السياقية، مثل وجود قناة اتصال آمنة.
- أدلة الموثوقية: (Evidence of Reliability) يمكن توسيع مصادر الثقة القائمة باستخدام تقنيات مختلفة تشمل العناصر البشرية والعملياتية والتقنية لتقديم أدلة على موثوقية التوقيع بما يتجاوز ما يمكن تحقيقه بالاعتماد فقط على الثقة السابقة القائمة. والشكل الآتي بوضح أبعاد التوقيع الإلكتروني.

شكل (2): أبعاد التوقيع الإلكتروني (المصدر: من إعداد الباحثين بالاعتماد على المصادر الواردة أعلاه)

ثانياً: الأمن السيبراني:

1. مفهوم الأمن السيبراني:

حدد إطار (NIST) الأمن السيبراني بأنه عملية حماية المعلومات من خلال اكتشاف ومنع والرد على الهجمات السيبرانية. وتتمثل حوادث الأمن السيبراني بفشل نظم المعلومات واختراق البيانات وما يترتب عليها من خسائر فادحة في بيانات الوحدة الاقتصادية وممتلكاتها وأضراراً كبيرة بسمعتها وبنيتها الرئيسية (NIST، 2014: 112). وفي السياق ذاته، أوضح (Alina) أن الأمن السيبراني هو النشاط الذي يؤمن حماية الموارد المالية والبشرية ذات العلاقة بتقنيات المعلومات والاتصالات وإمكانية الحد من الأضرار والخسائر التي تترتب في حال تحقق التهديدات والمخاطر كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتحول الأضرار إلى خسائر مادية ولا تتوقف عجلة الإنتاج (Alina et al., 2017: 510-513)، وهو ما يعكس بُعدًا عمليًا يرتبط باستمرارية الأعمال.

أما جيجان فقد ركز على الجانب الاحترازي معرفًا الأمن السيبراني بأنه مجموعة الإجراءات الاحترازية التي يتعين اتخاذها من قبل الأجهزة الأمنية والمؤسسات الأخرى للمحافظة على سرية المعلومات الرقمية ومنع الاختراقات الفايروسية... (جيجان، 2021: 36). بينما عرف (Krishnasamy & Venkatachalam, 2021: 144). نطاق المفهوم ليشمل تقنيات متقدمة مثل التشفير القائم على الأنماط، مؤكدين دوره في أمن تدفق البيانات السحابية وتقليل تكاليف التخزين.

وتطور المفهوم لاحقًا عند (Salin & Lundgren, 2022: 276-291) حيث أشارا إلى أن الأمن السيبراني هو حماية الموجودات الرقمية من المخاطر الموجودة نتيجة استعمال الاتصالات وتكنولوجيا المعلومات التي تشكل أساس الفضاء الرقمي، وهو تعريف يبرز بوضوح علاقة الأمن السيبراني بالبنية التحتية الرقمية الحديثة.

2. أبعاد أمن السيبراني:

الأمن السيبراني يتضمن عدة أبعاد لحماية المعلومات والأنظمة من التهديدات. أبرز هذه الأبعاد: (Ofoegb & Osundare, 2024: 6)

أ. أمن التطبيقات: يركز على حماية البرمجيات والتطبيقات من الثغرات الأمنية، مثل هجمات حقن.SQL يشمل التشفير واختبارات الأمان وتحديث البرمجيات دورياً لتعزيز الحماية. (Han et al., 2021:3197)

تجدر الإشارة إلى أن بعض الدراسات قد ذكرت بأن أمن التطبيقات هو مصطلح أخر للأمن السيبراني أي أنهما مترادفان، ولكن الحقيقة أنه لا يعد مرادفاً له فإن الأمن السيبراني يتجاوز أمن المعلومات في نطاقه ومجاله، ففي حين تركز حوادث أمن المعلومات على خروقات السرية أو السلامة أو التوفر، فإن الأمن السيبراني يشمل تلك الجوانب ويضيف إليها تهديدات لا تقع ضمن التعريف التقليدي لأمن المعلومات، ويُعد السبب الجوهري للثغرات في الأمن السيبراني هو الاعتماد على تكنولوجيا المعلومات والاتصالات، ما يجعل جميع الأصول سواء كانت معلومات أو بنى تحتية أو حتى مصالح وطنية معرضة للخطر وتحتاج إلى الحماية، ولذلك، فإن الميزة الأبرز للأمن السيبراني تكمن في شموليته وارتباطه الوثيق بالتقنيات الرقمية التي تشكل الفضاء السيبراني. (الدعمي، 2025: 78)

ب. أمن السحابي: يضمن حماية البيانات والتطبيقات التي تعتمد على الخدمات السحابية مثل AWS. Google Cloud يشمل استخدام تقنيات التشفير والمراقبة المستمرة للكشف عن الأنشطة غير العادية (Chandra, 2019 :2072).

فالأمن السحابي هو مجموعة من السياسات والتقنيات والممارسات المصممة لحماية البيانات والتطبيقات والبنية التحتية المخزنة على الحوسبة السحابية، ويهدف إلى تأمين الأنظمة السحابية ضد التهديدات السيبرانية مثل الاختراقات، وسرقة البيانات، والهجمات الإلكترونية، وضمان الامتثال للمعايير الأمنية ومع تزايد الاعتماد على الخدمات السحابية في المؤسسات والأفراد، أصبحت الحاجة إلى أمن سحابي قوي ضرورة لضمان حماية البيانات الحساسة من الوصول غير المصرح به، ومكافحة الهجمات الإلكترونية مثل البرمجيات الخبيثة والتصيد الاحتيالي، والامتثال للقوانين وضمان استمرارية الأعمال من خلال أنظمة النسخ الاحتياطي واستعادة البيانات بعد الأمن السحابي عنصرًا أساسيًا لحماية البيانات والتطبيقات المخزنة على السحابة، وأصبح من الضروري تطبيق استراتيجيات أمان قوية لضمان سرية وسلامة المعلومات الهيئة الوطنية للأمن السيبراني.

ت. أمن التشغيلي: يركز على حماية البيانات أثناء العمليات النظامية، من خلال سياسات الوصول وإدارة الهوية للتحكم في النظام (Salem & Mijwil 2023:9).

يمثل الأمن التشغيلي عنصراً أساسياً في الاستراتيجية الشاملة للأمن السيبراني، إذ يهدف إلى تحديد وتنفيذ الإجراءات اللازمة للحد من الوصول غير المصرح به أو القضاء عليه، ويشمل ذلك مراقبة الأنظمة بشكل مستمر، وإدارة الثغرات الأمنية، وتطبيق بروتوكولات الحماية لضمان سرية البيانات وسلامتها، كما يتضمن الأمن التشغيلي استخدام أدوات متقدمة لاكتشاف التهديدات والاستجابة لها، مما يعزز من قدرة المؤسسات على التصدي للهجمات الإلكترونية وتقليل المخاطر التشغيلية التي قد تؤثر على استمرارية الأعمال (المطيري والسدراني 2024:477) فالأمن التشغيلي هو آلية لحماية أنظمة التقنيات التشغيلية بكل أشكالها وما تحتويه من بيانات والتصدي للهجمات الإلكترونية إذ أن من أهم مهامه توفير بيئة آمنة يثق بها العملاء وحماية البنية التحتية من الهجمات من الهجمات الإلكترونية، كما يساعد على حماية الاستثمارات في

الأنظمة الخاصة بالمؤسسات إذ إنّ التهديدات تهدف إلى تعطيل عمليات النظام وهو ما يكون له عواقب وخيمة (مرسي، 4370:2024).

شكل (3): أبعاد الأمن السيبراني (المصدر: من إعداد الباحثين بالاعتماد على المصادر الواردة أعلاه)

3. أنواع هجمات الأمن السيبراني:

يتعامل الأمن السيبراني مع مستويات مختلفة من الخطر ومنها الآتي: (Shruti M, 2024: 1)

