سبل الاستفادة من الحوسبة السحابية في حماية العمليات المصرفية الالكترونية

أ.د/ كتوس عاشور *
جامعة الشلف – الجزائر
أ/ **حسيني جازية** **
جامعة الشلف – الجزائر

Abstract:
The stunning and rapid deployment resulted in the Internet to fundamental changes in the nature of the work of the banking and financial sector, by providing modern mechanisms more flexible and dynamic and speed services Electronic banking has appeared and worked to make information and communication technologies in order to develop systems and means of provision of banking services, But safety became threatening any development bank transactions that are accompanied by the Internet and realized this item through many technological applications and new programs that appear every day However, whenever the sectors benefited from technological evolution appears to return a new type of hack for the confidentiality and security of this technology, in this study we focused on cloud computing technology and the security of electronic banking through which And the availability of adequate protection through applications for services provided by banks and Saudi Arabia has been a leader in applying this technique compared to other Arabic countries and the technology market expands from year to year.
Keywords: e-banking, Safety of Information, electronic banking operations ,clod computing

تمهيد:

أفرز التقدم التقني الهائل منذ انطلاق شبكة الانترنيت ما يعرف باسم العمل المصرفي الالكتروني، الذي يعتمد على المعالجة الالكترونية للبيانات مما يوفر مزايا هائلة في مجال الكلفة حيث انخفضت بشكل كبير ، فمثلا يقوم الصراف الآلي بعمل يغني عن اللجوء إلى افتتاح فرع

* أستاذ التعليم العالي بكلية العلوم الإقتصادية والتجارية وعلوم التسيير جامعة الشلف مايل Kettouche_achour@yahoo.fr
** أستاذة مساعدة قسم أ بكلية العلوم الإقتصادية والتجارية وعلوم التسيير جامعة الشلف مايل hdjazia@yahoo.fr

للمصرف ، كما أن استعمال البنك الالكتروني يوفر الوقت على المصرف و العميل ،و ينجز العمليات المصرفية بكفاءة إلا أنه و بالرغم من المزايا المتعددة للعمل المصرفي الالكتروني إلا أن هذا العمل محفوف بالمخاطر حيث أن هناك ارتباط وثيق بين العمليات المصرفية الالكترونية و أمن المعلومات و التي قد تؤدي إلى العبث في أرصدة العملاء ذاتها أو إجراء عمليات دفع أو تحويل إلكترونية مبتكرة من خلال حسابات العملاء، و لمواجهة هذه التحديات لم يكن أمام المصارف إلا العمل الجاد لقبول هذه المخاطر مما يستوجب عليها مسؤوليات كبيرة لمواجهتها من خلال تبني إدارة مخاطر شاملة .

و مما أضفى عليه التقدم التكنولوجي في الفترة الأخيرة ظهور ما يسمى بالحوسبة السحابية التي تسمح بإدارة عمليات البنوك الكترونيا دون الحاجة إلى بنية تحتية كبيرة ، بحيث يمكن للبنك أن يدير أعماله بتوفر تجهيزات محدودة و من أي مكان دون الحاجة إلى المقر كما تسمح تطويرّ أساليب الخزن و توفير المعلومات بسرعة حيث أن انتشار المعلومات المحوسبة أدى إلى أن تكون عرضة للاختراق لذا أصبحت هذه التقنية سلاحا ذو حدين تحرص المؤسسات و الهيئات على اقتنائه و توفير سبل الحماية له .

تهدف هذه الورقة البحثية إلى إبراز مختلف العمليات المصرفية الالكترونية التي تقوم بها البنوك الالكترونية و أهم وسائل الدفع الحديثة كما تهدف إلى إبراز المخاطر و الجرائم التي تتعرض إليها و كيفية معالجتها خصوصا باستعمال تقنية الحوسبة السحابية و مدى أمن هذه المعلومات في حال تطبيقها على البنوك الالكترونية تماشيا مع التطور التكنولوجي الحاصل .

و لدراسة هذا الموضوع يمكن طرح الإشكال التالي : **ما مدى مساهمة الحوسبة السحابية في تأمين و حماية العمليات المصرفية الالكترونية** و الذي يمكن الإجابة عليه من خلال المحاور التالية :

المحور الأول : ماهية الصيرفة الالكترونية .

المحور الثاني : مخاطر العمليات المصرفية الالكترونية و الجرائم الالكترونية .

المحور الثالث: أساليب تأمين العمليات المصرفية الالكترونية .