- برامج الفنية الضارة: هي نوع من البرامج الضارة التي تصيب أجهزة الكومبيوتر مثلاً، دخول هذا البرنامج إلى الجهاز يقوم بتشفير الملفات ويصبح من غير الممكن الوصول إليها، لتطالب بغدية مقابل فك التشفير.
- البرامج الضارة تشير إلى أشكال مختلفة من البرامج التي تغير طريقة عمل الأجهزة، ومجرد تثبيتها، تؤدي مهاماً دون علم أو موافقة مستخدمي أجهزة الكمبيوتر أو الهاتف، وذلك للوصول إلى تلك الأجهزة وسرقة البيانات والمعلومات الأخرى بهدف الابتزاز وسرقة الأموال.
- حصان طروادة: وهو اسم لأكثر البرامج الضارة التي تؤدي إلى خسائر كبيرة مثل سرقة الحسابات المصرفية كونه غير واضح ومن الصعب اكتشافه من قبل المستخدم العادي، إذ يدخل إلى الأنظمة من خلال وسائل يفترض أنها مشروعة.
- التصعيد الاحتيالي: وهو من أشهر الأساليب الهجوم السيبراني حيث يتم من خلالها إرسال رسائل عبر البريد الإلكتروني، أو رسائل نصية لخداع المستخدمين للنقر فوق رابط معين أو تنزيل برامج ضارة أو تحويلهم أو نقلهم على مواقع سيئة.
- التحايل بالهندسة الاجتماعية: يمثل شكل من أشكال الهندسة الاجتماعية، يتم من خلالها الحصول على بيانات المستخدمين عبر الاستدراج من خلال عدد من الخطوات التي قد تؤدي إلى دفع نقدي أو الوصول إلى البيانات السرية عن طريق النقر أيضاً على روابط أو تنزيل برامج ضارة.
- هجوم التوائم يقوم على أساس إنشاء نقاط اتصال غير حقيقية من شبكة الواي فاي الأصلية ولكنها تعمل على التنصت على الاتصالات والحصول على معلومات سرية مثل كلمة المرور واسم المرور خاصة بالمستخدمين.
- هجوم حجب الخدمة: يعمل هجوم حجب الخدمة (DoS) على منع المستخدمين من الدخول إلى الموقع الإلكتروني، مما يسبب ضررًا كبيرًا، ويتم ذلك عن طريق توجيه كميات كبيرة من حركة مرور الإنترنت إلى خادم الويب حتى يتم شغلها بالكامل ليمنع المستخدمين الحقيقيين من الدخول.

ثالثاً: الأداء المصرفي:

1. مفهوم الأداء المصرفي:

يمثل الأداء المصرفي أحد الركائز الأساسية لنجاح المصارف التجارية، إذ يختلف مستوى الخدمات المصرفية المقدمة بين مؤسسة وأخرى وفق طبيعة نشاطاتها والجهود المبذولة لتحقيق الأهداف التنظيمية في ظل البيئة المحيطة، ويعكس الأداء المصرفي القدرة على استثمار الموارد المتاحة لتحقيق الأهداف الطويلة الأجل وضمان استمرارية المصرف في مواجهة التحديات المالية والتشغيلية. وقد عرف الباحثون الأداء المصرفي بعدة مفاهيم، إذ يُعد أداة لقياس النشاط المصرفي تُستخدم لتقييم أنشطة المصرف وقياس النتائج المحققة لمقارنتها مع الأهداف الموضوعة والوقوف على المعوقات واتخاذ القرارات اللازمة لتجاوزها. (Aljanabi & Roish, 2022, 148)

ويشير العتابي إلى أن الأداء يعكس جميع الأنشطة والفعاليات التي يقوم بها المصرف بهدف تحقيق الأهداف المرجوة بكفاءة وفعالية عالية (العتابي، 2016, 10).

2. أهداف الأداء المصرفي:

أهداف الأداء المصرفي: إن الهدف الأساسي للأداء المصرفي تجسد في تطوير الأداء المالي وتحسين مستوى النشاط المصرفي ليتماشى في تطوره مع التوسع والتقدم الاقتصادي للبلد، فضلاً عن تحقيق عدد من الأهداف النوعية المتعلقة أساساً بإمداد الوظيفة التخطيطية والإشرافية بالمعلومات والبيانات التي تمكنهم من حسن أدائهم لمهامهم. وإن لتحقيق الهدف الأساسي لتقويم الأداء وأهدافه الفرعية المكملة له يجب أن يتميز بعدد من الخصائص أهمها شموله لفروع وأقسام النشاط المصرفي كافة، ويبرز ارتباط تقويم الأداء بالوظائف الإدارية الأخرى كالتنظيمية والتخطيطية وضرورة تمتع هذه الأهداف بالواقعية والموضوعية، والقدرة العالية للقائمين عليها بتحقيق نتائج إيجابية، لذلك تتمتع هذه العملية بالمرونة والقدرة على التطور الدائم لتتماشى مع التطورات والتغييرات الحاصلة في البنية الاقتصادية عموماً والنشاط المصرفي خصوصاً. (Chaudhary et al., 2020, 390)

3. الأبعاد الأساسية للأداء المصرفي:

يمكن قياس الأداء المصرف من خلال ثلاثة أبعاد:

أ. رضا العاملين يُعرف رضا العاملين بأنه حالة عاطفية إيجابية بين الفرد في وظيفته والمنظمة وإن رضا العاملين يمثل مزيج من ردود الفعل العاطفية على التوقعات التفاضلية لما يحتاجه العاملين في الحصول عليه مقارنة بما يتلقونه في مكان العمل.

ب. تحسين الإنتاجية: إن تحسين الإنتاجية يعتمد على استكشاف الفرص الإنتاجية المشتركة في المنظمة من أجل إحداث التطورات على المنتجات، فإن إنتاجية العاملين تمثل النسبة بين ساعات العمل المنجز وساعات العمل المستغرقة في تنفيذ مشاريع المنظمة. (Chaudhary et al., 2020: 390)

ت. النمو: يمثل النمو المرتكز الأساس الذي يعكس نية الشركة لتحقيق النمو البسيط وزيادة قيمتها الجزئية من خلال تخصيص الموارد والاهتمام باستمرار بهدف زيادة استراتيجيات نمو الشركة، فضلاً عن أنه يهدف باستمرار إلى تحقيق حصة أعلى من المتوسط في السوق والمبيعات والحجم (في أعداد الموظفين)، فضلاً عن تقديم مساهمة فوق المتوسط لأداء السوق في الشركة، فممارسة التنفيذ المتزامن للاستراتيجيات الموالية للربح والمؤيدة للنمو تزيد من القيمة الإجمالية للشركة (العبيدي، 2025: 414)

شكل (4): أبعاد الأداء المصرفي (المصدر: من إعداد الباحثين بالاعتماد على المصادر الواردة أعلاه)

يشكل التوقيع الإلكتروني أحد الأدوات المحورية في دعم استراتيجيات الأمن السيبراني داخل المؤسسات المصرفية، إذ لا يقتصر دوره على كونه وسيلة تقنية للتوثيق والمصادقة على المعاملات الرقمية، بل يتجاوز ذلك ليصبح آلية متكاملة لحماية الأنظمة المالية من المخاطر السيبرانية. فهو يوفر ضمانات قوية تتعلق بالمصداقية وعدم الإنكار وسلامة البيانات، ما يقلل بدرجة كبيرة من احتمالية التزوير، الانتحال، أو التلاعب بالمعاملات الإلكترونية. وبذلك يسهم في ترسيخ الثقة المتبادلة بين المصارف وعملائها، ويعزز موثوقية البيئة المصرفية الرقمية. كما أن اعتماد التوقيع الإلكتروني يساهم في رفع مستوى الكفاءة التشغيلية، من خلال تسريع إنجاز المعاملات وتقليل الحاجة إلى الإجراءات الورقية، بما يؤدي إلى تحسين جودة الخدمات وزيادة دقة العمليات. ويتجلى أثره المباشر في تطوير الأداء المصرفي عبر تحقيق التكامل بين السرعة والموثوقية واستمرارية تقديم الخدمات المالية. وإلى جانب ذلك، فإن دمج التوقيع الإلكتروني ضمن استراتيجيات إدارة المخاطر يتيح للمصارف بناء أنظمة وقائية استباقية قادرة على مواجهة التهديدات السيبرانية بفاعلية أكبر، مع تعزيز البنية التحتية الرقمية لتكون أكثر قدرة على التكيف مع متطلبات التحول الرقمي.

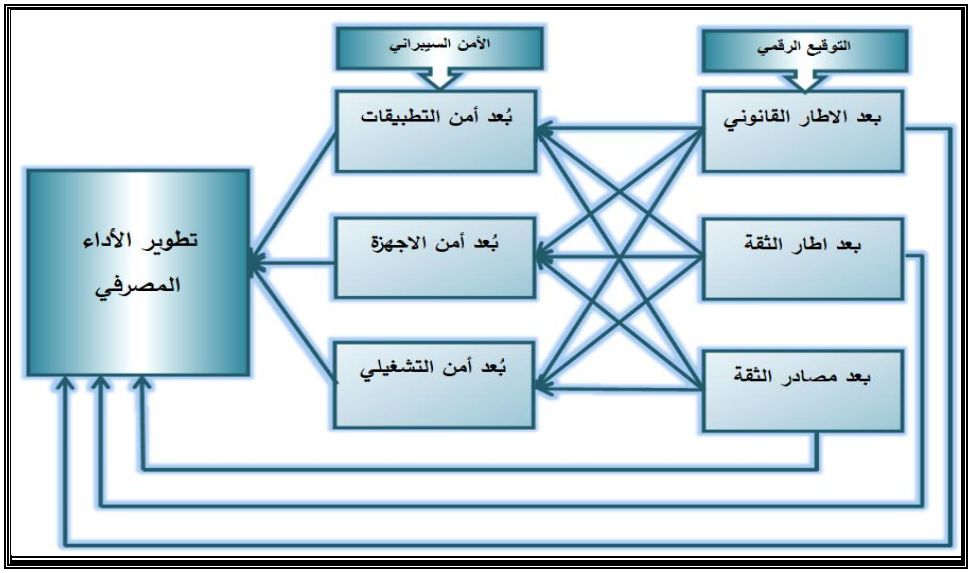
وعليه، يمكن القول إن التوقيع الإلكتروني يمثل مدخلاً متكاملاً يربط بين الأمن السيبراني وكفاءة الأداء المصرفي، ويشكل ركيزة أساسية لتحقيق التحول الرقمي المستدام في القطاع المصرفي، بما ينسجم مع التوجهات العالمية نحو اقتصاد أكثر أمانًا وابتكارًا.

المبحث الثالث: الجانب التطبيقي

أولاً: الهدف من الدراسة التطبيقية:

تهدف هذه الدراسة إلى الحصول على دليل ميداني عن التوقيع الإلكتروني كمدخل لتعزيز الأمن السيبراني وتطوير الأداء المصرفي من خلال تحليل وجهات النظر العلمية والعملية للفئات المعنية بالبحث، وذلك من خلال اختبار فروض البحث وتحديد مدي قبول هذه الفروض من عدمه.

ثانياً: الأنموذج الفرضي:



الشكل (5): أنموذج الفرضي للدراسة (المصدر: من إعداد الباحثين بالاعتماد على المصادر المذكورة)

ثالثاً: فروض الدراسة:

في ضوء طبيعة مشكلة البحث وأهميته وأهدافه يمكن صياغة فرضيات البحث على النحو التالي:

1. للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.
2. للأمن السيبراني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.
3. للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي.

رابعاً: تحديد مجتمع البحث واختيار العينة:

1. تتناول الدراسة المصارف العراقية الحكومية المتمثلة بمصرفي الرافدين والرشيد في النجف الاشرف.
2. عينة الدراسة: تم اختيار عينة من مجتمع الدراسة، وقد اعتمد الباحث في تحديد مفردات هذه العينة على أسلوب العينات الحكمية Judgmental Sampling نظراً لعدم توافر المعلمات الإحصائية لفئات الدراسة، وبالتالي عدم إمكانية الاعتماد على أسلوب العينات الإحصائية في تحديد عينة الدراسة.

خامساً: حدود البحث:

1. الحدود المكانية: تحقيقاً لهدف البحث واختبار فرضياتها تم اختيار مصرفي الرافدين والرشيد في النجف الاشرف لتحقيق الأهداف المرجوة بشأن موضوع البحث.
2. الحدود الزمانية: جرى توزيع الاستبانة بتاريخ (2025/8/15) وجرى جمعها بتاريخ (2025/9/15).
3. الحدود البشرية: العينة التي أُختيرت كانت تمثل القيادات في الإدارة العليا والوسطى والإشرافية في مصرفي الرافدين والرشيد في النجف الاشرف.

سادساً: خصائص عينة البحث:

استُخدمت العينة القصدية إذ جرى اختيار المدراء ورؤساء الأقسام في المصارف المبحوثة من المراكز الوظيفية العاملة في

بغداد. وبلغ المجموع الكلي لعينة البحث (100) شخص، فقد جرى توزيع (85) استبانة بصورة مباشرة وتم استبعاد (5) لم يتم الإجابة عليها وقد تم اعتماد (80) استبانة في التحليل. يوضح الجدول (1) توزيع الخصائص الديموغرافية للعينة كما يلي:

1. الجنس: أظهرت النتائج أن غالبية المشاركين من الذكور، حيث بلغ عددهم (56) فرداً بنسبة (70%)، مقابل (24) أنثى بنسبة (30%).
2. الفئة العمرية: سجلت الفئة العمرية (31-40) النسبة الأعلى بين المشاركين بواقع (38) فرداً و(48%)، تلتها الفئة (41-50) بنسبة (36%) وعدد (29) فرداً، ثم الفئة (أكثر من 50) بنسبة (16%) وعدد (13) فرداً، بينما لم تُسجَّل أي استجابة للفئة (30 سنة فأقل).
3. عدد سنوات الخدمة في المنصب الحالي: جاءت الفئة (8-12) سنة على رأس التوزيع بنسبة (43%) وعدد (34) فرداً، تلتها الفئة (13-17) سنة بنسبة (36%) و(29) فرداً، ثم الفئة (3-7) سنوات بنسبة (17%) و(14) فرداً، وأقل فئة هي (أقل من 3 سنوات) بنسبة (4%) و(3) أفراد، ولم تسجل أي استجابة لفئة (18 سنة فأكثر).
4. إجمالي الخدمة في المصرف: توزعت الاستجابات على أربع فئات، حيث جاءت الفئة (11-20) سنة النسبة الأعلى (34%) و(29) فرداً، تلتها الفئة (5-10) سنوات بنسبة (26%) و(21) فرداً، ثم كل من الفئتين (21-30) و(31-40) بنسبة متساوية (20%) و(16) فرداً لكل منهما.
5. المؤهل العلمي: شكلت الفئة الحاصلة على شهادة البكالوريوس النسبة الأكبر (63%) وعدد (52) فرداً، تلتها الفئة الحاصلة على الدبلوم بنسبة (20%) و(16) فرداً، ثم الإعدادية بنسبة (10%) و(6) أفراد، وأخيراً الدبلوم العالي بنسبة (7%) وعدد (6) أفراد.

جدول (1): خصائص عينة البحث

ت	المتغيرات	توزيع الخاصية	العـــــــــــدد	النسبة
-1	الجنس	ذكر	56	70%
		انثى	24	30%
		المجموع	80	100%
-2	الفئة العمرية	30 سنة فأقل	-	-
		40-31	38	48%
		50-41	29	36%
		أكثر من 50	13	16%
		المجموع	80	100%
-3	عدد سنوات الخدمة في المنصب الحالي	أقل من 3	3	4%
		7-3	14	17%
		12-8	34	43%
		17-13	29	36%
		18 فأكثر	-	-
		المجموع	80	100%
-4	اجمالي الخدمة في المصرف	أقل من 5	-	-
		10-5	21	26%
		20-11	29	4%3
		30-21	16	%20
		35-31	16	20%
		المجموع	80	100%
-5	المؤهل العلمي	اعدادية	6	0%1
		دبلوم	16	20%
		بكالوريوس	52	3%6
		دبلوم عالي	6	7%
		المجموع	80	100%

سابعاً: الأساليب الإحصائية المستخدمة في الدراسة:

بعد مراجعة استمارات الاستقصاء، تم ترميز البيانات، وإدخال إجاباتها على الحاسب الآلي باستخدام برنامج التحليل الإحصائي Version 17 (SPSS) Statistical Packge for Social Sciences، وذلك لإجراء التحليل الإحصائي لبيانات الدراسة الميدانية، حيث استخدم الباحث الأساليب الإحصائية التالية:

1. الأساليب الإحصائية الاعتمادية: وهي الأساليب التي تهتم بمدي إمكانية الاعتماد على نتائج تحليل بيانات قائمة الاستقصاء بمعني مدي تجانس الإجابات بين المستقصي منهم ومدي إمكانية تعميم نتائجها على المجتمع وذلك من خلال اختبارات معامل الثبات ومعامل الصدق، وقد تم الاعتماد على معامل الفا كرونباخ (Alpha Cronbach).
2. الأساليب الإحصائية الوصفية: هي تلك الأساليب التي تعني بإعطاء معلومات عن خصائص البيانات الداخلة في التحليل بهدف تحديد سمات وخصائص واتجاهات عينة البحث نحو فروض الدراسة ومنها:
   - الوسط الحسابي Mean لمعرفة مدي ارتفاع أو انخفاض إجابات مفردات الدراسة عن المحاور الرئيسية للدراسة.
   - الانحراف المعياري Std. Deviation لمعرفة تشتت إجابات مفردات عينة الدراسة عن المتوسط العام للإجابات.
   - معامل الاختلاف Coefficient of Variance حيث يعتبر أنسب الأساليب الإحصائية التي تستخدم لقياس درجة التشتت في استجابات مفردات عينة الدراسة ويشير التقارب بين المعاملات الى تجانس مفردات العينة.
3. تحليل الانحدار المتدرج Multiple Linear Regressionبطريقة Stepwise لتحديد العلاقة بين المتغيرات وتحديد أهم المتغيرات المستقلة المؤثرة في المتغير التابع.

ثامناً: اختبار الثبات والصدق الذاتي لمتغيرات البحث:

قام الباحث بحساب معامل ألفا كرونباخ Alpha Cronbach باعتباره أكثر أساليب تحليل الاعتمادية (Reliability) دلالة في تقييم درجة التناسق الداخلي بين بنود المقياس الخاضع للاختبار، ويستخدم لبحث مدي إمكانية الاعتماد على نتائج الدراسة الميدانية في تعميم النتائج، وتتراوح قيمة معامل Alpha بين (صفر) و (واحد)، وكلما اقتربت من الواحد دلت على وجود ثبات مرتفع، وكلما اقتربت من الصفر دلت على عدم وجود ثبات.