المحور الرابع :دور الحوسبة السحابية في تأمين العمليات المصرفية الالكترونية .

المحور الأول : ماهية الصيرفة الالكترونية

شهدت العقود الأخيرة تطورات تكنولوجية ،أحدثت تغيرات كبيرة في قطاعات النشاط الاقتصادي، و بالأخص على القطاع البنك، حيث شرعت مختلف البنوك بتكثيف الاستفادة من أحدث التقنيات الحديثة كتكنولوجيا المعلومات والاتصال، والحواسيب الآلية وكذلك شبكة الإنترنت وتطويعها بكفاءة عالية بغية ابتكار خدمات مصرفية مستحدثة وتطوير أساليب تقديمها سعيا منها لمواكبة التطورات الحاصلة في هذا النوع من الصناعة، يتم من خلالها الانتقال التدريجي من المصارف التقليدية التي لها وجود مادي ومعاملات تتبادل فيها المستندات و النقود المعدنية و الورقية إلى مصارف افتراضية على شبكة الانترنيت .

أولا - تعريف الصيرفة الالكترونية و تطورها التاريخي

عرفت الصيرفة الالكترونية من قبل وزارة التنمية الدولية البريطانية[1] على أنها الخدمات المصرفية المقدمة بدون فروع بنكية، أي تقديم خدمات مالية خارج الإطار التقليدي للفروع البنكية باستخدام تكنولوجيا المعلومات والاتصالات كاستخدام البطاقات، الهواتف النقالة و الانترنيت ،فالمقصود بالصيرفة الالكترونية هو إجراء العمليات المصرفية بشكل إلكتروني وبذلك فهي بنوك افتراضية تنشئ لها مواقع الكترونية على الانترنيت لتقديم نفس خدمات موقع البنك من سحب و دفع وتحويل دون انتقال العميل إليها،أما العمليات المصرفية الالكترونية فنعني بها قيام البنوك بتقديم الخدمات المصرفية التقليدية أو المستحدثة و ذلك باستخدام وسائط الاتصال الالكترونية إما بغرض تعزيز حصتها في السوق المصرفي أو لخفض التكاليف أو لتوسيع نطاق خدمتها داخل أو خارج حدودها الوطنية .

و ترجع نشأة الصيرفة الالكترونية إلى بداية الثمانينات تزامنا مع ظهور النقد الالكتروني[2] ، أما استخدام البطاقات كان مع بداية القرن الماضي، ففي فرنسا ظهرت على شكل بطاقات كرتونية تستعمل في الهاتف العمومي ، و في الولايات المتحدة الأمريكية ظهرت بطاقات معدنية تستعمل على مستوى البريد و ذلك في عام 1958حيث أصدرت american express أول بطاقة بلاستيكية، لتنتشر على نطاق واسع ، ثم قامت بعدها ثمانية بنوك بإصدار بطاقة Bank americanعام 1968 لتتحول فيما بعد إلى شركة visa العالمية ، كما تم إصدار في نفس العام البطاقة الزرقاء carte bleue من طرف ستة بنوك فرنسية ، وفي عام 1986 قامت اتصالات فرنسا france telecom بتزويد الهواتف العمومية بأجهزة قارئة البطاقات الذاكرة carte a memoire لتصبح عام 1992 كل البطاقات المصرفية بطاقات برغوثية carte apuces تحمل بيانات شخصية لحاملها .

و في منتصف التسعينات ظهر أول بنك الكتروني في الولايات المتحدة الأمريكية يميز بين نوعين من البنوك كلاهما يستخدم تقنية الصيرفة الالكترونية ،أما في السوق العربية فقد أدخلت البطاقة الممغنطة debit card عام 1981 من خلال البنك العربي الإفريقي في مصر ثم انتشرت بعد ذلك في معظم الدول العربية .[3]

ثانيا :مزايا العمليات المصرفية الالكترونية

يعتبر القطاع المصرفي سريع التأثير و الاستجابة للمتغيرات الخارجية ، لذا فظهور الانترنيت أدى إلى تغييرات جوهرية في طبيعة عمل هذا القطاع و أسهم في ظهور الصيرفة الالكترونية التي تتميز بما يلي[4] :

1- المزايا المتعلقة بالعملاء :

· منح العملاء قدرة أكبر لاختبار الخدمة المصرفية الأكثر ملاءمة لهم و هذه الميزة التي توفرها الانترنيت تعتبر نقلة نوعية في علاقة البنوك مع عملائها ، أي إذا كانت الخدمة المطلوبة غير متوفرة لدى البنك المختار على الانترنيت أو أن سعرها غير تنافسي فإن العميل سيتحول بسهولة إلى بنك آخر له موقع على الانترنيت .