1. وصف المتغير المستقل (التوقيع الإلكتروني):

تكون المتغير الرئيسي الأول الذي يمثل التوقيع الإلكتروني (المتغير المستقل) للدراسة من (24) فقرة (تساؤلاً) موزعة على خمسة أبعاد فرعية وبواقع (8) فقرات (اسئلة) لكل بعد فرعي، وكالآتي:

- **البُعد الأول: البعد القانوني:**

يُظهر هذا البعد متوسطًا حسابيًا عامًا قدره (4.19)، مما يعكس مستوى مرتفعًا من الالتزام بالضوابط القانونية بين المشاركين. الفقرات المرتبطة بالبعد القانوني تكشف عن تباين نسبي في قوة الالتزام، إذ جاءت فقرة (X1) بأعلى متوسط حسابي (4.39) ونسبة استجابة (87.80%)، وهو ما يدل على اتفاق واسع على أهمية الالتزام الصارم بالقوانين والتعليمات. تلتها فقرة (X2) بمتوسط (4.34) ونسبة (86.83%)، بما يعكس قناعة المشاركين بضرورة الالتزام بالقوانين في مختلف الممارسات. في المقابل، جاءت الفقرتان (X7 وX8) بأدنى متوسطين (3.97 و4.00) على التوالي مع نسب استجابة (79.51% و80%)، ما يشير إلى وجود بعض التباين النسبي في الآراء، وربما حاجة هذه الجوانب لمزيد من التركيز والتعزيز. أما الانحراف المعياري البالغ (0.767) في المتوسط العام، ومعامل الاختلاف البالغ (18.27%)، فيدلان على درجة مقبولة من التجانس بين المشاركين، حيث أن غالبية آرائهم متقاربة وتميل إلى الاتفاق.

الجدول (2): المقاييس الوصفية لبُعد القانوني (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة[1]	معامل الاختلاف[2]
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	36	44	44	54	1	1	0	0	1	1	4.39	0.643	87.80	14.65
X2	34	41	44	54	3	4	0	0	1	1	4.34	0.670	86.83	15.45
X3	35	43	39	48	6	7	1	1	1	1	4.29	0.761	85.85	17.74
X4	30	37	44	54	5	6	2	2	1	1	4.21	0.770	84.39	18.25
X5	30	37	44	54	5	6	3	4	0	0	4.23	0.725	84.63	17.14
X6	27	33	45	55	6	7	3	4	1	1	4.14	0.803	82.93	19.37
X7	22	27	43	52	11	13	5	6	1	1	3.97	0.874	79.51	22.00
X8	22	27	45	55	11	13	1	1	3	4	4.000	0.8888	80.00	22.22
المعدل العام	90%				7%		3%				4.19	0.767	83.9	18.27%

- **البُعد الثاني إطار الثقة:**

يُظهر هذا البعد متوسطًا حسابيًا عامًّا قدره (4.176)، مما يعكس مستوى مرتفعًا من الالتزام بالجوانب التكنولوجية والأنظمة بين المشاركين. الفقرات المرتبطة بالبعد تكشف عن تباين نسبي في قوة هذا الالتزام، إذ جاءت الفقرة (X4) بأعلى متوسط حسابي (4.280) ونسبة استجابة (85.61%)، وهو ما يدل على وجود قناعة راسخة بأهمية تعزيز إطار الثقة في بيئة العمل. تلتها الفقرة (X1) بمتوسط (4.268) ونسبة (85.37%)، بما يعكس إدراكًا متزايدًا لدى المشاركين بأهمية الجوانب المرتبطة بإطار الثقة. في المقابل، جاءت الفقرات (X5) و ** (X7) ** بأدنى متوسطين (4.073 و4.097) على التوالي مع نسب استجابة (81.46%) و (81.95%)، ما يشير إلى وجود بعض التباين النسبي في الآراء، وربما حاجة هذه الجوانب لمزيد من التركيز والتطوير مقارنة ببقية الفقرات. أما الانحراف المعياري البالغ (0.6867) في المتوسط العام، ومعامل الاختلاف البالغ (16.44%)، فيدلان على وجود درجة جيدة من التجانس بين المشاركين، حيث أن غالبية آرائهم متقاربة وتميل إلى الاتفاق على أهمية إطار الثقة.

الجدول (3): المقاييس الوصفية لبُعد إطار الثقة (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	28	34	48	59	6	7	0	0	0	0	4.268	0.5889	85.37	13.80
X2	25	30	51	62	5	6	1	1	0	0	4.219	0.6090	84.39	14.43
X3	28	34	43	52	11	13	0	0	0	0	4.207	0.6617	84.15	15.73
X4	31	38	45	55	4	5	2	2	0	0	4.280	0.6717	85.61	15.69
X5	21	26	50	61	7	9	4	5	0	0	4.073	0.7333	81.46	18.00
X6	26	32	44	54	8	10	4	5	0	0	4.122	0.7760	82.44	18.83
X7	22	27	50	61	6	7	4	5	0	0	4.097	0.7304	81.95	17.83
X8	25	30	47	57	7	9	3	4	0	0	4.146	0.7221	82.93	17.42
المعدل العام	89%				9%		2%				4.176	0.6867	83.54	16.44

- **البُعد الثالث: مصادر الثقة (تقبل المستخدم):**

يُظهر هذا البعد متوسطًا حسابيًا عامًّا قدره (4.144)، مما يعكس مستوى مرتفعًا من مصادر الثقة (تقبل المستخدم) بين المشاركين. وتُظهر الفقرات المرتبطة بهذا البعد بعض التباين في مستويات الاستجابة، إذ جاءت الفقرة (X2) بأعلى

[1] (نسبة الاستجابة بالمئة = الوسط الحسابي \بدائل الاستجابة 5 * 100).
[2] (معامل الاختلاف = الانحراف المعياري \الوسط الحسابي * 100).

متوسط حسابي (4.256) ونسبة استجابة (85.12%)، ما يشير إلى إدراك قوي لدى المشاركين بأهمية مصادر الثقة تلتها الفقرتان (X1) و** (X4) ** بمتوسطين (4.219) و (4.207) ونسب استجابة (84.39%) و(84.15%)، بما يؤكد استقرار مستوى الالتزام في جوانب مصادر الثقة (تقبل المستخدم) الأساسية. في المقابل، جاءت الفقرتان (X6) و ** ** (X8) بأدنى متوسطين (4.048) و (4.036) على التوالي مع نسب استجابة (80.98%) و (و80.73%)، وهو ما يعكس وجود بعض التباين النسبي في آراء المشاركين، ويُظهر أن هذه الجوانب بحاجة إلى اهتمام إضافي لتعزيز الالتزام فيها. أما الانحراف المعياري البالغ (0.6803) ومعامل الاختلاف (16.42%) في المتوسط العام، فيدلان على درجة جيدة من التجانس بين المشاركين، حيث إن معظم آرائهم متقاربة وتميل إلى الاتفاق حول أهمية مصادر الثقة (تقبل المستخدم).

الجدول (4): المقاييس الوصفية لبُعد مصادر الثقة (تقبل المستخدم) (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

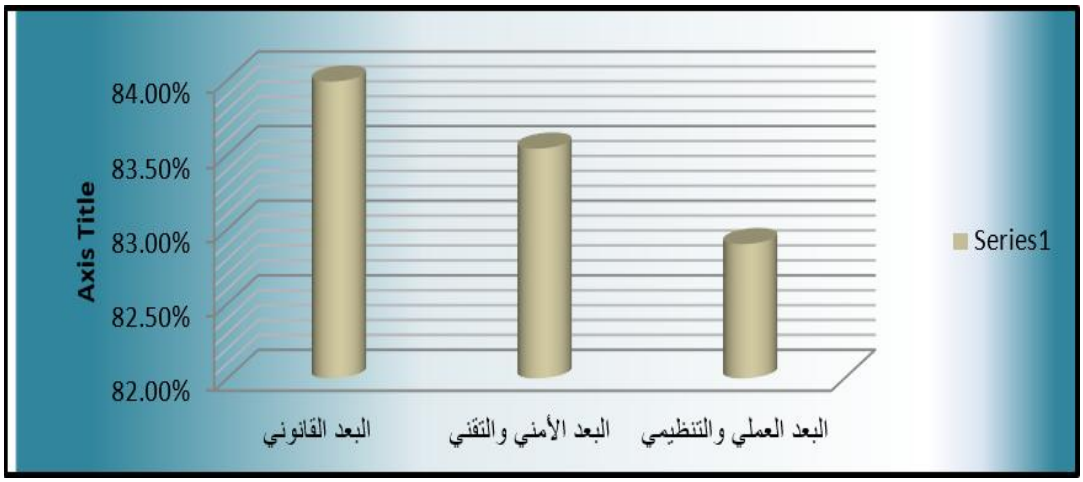
الفقرات	بدائل الاستجابة												الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً							
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%						
X1	26	32	49	60	6	7	1	1	0	0			4.219	0.629	84.39	14.91
X2	**27**	**33**	**50**	**61**	**4**	**5**	**1**	**1**	**0**	**0**			**4.256**	**0.6047**	**85.12**	**14.21**
X3	22	27	53	65	6	7	0	0	1	1			4.158	0.6567	83.17	15.79
X4	28	34	46	56	6	7	1	1	1	1			4.207	0.7326	84.15	17.41
X5	22	27	50	61	8	10	2	2	0	0			4.122	0.6738	82.44	16.35
X6	18	22	53	65	8	10	3	4	0	0			4.048	0.6831	80.98	16.87
X7	25	30	45	55	8	10	4	5	0	0			4.1098	0.7699	82.20	18.73
X8	18	22	52	63	9	11	3	4	0	0			4.036	0.6929	80.73	17.17
المعدل العام	89%				9%		2%						**4.144**	**0.6803**	**82.90**	**16.42**

ويدرج الباحث جدولاً بنتائج المقاييس الوصفية للأبعاد الخمسة للمتغير المستقل (التوقيع الإلكتروني) وكالآتي:

الجدول (5): خلاصة نتائج المقاييس الوصفية لأبعاد المتغير المستقل (التوقيع الإلكتروني) (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الأبعاد	الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
البعد القانوني	4.1997	0.76718	83.99%	18.27%
البعد التكنولوجي والأنظمة	4.1768	0.68670	83.54%	16.44%
البعد العملي (تقبل المستخدم)	4.1448	0.68037	82.90%	16.42%

يتضح من خلال معطيات الجدول (5) امتلاك البعد الأول والمتمثل بـ (البعد القانوني) للصدارة ومجيئه بالمرتبة الأولى قياساً بالأبعاد الأخرى، وذلك نتيجة لامتلاكه لأعلى وسط حسابي والبالغ (4.1997)، والشكل (6) الآتي يوضح نسب الاستجابة للأبعاد الخمسة والتي تمثل تقنيات التوقيع الإلكتروني.



الشكل (6): نسبة الاستجابة لأبعاد التوقيع الإلكتروني (المصدر: الشكل من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26).

وصف المتغير المستقل (الأمن السيبراني):

تكون المتغير الرئيسي الثاني الأمن السيبراني الذي يمثل (المتغير المستقل) للدراسة من (9) فقرة (تساؤلاً) موزعة على ثلاثة أبعاد الأول: أمن التطبيقات والبُعد الثاني: أمن السحابي، والبُعد الثالث: أمن التشغيلي، وكالآتي:

أولاً: بُعد أمن التطبيقات:

يُظهر هذا البعد متوسطًا حسابيًا عامًّا قدره (4.1667)، مما يعكس مستوى مرتفعًا من الالتزام بالإجراءات أمن التطبيقات بين المشاركين. وتُبين نتائج الفقرات أن الفقرة (X1) سجلت أعلى متوسط حسابي (4.243) وبنسبة استجابة (84.88%)، وهو ما يعكس إدراكًا قويًا لدى المشاركين بأهمية الإجراءات أمن التطبيقات في بيئة العمل. تلتها الفقرة (X2) بمتوسط (4.134) ونسبة استجابة (82.68%)، بما يشير إلى اتفاق واسع على أهمية الالتزام بجوانب الوقاية المختلفة. أما الفقرة (X3) فقد جاءت بأدنى متوسط حسابي (4.122) مع نسبة استجابة (82.44%)، ورغم أنها أقل نسبيًا من غيرها، إلا أنها ما تزال ضمن المستوى المرتفع، ما يدل على وجود اتفاق عام مع بعض التباين البسيط في الآراء. وبالنسبة للانحراف المعياري البالغ (0.60456) ومعامل الاختلاف (14.51%)، فهما يعكسان درجة عالية من التجانس بين آراء المشاركين، حيث أن معظمهم متقاربون في تقييمهم ويؤكدون على أهمية الالتزام بالإجراءات أمن التطبيقات.

الجدول (6): المقاييس الوصفية لبُعد أمن التطبيقات (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	**25**	**30**	**52**	**63**	**5**	**6**	**0**	**0**	**0**	**0**	**4.243**	**0.5569**	**84.88**	**13.12**
X2	19	23	56	68	6	7	1	1	0	0	4.134	0.5829	82.68	14.10
X3	22	27	50	61	8	10	2	2	0	0	4.122	0.6738	82.44	16.35
المعدل العام	**92%**				**7%**		**1%**				**4.1667**	**0.60456**	**83.33%**	**14.51%**

ثانياً: بُعد أمن السحابي:

يُظهر هذا البعد متوسطًا حسابيًا عامًّا قدره (4.056)، مما يعكس مستوى جيدًا من الاهتمام بالجانب أمن السحابي لدى المشاركين، وإن كان أدنى نسبيًا مقارنةً ببعض الأبعاد الأخرى. وتشير النتائج إلى أن الفقرة (X1) سجلت أعلى متوسط حسابي (4.097) بنسبة استجابة (81.95%)، ما يدل على إدراك المشاركين لأهمية الاستكشاف في تطوير بيئة العمل. تلتها الفقرة (X2) بمتوسط (4.085) ونسبة استجابة (81.71%)، لكنها سجلت انحرافًا معياريًا أعلى (0.8043) ومعامل اختلاف (19.69%)، وهو ما يشير إلى وجود تباين أو اختلاف نسبي في آراء المشاركين حولها. أما الفقرة (X3) فقد جاءت بأدنى

متوسط حسابي (3.987) ونسبة استجابة (79.76%)، وهو ما يعكس مستوى مقبولًا من الاتفاق، مع بعض التفاوت النسبي في التقييمات. وبالنسبة للانحراف المعياري البالغ (0.7424) ومعامل الاختلاف (18.30%) في المتوسط العام، فهما يعكسان درجة مقبولة من التجانس بين آراء المشاركين، مع وجود بعض التباين في الاستجابات، خصوصًا في الفقرتين (X2 و X3).

الجدول (7): المقاييس الوصفية لبُعد أمن السحابي (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	**21**	**26**	**50**	**61**	**9**	**11**	**2**	**2**	**0**	**0**	**4.097**	**0.6778**	**81.95**	**16.54**
X2	25	30	44	54	8	10	5	6	0	0	4.085	0.8043	81.71	19.69
X3	17	21	52	63	8	10	5	6	0	0	3.987	0.7452	79.76	18.69
المعدل العام	**85%**				**10%**		**5%**				**4.056**	**0.7424**	**81.14**	**18.30**

ثالثاً: بُعد أمن التشغيلي:

يبين الجدول (8) النتائج الإحصائية المتعلقة ببُعد أمن التشغيلي، إذ جاءت قيم المتوسطات الحسابية للفقرات الثلاث (X1، X2، X3) ضمن نطاق مرتفع، تراوحت بين (4.036 – 4.061)، وهو ما يعكس مستوى إيجابي في استجابات المبحوثين. وقد أظهرت الانحرافات المعيارية قيماً معتدلة (0.6748 – 0.7769)، مما يدل على تقارب نسبي في آراء الأفراد حول الفقرات. كما أن نسب الاستجابة الكلية أظهرت أن (86%) من المبحوثين اختاروا بدائل (أتفق تماماً /أتفق)، مقابل (10%) لمحايدين، و(4%) فقط اختاروا عدم الاتفاق بدرجاته، وهو ما يؤكد أن الغالبية العظمى من العينة تنظر بشكل إيجابي إلى هذا البعد. أما معامل الاختلاف، فقد تراوح بين (16.72% – 19.25%)، وهو أقل من الحد المقبول (25%)، مما يعزز من تجانس البيانات وصدق الاعتمادية الإحصائية. وبالمحصلة، بلغ المتوسط العام (4.044) بنسبة استجابة (80.89%) ومعامل اختلاف (17.81%)، ما يشير إلى أن بُعد الاستجابة والتعافي قد تحقق بدرجة جيدة جداً في عينة الدراسة.