· تقديم الخدمات المصرفية على طول أيام الأسبوع و على مدار 24سا /24سا ، بمعنى خدمة متواصلة 365 يوم في السنة .

· تمكين العميل من الاطلاع على الحساب بالإضافة إلى معرفة أسعار الفائدة و مواعيد استحقاق أقساط القروض .

· سهولة إجراء التحويلات المالية من حساب إلى آخر .

2 المزايا المتعلقة بالبنوك :

· إمكانية البنوك الاستفادة من البيانات المتوفرة لديها من عملائها وتحويلها إلى معلومات كاملة عنهم باستخدام برامج الكمبيوتر الخاصة بقواعد البيانات .[5]

· زيادة المنافسة بين البنوك ، مما يسمح لها بالتغلغل إلى أسواق جديدة و من ثم إلى زيادة انتشارها الجغرافي .

· إيجاد الولاء المصرفي للعملاء الحاليين للحفاظ عليهم من جهة و جذب عملاء مرتقبين من جهة أخرى.

· الميزات التنافسية التي يحاول كل بنك ناجح التميز بها في خدماته ، فاتصال الزبون ببنكه عبر الانترنيت يزيد حسب جودته و سرعته من تميز البنك و بالتالي زيادة قوته التنافسية .

· تساعد في تخفيض تكاليف الطرق الأخرى مثل الفروع البنكية الحقيقية.

· التسويق الإلكتروني كميزة عصرية و إستراتيجية تسويقية حديثة لها فوائد عديدة لا يمكن الإغفال عنها.

ثالثا : قنوات الخدمات المصرفية الالكترونية

1-آلات الصرف الآلي Automated Teller Macgines

بدأ استخدام آلات الصرف الذاتي عام 1967 بأحد فروع بنك باركلز بالمملكة المتحدة حيث كانت تسمح فقط بخدمة السحب النقدي ، و يعتمد مفهوم هذه الآلات على وجود اتصال بين الحاسب الرئيسي للبنك و آلة الصرف بحيث يمكن استقبال بيانات العميل بمجرد قيام العميل بإدخال البطاقة في الآلة لتقوم بعد ذلك بإعطاء استجابات فورية تتمثل في الخدمات المصرفية المطلوبة كالسحب النقدي ، الإيداع النقدي ، إيداع الشيكات ، كشف الحساب ، كما أضيفت إليها مؤخرا العديد من الخدمات الأخرى المتطورة مثل تحويل الأموال الكترونيا ، و لإتمام هذه الأعمال يزود العميل برقم سري للدخول على الآلة.[6]

2- البنوك المنزلية Home Banks:

هي عبارة عن استخدام الحاسب الآلي الشخصي للعميل وربطه مع نظام الحاسب الآلي بالبنك ،و يعتمد على فكرة تحويل البيانات من حاسب العميل إلى حاسب البنك والعكس وذلك من إشارات رقمية إلى موجات أو إشارات ضوئية (تناظرية) بواسطة أجهزة التحويل الخاصة بالحاسب (Modems) لتمر عبر وسائط اتصال متعددة إلى الحاسب الشخصي بمنازل العملاء ، ومن أمثلة وسائل الاتصال المستخدمة، الأسلاك المحورية، والموجات الهوائية والأقمار الاصطناعية والخطوط الهاتفية[7] .

3-الوحدات الطرفية عند نقاط البيع Point and Sale:

هي عبارة عن حاسبات آلية موجودة في المحلات والأسواق والمتاجر الكبرى والتي تكون على اتصال مباشر بالحاسب الآلي للبنك، حيث تجرى عمليات التحويل وإعادة التحويل عبر شبكة وقنوات الاتصال المختلفة، ومن خلال هذه الوحدات الطرفية يمكن إدخال قيمة مشتريات العميل لتخصم من رصيد حسابه مباشرة في البنك وإضافة القيمة إلى حساب المتجر في نفس البنك .