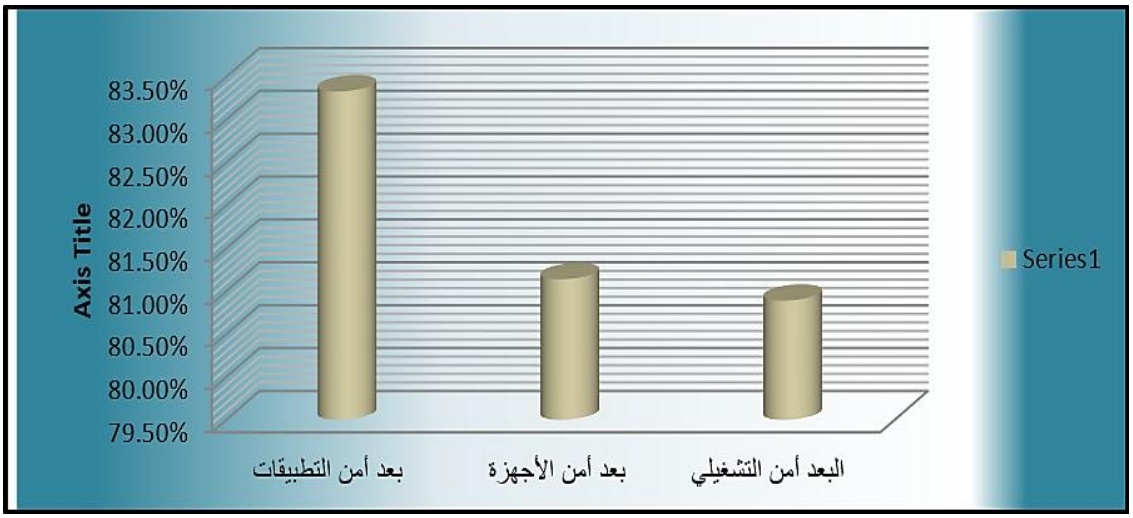
الجدول (8): المقاييس الوصفية لبُعد أمن التشغيلي (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	**19**	**23**	**53**	**65**	**6**	**7**	**4**	**5**	**0**	**0**	**4.061**	**0.7088**	**81.22**	**17.45**
X2	20	24	50	61	8	10	3	4	1	1	4.036	0.7769	80.73	19.25
X3	18	22	51	62	11	13	2	2	0	0	4.036	0.6748	80.73	16.72
المعدل العام	**86%**				**10%**		**4%**				**4.044**	**0.7201**	**80.89**	**17.81**

ويدرج الباحث جدولاً بنتائج المقاييس الوصفية للأبعاد الخمسة للمتغير (الأمن السيبراني) وكالآتي:

الجدول (9): خلاصة نتائج المقاييس الوصفية لأبعاد المتغير (الأمن السيبراني) (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الأبعاد	الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف
بُعد أمن التطبيقات	4.1667	0.60456	83.33%	14.51%
بُعد أمن السحابي	4.0569	0.74248	81.14%	18.30%
بُعد أمن التشغيلي	4.0447	0.72019	80.89%	17.81%



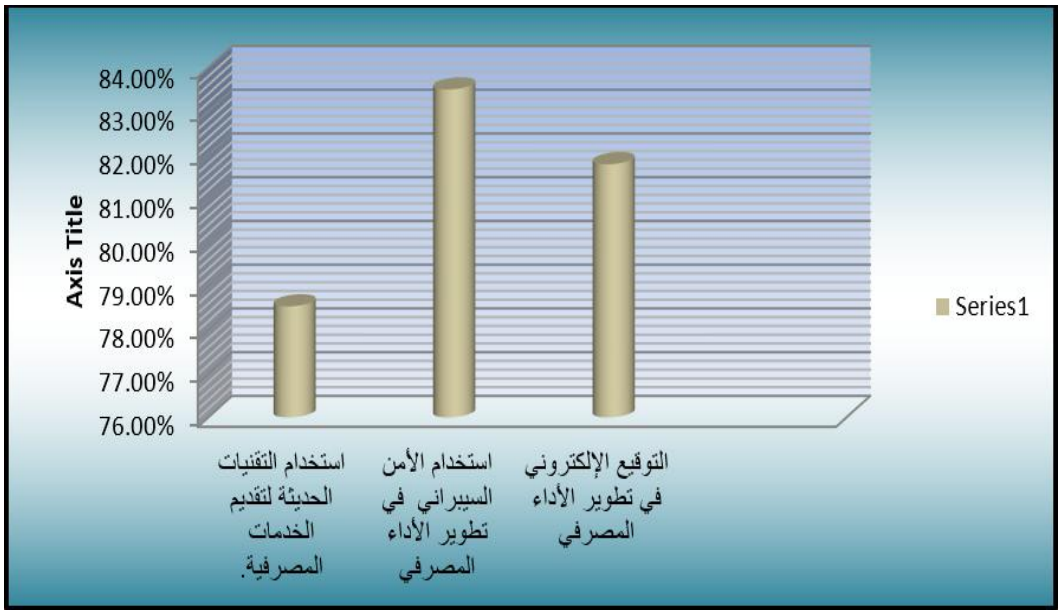
الشكل (3): نسبة الاستجابة للأبعاد الأمن السيبراني (المصدر: الشكل من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية (SPSS V26))

وصف المتغير التابع (الأداء المصرفي):

يتجسد المتغير التابع تطوير الأداء المصرفي بـ (3) متغيرات فرعية والمتمثلة بـ (X1-X3)، وكما في الجدول (10) وجاءت نسبة الاتفاق الكلي لهذا البعد بما نسبته (81%) من إجابات الأفراد المبحوثين، أما الإجابات المحايدة فقد تمثلت بما نسبته (13%)، وجاءت نسبة عدم الاتفاق الكلي بواقع (6%)، وقد جاءت قيمة الوسط الحسابي معززة لهذه النسبة إذ بلغت قيمته ما مقداره (3.9268) والتي جاءت بدورها أكبر من قيمة الوسط الحسابي الفرضي التي تبلغ (3)، فضلاً عن قيمة الانحراف المعياري التي بلغت (0.80136)، أما نسبة الاستجابة فقد جاءت بما مقداره (78.54%)، أما نسبة معامل الاختلاف فقد بلغت (20.41%)، وجاءت أعلى نسبة اتفاق للمتغيرات الفرعية لهذا البعد لكل من الفقرة (X1) و (X2) بنسبة (80%).

الجدول (10): تطوير الأداء المصرفي (المصدر: الجدول من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية SPSS V26)

الفقرات	بدائل الاستجابة										معامل الاختلاف	نسبة الاستجابة	الانحراف المعياري	الوسط الحسابي
	أتفق تماماً		أتفق		محايد		لا أتفق		لا أتفق تماماً					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
X1	**14**	**17**	**52**	**63**	**11**	**13**	**5**	**6**	**0**	**0**	**18.91**	**78.29**	**0.740**	**3.914**
X2	**19**	**23**	**47**	**57**	**11**	**13**	**4**	**5**	**1**	**1**	**20.77**	**79.27**	**0.823**	**3.963**
X3	17	21	47	57	12	15	5	6	1	1	21.54	78.05	0.840	3.902
المعدل العام	**81%**				**13%**		**6%**				**20.41**	**78.54**	**0.801**	**3.926**



الشكل (4): نسبة الاستجابة لمتغير التابع تطوير الأداء المصرفي (المصدر: الشكل من إعداد الباحث اعتماداً على نتائج البرمجة الإحصائية (SPSS V26))

عاشراً: اثبات متغيرات الدراسة للعينة المبحوثة:

أولاً: فرضية الدراسة الأولى: للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.

الجدول (10): نتائج تأثير التوقيع الإلكتروني في الأداء المصرفي (المصدر: من إعداد الباحث اعتماداً على ما جاءت به نتائج البرمجة الإحصائية (SPSS

الأداء المصرفي / التوقيع الإلكتروني	معامل الارتباط	T		مستوى المعنوية P-Value
		المحسوبة	الجدولية	
	0.697	8.694	1.993	0.000**

$P \leq 0.05$, $N = 82$, $df^{1} = 80$

**highly significant at $p \leq 0.01$

استناداً لما قدمته النتائج الواردة ضمن الجدول (10) أعلاه فقد لوحظ وجود علاقة ارتباط معنوية بين التوقيع الإلكتروني والأداء المصرفي، وجاء ذلك عند مستوى معنوية (0.000)، إذ جاء معامل الارتباط بما قيمته (0.697)، عند مستوى المعنوية (0.05) ودرجة حرية (80)، واعتماداً على ما جاءت به قيمة (T) المحسوبة والبالغة (8.694)، فقد كانت أكبر من قيمتها الجدولية البالغة (1.993)[2]، وعليه تحققت الفرضية الأولى، التي نَصت على أنه (للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي).

[1] (درجة الحرية df (degrees of freedom) وهي عدد القيم التي يمكننا استعمالها فعلياً في التقدير، وتحسب في علاقات الارتباط عند قيمة تساوي (80) كما في الفرضية الرئيسية الأولى والفرضيات المتفرعة منها، وكذلك بالنسبة للفرضية الثالثة والفرضيات المتفرعة منها. وتحسب في علاقات التأثير عند قيمة تساوي (80 & 1) كما في الفرضية الرئيسة الثانية والفرضيات المتفرعة منها، وكذلك بالنسبة للفرضية الرابعة والفرضيات المتفرعة منها).

[2] (إحصائياً إذ كانت قيمة T المحسوبة أكبر من قيمة T الجدولية، يتم في هذه الحالة قبول فرضية الدراسة ورفض الفرضية الصفرية "العدمية"، والعكس صحيح أيضاً).

ثانياً: فرضية الدراسة الثانية: للأمن السيبراني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي.

الجدول (11): نتائج تأثير وأمن السيبراني في الأداء المصرفي (المصدر: من إعداد الباحث اعتماداً على ما جاءت به نتائج البرمجة الإحصائية SPSS)

الأداء المصرفي / أمن السيبراني	التأثير β1	R^2	F المحسوبة	F الجدولية	مستوى المعنوية P-Value
	0.264 (8.700)*	0.486	75.684	3.973	0.000**

$P \leq 0.05$, N =82, df = (1 & 80)

**highly significant at $p \leq 0.01$

توضح النتائج الواردة ضمن الجدول (11) أعلاه وجود تأثير ذو دلالة معنوية للأمن السيبراني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي، إذ اكدت قيمة (F) المحسوبة هذا الأمر عندما بلغت قيمتها (75.684) والتي جاءت بقيمة أكبر من قيمتها الجدولية التي تبلغ (3.937) عند مستوى معنوية (0.05) ودرجتي حرية (80 & 1)، وعلى هذا الأساس يمكن الاستدلال حول مستوى تأثير الأمن السيبراني وقوته على الأداء المصرفي، وإلى جانب ما سبق، تبلغ قيمة معامل التحديد (R^2) ما قيمته (0.486)، الأمر الذي يوضح بدوره أن الأمن السيبراني قد أسهم في تفسير ما نسبته (48.6%) من مجموع ما تحقق من تأثيرات في الأداء المصرفي، وفيما يتعلق بالمتبقي منها فبالإمكان أن تسند لمتغيرات أخرى عشوائية تعد خارج أنموذج الانحدار من الأساس، فضلاً عن ذلك يمكن ومن خلال متابعة معاملات (β) توضيح نتائج (T) والتي جاءت قيمتها المحسوبة بما مقداره (8.700)، وهو ما جاء بمقدار أكبر من قيمتها الجدولية التي تبلغ (1.993)، ووفقاً لذلك تحققت الفرضية الثانية، التي نَصت على أنه (للأمن السيبراني علاقة ارتباط ذو دلالة إحصائية على الأداء المصرفي).

ثالثاً: فرضية الدراسة الثالثة: للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي.

الجدول (12): نتائج تأثير التوقيع الإلكتروني في أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي (المصدر: من إعداد الباحث اعتماداً على ما جاءت به نتائج البرمجة الإحصائية SPSS)

تطوير الأداء المصرفي / التوقيع الإلكتروني أمن السيبراني	التأثير β1	R^2	F المحسوبة	F الجدولية	مستوى المعنوية P-Value
	0.265 (7.534)*	0.415	56.756	3.973	0.000**

$P \leq 0.05$, N =82, df = (1 & 80)

**highly significant at $p \leq 0.01$

يستدل استناداً لما قدمه الجدول (12) أعلاه من نتائج حول للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي إذ اكدت قيمة (F) المحسوبة هذا الأمر عندما بلغت قيمتها (56.756) والتي جاءت بقيمة أكبر من قيمتها الجدولية التي تبلغ (3.937) عند مستوى معنوية (0.05) ودرجتي حرية (80 & 1)، وعلى هذا الأساس يمكن الاستدلال حول مستوى تأثير التوقيع الإلكتروني وأمن السيبراني وقوته على تطوير الأداء المصرفي، وإلى جانب ما سبق، تبلغ قيمة معامل التحديد (R^2) ما قيمته (0.415)، الأمر الذي يوضح بدوره أن التوقيع الإلكتروني وأمن السيبراني قد أسهما في تفسير ما نسبته (41.5%) من مجموع ما تحقق من تأثيرات في تطوير الأداء المصرفي، وفيما يتعلق بالمتبقي منها فبالإمكان أن تسند لمتغيرات أخرى عشوائية تعد خارج أنموذج الانحدار من الأساس، فضلاً عن ذلك يمكن ومن خلال متابعة معاملات (β) توضيح نتائج (T) والتي جاءت قيمتها المحسوبة بما مقداره (7.534)، وهو ما جاء بمقدار اكبر من قيمتها الجدولية التي تبلغ (1.993)، ووفقاً لذلك تحققت الفرضية الثالثة التي نَصت على أنه (للتوقيع الإلكتروني علاقة ارتباط ذو دلالة إحصائية على أمن السيبراني للاستفادة من إيجابيات هذه النظم وتكييفها لتطوير الأداء المصرفي).

مناقشة النتائج

تركز هذه الدراسة التطبيقية على استكشاف أثر التوقيع الإلكتروني والأمن السيبراني على الأداء المصرفي في المصارف الحكومية العراقية، وذلك عبر تحليل البيانات الميدانية المتعلقة بوجهات نظر القيادات في الإدارة العليا والوسطى والإشرافية في مصرفي الرافدين والرشيد. أظهرت نتائج الدراسة أن المتغيرات المستقلة، المتمثلة بالتوقيع الإلكتروني والأمن السيبراني، تسهم بشكل بارز في تعزيز الأداء المصرفي وتحقيق كفاءة وفاعلية العمليات البنكية.

كشف التحليل الوصفي للبيانات أن التوقيع الإلكتروني يحظى بمستوى عالٍ من الالتزام لدى المشاركين، لا سيما فيما يتعلق بالأبعاد القانونية والتكنولوجية وإطار الثقة. وقد بينت النتائج أن الالتزام بالضوابط القانونية يسجل أعلى معدل، مما يعكس أهمية توافق العمليات المصرفية مع الأطر القانونية في تعزيز المصداقية والشفافية. كما أشارت أبعاد التوقيع الإلكتروني المرتبطة بإطار الثقة وتقبل المستخدم إلى مستوى جيد من التفاعل الإيجابي، مما يوضح أن تبني هذه النظم يساهم في تعزيز الثقة الداخلية والخارجية للمؤسسة.

أما فيما يتعلق بالأمن السيبراني، فقد أبرزت النتائج وعي المشاركين بأهمية الأبعاد الثلاثة للأمن، وهي أمن التطبيقات، والأمن السحابي، والأمن التشغيلي، في حماية المعلومات وضمان استمرارية العمليات البنكية. وقد سجل بُعد أمن التطبيقات أعلى مستوى استجابة، مما يدل على اهتمام العاملين بالالتزام بالإجراءات الوقائية والحماية التقنية للأنظمة المصرفية.

وبخصوص الأداء المصرفي، أظهرت البيانات مستويات مرتفعة من التطور وفق تقييمات المشاركين، حيث بلغ متوسط معدلات الاستجابة حوالي 81%، مما يشير إلى إدراك جيد لتأثير التوقيع الإلكتروني والأمن السيبراني في تحسين جودة وكفاءة الخدمات المصرفية.

أظهرت تحليلات الارتباط والانحدار وجود تأثير معنوي لكل من التوقيع الإلكتروني والأمن السيبراني على الأداء المصرفي، حيث يرتبط التوقيع الإلكتروني ارتباطاً إيجابياً قوياً بالأداء، فيما يساهم الأمن السيبراني في تفسير نسبة كبيرة من التباين في النتائج. كما أشارت الدراسة إلى أن التوقيع الإلكتروني يعزز الأمن السيبراني، مما يتيح الاستفادة المتبادلة من هذه النظم لتطوير الأداء المصرفي بشكل مستدام.

بناءً على ذلك، يمكن الاستنتاج أن التكامل بين التوقيع الإلكتروني ونظم الأمن السيبراني يعزز فاعلية العمليات المصرفية ويرفع مستويات الثقة والأمان، ويتيح للقيادات المصرفية تبني سياسات تشغيلية أكثر توافقاً مع متطلبات الرقمنة وحماية المعلومات، بما يسهم في تحسين الأداء الكلي للمؤسسة.

المبحث الرابع: الاستنتاجات والتوصيات

أولاً: الاستنتاجات:

1. يسهم التوقيع الإلكتروني بشكل فعّال في تعزيز الثقة بالمعاملات المصرفية عبر ضمان التوثيق، المصداقية، وعدم الإنكار.
2. يمثل الأمن السيبراني عنصرًا تكامليًا مع التوقيع الإلكتروني في حماية البنية التحتية المصرفية من الاختراق والتزوير.
3. أظهرت المصارف التي تبنت التوقيع الإلكتروني جزئيًا تحسنًا ملموسًا في سرعة وكفاءة إنجاز المعاملات.
4. ضعف الإطار التشريعي والتنظيمي في البيئة المحلية يعد أحد أبرز المعوقات أمام تبني التوقيع الإلكتروني بشكل كامل وفعّال.
5. يساهم التوقيع الإلكتروني في تعزيز الشفافية وتقليل المخاطر المرتبطة بالتلاعب بالبيانات والمعاملات المالية.
6. يرتبط التوقيع الإلكتروني ارتباطًا إيجابيًا ومعنويًا بالأمن السيبراني، مما يعزز القدرة على حماية البيانات والبنية التحتية الرقمية.
7. يعكس التحليل الوصفي للبيانات وعي المشاركين بأهمية الأمن السيبراني، لا سيما في مجالات أمن التطبيقات، والأمن السحابي، والأمن التشغيلي.