4-بطاقة الائتمان المصرفية Credit-Card : [8]

هي بطاقات بلاستكية تمنحها البنوك لعملائها ويتم استخدامها من قبل عملاء البنك لأغراض الشراء ثم التسديد لاحقاً، مع السماح له بتأجيل سداد الرصيد المدين لفترة معينة مقابل

فائدة، ، حيث يتم إنجاز الخدمات عبر عدة وسائل أهمها شبكات عامة ذات أقفال و شبكات هيكلية مثل internet والتي تستعمل أدوات إلكترونية متاحة للمستهلك مثل الحواسيب الشخصية، والهواتف المستندة للشاشات ، وأجهزة الاتصال الشخصية المماثلة للأخرى ،ومن أشهر أنواع البطاقات المستخدمة في هذا الخصوص كل من Master card، و Visa Card ولهذه البطاقات استخدامات معينة من أمثلتها : .[9]

أ - بطاقة الحساب:charge card

تتيح هذه البطاقة للعميل الشراء على الحساب مع التسديد لاحقاً بقيمة المشتريات ضمن الحد الأقصى المسموح به للعميل في البطاقة، حيث يتم لاحقاً التسديد عندما ترسل الفواتير المتعلقة بها.

ب- البطاقة المدينة Debit Card:

تتيح هذه البطاقة للعميل الشراء على الحساب مع التسديد من خلال السحب على حساباتهم الجارية في المصرف مباشرة، فإذا كانت البطاقة المدينة على الخط مباشرة في حال كون الجهاز مربوطاً بجهاز مركزي ، فإن تحويل قيمة المشتريات تتم إلى الجهة الدائنة خلال اليوم نفسه الذي تم فيه الشراء، أما إذا كانت البطاقة المدينة خارج الخط off line، فإنه يسمح بتسجيل العملية على أن تتم التسوية خلال أيام لاحقة ، وقد تطورت مثل هذه العمليات إلكترونياً بفضل أجهزة الربط الإلكتروني بين نقاط البيع والبنوك ، و أشهر هذه البطاقات تك الصادرة عن شركة فيزا العالمية تحت إسم (Visa electron)

ج -البطاقة الدائنة credit card:

يقوم هذا النوع من بطاقات الائتمان على مبدأ عدم الدفع المسبق لمصدر البطاقة كما في حالة البطاقة المدينة ولكن الاختلاف بينهما يكون في وقت دفع المستحقات، بمعنى أن حامل هذه البطاقة لا يدفع كل المستحقات المترتبة عليه في نهاية الشهر وإنما بشكل أقساط دورية متناسبة مع دخله الشهري وما يتبقى على حامل هذه البطاقة يعتبر ديناً متجدداً في ذمته تضاف إليه الفوائد وتسدد بشكل شهري .

د-البطاقة الائتمانية المضمونة Secured credit card:

هي بطاقة توفر للعميل خط ائتمان بضمان الودائع وتتاح للأفراد غير المؤهلين للحصول على البطاقة الائتمانية التقليدية بسبب افتقارهم إلى ماض ائتماني معروف أو أنهم مدرجون في شريحة ائتمانية متدنية بسبب مشكلاتهم المالية السابقة .

هـ-البطاقة المدفوعة مسبقاً prepaid card:

هي بطاقة تقوم على أساس إدخال أو تثبيت مبلغ محدد في البطاقة ويجري التخفيض التدريجي للمبلغ آلياً كلما تم الصرف واستعمال البطاقة، ومن أمثلة ذلك بطاقة النداء الهاتفية.

و-البطاقة الذكية Smart Card[10]:

هي بطاقة تفاعلية تتضمن ذاكرة دقيقة وشريط إلكترو -مغناطيسي قابل للقراءة إلكترونياً وبمقدوره التفاعل مع الوحدات الطرفية أو وحدات الصرف الآلي أو أية آليات أخرى للقراءة أو التسجيل، ويمكن للعميل شحنها بمبلغ معين من النقود وتخزين كافة البيانات الخاصة بحاملها وهي تغني عن حمل النقود وتسمح تلك البطاقات بالتعامل على شبكة الإنترنت وبهذا تتم الصفقة مخلفة ورائها خيارات أوسع للمخاطر .

المحور الثاني : مخاطر العمليات المصرفية الالكترونية و الجرائم الالكترونية

أحدثت العمليات المصرفية الالكترونية نقلة نوعية في المخاطر البنكية و جعلت البنوك تواجه تحديات جديدة في مجال التحكم في هذه المخاطر ، و التي تجمع ما بين المخاطر التقليدية للبنوك إضافة إلى المخاطر المتعلقة بالإستعمال التقني الحديث و ما يترتب عليه من تجاوزات يقوم بها بعض الأفراد للحصول على أموال غير شرعية من خلال قدرتهم على اختراق المواقع الالكترونية للبنوك الالكترونية .

أولا: مخاطر العمليات المصرفية الالكترونية

نشأت العديد من المخاطر مع تزايد نشاط البنوك الالكترونية و تنفيذ العمليات المصرفية الالكترونية مقارنة بالمخاطر المرتبطة بالعمل المصرفي التقليدي لذا وجب مراقبة مستوى المخاطر التي تحيط بالعمل ووضع الإجراءات الرقابية اللازمة للسيطرة عليها و إدارتها بطريقة سليمة ، و يمكن تصنيف هذه المخاطر ضمن مجموعات تتمثل فيما يلي[11] :

1-المخاطر التقنية و الأمنية : يحدث هذا النوع من المخاطر من احتمال الخسارة الناتجة عن خلل في شمولية النظام أو من أخطاء العملاء في استخدام بطاقة الاعتماد في برامج غير محمية، مما يمكن الآخرين من الاطلاع على قاعدة البيانات الشخصية أو من برنامج إلكتروني غير ملائم أو إمكانية الاختراق من قبل القراصنة Hackers لشبكة المعلومات .

2- المخاطر القانونية : تحدث المخاطر القانونية عندما لا يحترم المصرف القواعد القانونية و التشريعات المنصوص عليها أو عندما لا يكون هناك نظم قانونية واضحة بخصوص عمليات مصرفية جديدة ،خاصة المتعلقة بالتوقيع الالكتروني و إثبات الشخصية .

3- مخاطر التشغيل : تنشأ نتيجة عدم توفر وسائل التأمين الكافية للنظم أو عدم تصميمها أو انجازها أو نتيجة خطأ معلومات ، أو خطأ في تشغيل البرمجيات و تتمثل في عدم التأمين الكافي لنظم حسابات البنك مما يتيح إمكانية اختراقها من قبل أشخاص ، غير مرخص لهم بذلك ، حيث يتم التعرف على المعلومات الخاصة بالعملاء و استغلالها سواء كان ذلك من خارج البنك أو من قبل العاملين فيه .

4- مخاطر السمعة : يحدث هذا النوع من المخاطر في حالة توافر رأي سلبي اتجاه البنك نتيجة عدم قدرته على تقديم الخدمات المصرفية عبر الانترنيت وفق معايير الأمان و السرية و الدقة ، مع الاستمرارية و الاستجابة الفورية لمتطلبات العملاء .

5- مخاطر أخرى : على غرار البنوك التقليدية تتعرض البنوك الالكترونية كذلك إلى مخاطر الائتمان و مخاطر السيولة و مخاطر السوق بممارسته للعمليات المصرفية الالكترونية مع اختلاف حدتها بحسب طبيعة العملية .

ثانيا - الجرائم الالكترونية:

الجريمة الالكترونية هي الجريمة التي لا تعرف الحدود الجغرافية و التي يتم ارتكابها بالحاسب الآلي عن طريق شبكة الانترنيت بواسطة شخص على دراية فائقة بهما ،و قد كان لظهور وسائل الدفع الالكترونية عاملا مساهما في ظهور هذا النوع من الجرائم بحيث تكون معظم عمليات الاحتيال على مستوى الحسابات المصرفية الإلكترونية على اضطرار المستخدم إلى الإفصاح عن كلمة السر ومعلومات سرية من خلال رسائل خبيثة أو بسبب تعرض الحاسوب أو الهاتف الذكي لبرنامج خبيث مصمم لسرقتها.ويمكن تلخيصها فيما يلي :

1- انتحال شخصية الفرد : تتم عندما يستغل اللصوص بيانات (كالعنوان،و تاريخ الميلاد ، رقم الضمان الاجتماعي...الخ) شخص ما على الشبكة الالكترونية أسوأ استغلال من أجل الحصول على بطاقة بنكية ائتمانية، حيث أن تلك البيانات تمكنهم من التقدم بطلبات استخراج البطاقات البنكية عبر الانترنيت من خلال هيئات لا تتخذ إجراءات أمنية صارمة على الشبكة .

2-جرائم السطو على أرقام البطاقات :تزايد هذا النوع من الحوادث التي أعقبتها عمليات الابتزاز لإرجاع تلك الأرقام أو لعدم نشرها أو لعدم استخدامها .