8. ثبت وجود تأثير معنوي للتوقيع الإلكتروني والأمن السيبراني على الأداء المصرفي، مما يؤكد أهمية دمجهما ضمن استراتيجيات التحول الرقمي.
9. يسهم التكامل بين التوقيع الإلكتروني والأمن السيبراني في رفع مستويات موثوقية المعاملات وجودة الخدمات المصرفية المقدمة للعملاء.
10. تشير نتائج الدراسة إلى أن تعزيز القدرات التقنية والقانونية للعاملين والعملاء يعد عاملاً حاسمًا لضمان فعالية تطبيق التوقيع الإلكتروني والأمن السيبراني في المصارف العراقية.

ثانياً: التوصيات:

1. ينبغي على الجهات التشريعية وضع إطار قانوني متكامل يحدد أبعاد التوقيع الإلكتروني، بما في ذلك الصلاحيات، المسؤوليات، وضمان حماية الحقوق لجميع الأطراف، سواء كانت المصارف أو العملاء، وذلك لتعزيز الثقة القانونية في المعاملات الرقمية وتقليل المخاطر القانونية المرتبطة بالتحويلات الإلكترونية والمعاملات المصرفية.
2. يتطلب الأمر تطوير أنظمة حماية متقدمة تشمل الأمن الشبكي، الأمن السحابي، والأمن التشغيلي للأنظمة المصرفية، بما يتوافق مع المعايير الدولية، لضمان استمرارية العمليات، تقليل مخاطر الاختراق، وحماية المعلومات المالية الحساسة.
3. يجب تنظيم حملات توعية وورش عمل تثقيفية لتعريف العاملين والعملاء بأهمية التوقيع الإلكتروني، وكيفية استخدامه بالشكل الصحيح، إضافة إلى رفع مستوى فهمهم لإجراءات الأمن السيبراني، مما يعزز الالتزام بالمعايير ويحد من الأخطاء والتلاعب المحتمل.
4. ينبغي ربط التوقيع الإلكتروني بخطط التحول الرقمي الشامل، بما يشمل تحديث البرمجيات، دمج الأنظمة، وتطبيق التقنيات الحديثة في إدارة المعاملات والخدمات المصرفية، وذلك لتحسين سرعة إنجاز العمليات، رفع كفاءة الأداء، وتعزيز رضا العملاء.
5. يمكن دراسة أفضل الممارسات الدولية في مجال التوقيع الإلكتروني والأمن السيبراني، ومن ثم تكييفها لتلبية احتياجات البيئة المصرفية العراقية، مع مراعاة التشريعات المحلية والقدرات التقنية، لضمان تطبيق حلول عملية وفعّالة.
6. يجب تصميم برامج تدريبية دورية للعاملين في المصارف لتعزيز مهاراتهم في الأمن السيبراني والتوقيع الإلكتروني، بما في ذلك التدريب على اكتشاف التهديدات، إدارة المخاطر، وصيانة الأنظمة، لضمان مستوى عالٍ من الكفاءة التشغيلية.
7. ينصح بدمج استخدام التوقيع الإلكتروني في سياسات إدارة المخاطر بالمصارف، لتعزيز حماية البيانات والمعاملات المالية، والحد من فرص التلاعب أو الاحتيال، وبالتالي رفع مستوى الثقة بالمؤسسة المصرفية داخلياً وخارجياً.
8. يُوصى بوضع مؤشرات كمية ونوعية تقيس فاعلية تطبيق التوقيع الإلكتروني والأمن السيبراني، مثل سرعة إنجاز المعاملات، عدد الاختراقات، مستوى رضا العملاء، وموثوقية البيانات، بهدف تحسين الأداء المستمر وتوجيه الاستثمارات المستقبلية.
9. ينبغي إنشاء آليات تنسيق دائمة بين المصارف والهيئات الرقابية لضمان الالتزام بالمعايير القانونية والأمنية، ومتابعة تطبيق الإجراءات الوقائية، مع توفير دعم فني واستشارات لتحسين مستوى الأمن وحماية المعلومات.
10. يُوصى بدعم الدراسات الأكاديمية والتطبيقية التي تبحث في تطوير التوقيع الإلكتروني ورفع مستوى الأمان السيبراني، بما يتيح للمصارف مواكبة التطورات التقنية، واستكشاف حلول مبتكرة لتعزيز الأداء المصرفي وحماية البيانات المالية.

المصادر العربية والأجنبية

أولًا: المصادر العربية:

1. جيجان، إسراء شريف، (2021)، "الأمن السيبراني الصيني: دراسة في الدوافع والتحديات"، جامعة بغداد كلية العلوم السياسية مجلة قضايا سياسية، 65.
2. العبيدي، فائز حازم. (2024). تأثير تقنيات التحول الرقمي في تعزيز فاعلية الأداء المصرفي: الدور الوسيط لنظم المعلومات المحاسبية. مجلة تكريت للعلوم الإدارية والاقتصادية، 20(1/67)، 100-122. كلية الحدباء الجامعة.
3. العتابي، دعاء صباح (2016)، دور أدارة المخاطر في تحسين أداء المصارف الإسلامية، رسائل ماجستير مقدمة إلى المعهد العالي للدراسات المحاسبية والمالية -جامعة بغداد.
4. مرسي محمد ابراهيم (2024)، دور الأمن السيبراني في حماية أطراف عقود التجارة الإلكترونية"، مجلة البحوث الفقهية والقانونية، 47(47)، 4351-4433.
5. المطيري، منيفة، السدراني، غادة، (2024)، "دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل" مجلة الدراسات التربوية والإنسانية، 16(2)، 463-502.

ثانيًا: المصادر الأجنبية:

1. Alina, C. M., Cerasela S.E., and Gabriela G, (2017) ,Internal audit role in cybersecurity ovidius university Annals Economic Sciences Series 17 (2) Pp. 510 – 513.
2. Al-Janabi, Saad Majeed, and Roish Ali Mashkor, 2022, Role of Financial Analyses by Liquidity Indicators in Diagnosing Banking Performance, Muthanna lournal of Administrative and Economic Sciences, Volume (12), Issue (2), Pages: 143-155.
3. Chandra،Vijaya, J., Challa, N., & Pasupuletti, S. K. (2019). "Authentication and authorization mechanism for cloud security". International Journal of Engineering and Advanced Technology, 8(6), 2072-2078.
4. Chaudhary A. Singh A. K. & Meena M. L., 2020, Productivity improvement of an electrical appliance industry by implementing lean manufacturing tools and a low-cost intervention (a case study). I
5. Christianto, A., Colin, J., & Gede Putra Kusuma Negara, I. (2024). Authentic Signature Verification Using Deep Learning Embedding With Triplet Loss Optimization And Machine Learning Classification. International Journal of Computing and Digital Systems, 16(1), 265-277.
6. Djouadi Abdelouahed, O. R. D. M. L. (2024). smartcard based cryptographique E-signature (Doctoral dissertation, faculté des sciences et de la technologie* univ bba).
7. Ege, O., Cagal, M., & Bicakci, K. (2025). Usability of Token-based and Remote Electronic Signatures: A User Experience Study. arXiv preprint arXiv:2505.18814.
8. Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. International Journal of Accounting Information Systems, 48, 100598.

9. Isono, I., Prilliadi, H., & Mahusin, M. Enhancing E-authentication and E-signature across ASEAN: Building Interoperable Frameworks for Seamless Digital Transactions, (2025).
10. Karonen, K. (2025). PDF advanced electronic signature with smart cards.
11. Krishnasamy, V., andVenkatachalam, S. (2021),"An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryptionalgorithm",Materials Today: Proceedings.
12. Liu, F., Zheng, Z., Gong, Z., Tian, K., Zhang, Y., Hu, Z., ... & Xu, Q. (2024). A survey on lattice-based digital signature. Cybersecurity, 7(1), 7.
13. Mijwil, M., Salem, I. E. (2023). "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity", A Comprehensive Review. Iraqi Journal For.
14. National Institute of Standards and Technology "NIST" (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
15. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. researchgate.net.
16. Oleksiv, N., & Nazarkevych, M. (2025). Development of a Biometric Electronic Signature based on Iris Features.
17. Pourteymour, S., & Shams Nateri, M. E. (2024). Electronic Signature and Crime Prevention. Journal of Criminal Law and Criminology, 12(23), 83-122.
18. Salin, H. and Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. J. Cybersecurity. Priv., 2, 276–291.
19. Shruti M, (2024) ,Types of Cyber Attacks You Should Be Aware of in 2025, https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks.
20. Stanešić, J., Morić, Z., Regvart, D., & Bencarić, I. (2025). Digital signatures and their legal significance. Edelweiss applied science and technology, 9(1), 403-412.
21. Tullis, C. (2024). Public Key Infrastructure: Implementing High-Trust Electronic Signatures. World Bank Digital Transformation white paper series.
22. Tullis, C., [Author 2], & [Author 3]. (2024, September). Electronic signatures: Enabling trusted digital transformation [Technical report]. Research Gate https://www.researchgate.net/publication/389571305