3-غسيل الأموال : و هي عملية تحويل المصدر غير المشروع للأموال كالمخدرات إلى أموال مصدرها مشروع كالتجارة بالسيارات و أبسط الطرق لهذا هو سحب مبالغ كبيرة على دفعات من الصراف الآلي من بلد أجنبي ثم يقوم فرع البنك الذي سحب المبلغ من جهازه بطلب تحويل

المبلغ من الفرع الذي أصدر البطاقة فتتم عملية التحويل بخصم المبلغ من رصيد الزبون الذي يكون قد تهرب من دفع رسوم التحويل و استطاع غسل أمواله .

4- السلب بالقوة الالكترونية: حيث يتم استخدام الحاسب في التلاعب بالمعلومات و ذلك بإدخال بيانات زائفة من جانب المتحايل باختلاق دائنين كأجور يجب دفعها و اختلاق مدينين غير حقيقيين يجب عليهم سداد فواتير صادرة عن الحاسوب ، أما المدين المعتدى عليه فلن يتمكن من إثبات كونه غير مدين بوجود فواتير معلوماتية ، و هكذا يستغل المتحايل طرق الدفع الآلية للحصول على أموال غير شرعية .

تبني العمليات المصرفية الالكترونية من قبل العملاء ولاسيما باستعمال الهواتف النقالة على اسم مستخدم وكلمة سر لتسجيل الدخول والوصول إلى المعلومات الدقيقة والقيام بالعمليات المصرفية إلكترونياً وتحويل الأموال من حساب إلى آخر. ومع زيادة هجمات التصيد والبرمجيات الخبيثة التي تهدف إلى سرقة المعلومات عبر شبكة الإنترنت، باتت كلمات السر للعمليات المصرفية الإلكترونية غير موثوق فيها لأنّها لم تعد توفّر المستوى الصحيح من الأمن. لذا تعين على المصارف أن تعتمد سياسة أمنية جديدة لخدماتها المصرفية الإلكترونية والهاتفية للحد من مخاطر العمليات الإلكترونية أو الهاتفية إلى أبعد حد ممكن وزيادة نسبة لجوء المستخدم إلى هذا النوع من الخدمات. فالعمليات العالية القيمة وتلك التي تحتاج إلى عدم تنصّل المستخدم قد تتطلب أمناً أكثر تطوراً وتقدماً للتوقيع على المعاملة.

المحور الثالث : أساليب تأمين العمليات المصرفية الالكترونية

المقصود بأمن المعلومات هو مجموعة العمليات و الإجراءات و الأدوات التي تتخذها القطاعات و المنظمات لتأمين و حماية معلوماتها و أنظمتها ووسائطها من وصول غير المصرح لهم سواء من داخل القطاع أو من خارجه و توصف هذه العمليات بالاستمرارية في التطوير و المتابعة للمستجدات و الاستمرار في مراقبة و افتراض المخاطر و ابتكار الحلول لها .

فالمؤسسات تقوم بحماية تأمين معلوماتها من خلال [12]:

- اعتماد العمليات الأمنية التي تقوم بالتعرف على المخاطر .
- تكوين استراتيجيات لإدارة المخاطر و تطبيقها.
- اختبار تلك التطبيقات .
- مراقبة بيئة العمل للتحكم بالمخاطر .

الهدف من البحث في وسائل و أساليب أمن المعلومات هو ضمان توفير العناصر التالية لأية معلومات :

السرية أو الموثوقية : و تعني أن المعلومات المستهدفة لا يمكن الكشف عنها إلا عبر الأشخاص المعنيين بها ، بالإضافة إلى سرية و سلامة أماكن تواجد المعلومات و حفظها، لاسيما أن المعلومات تصنف إلى معلومات متاحة و موثوق بها، و سرية و سرية للغاية .

التكاملية و سلامة المحتوى: و تعني انه يجب التأكد من صحة محتوى المعلومات و لم يتم تعديله أو العبث به في أيه مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق التدخل الخارجي غير المشروع.

استمرارية توفر المعلومة أو الخدمة:و بالتالي استمرار عمل الأنظمة المعلومات و استمرار قدرتها على التفاعل مع المعلومات.

قدرة إثبات التصرف المرتبط بالمعلومات ممن قام به بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت ما.

كما يوجد عدة بروتوكولات من خلالها يمكن للبنوك الالكترونية أن تعمل من خلالها على حماية عملياتها المصرفية، و الحماية الحركات المالية الالكترونية.

أولا : أنواع بروتوكولات حماية العمليات المصرفية الالكترونية

يستخدم مصطلح بروتوكول في مجال الاتصالات بين الحاسبات الالكترونية، و هو مجموعة من القواعد و الأسس التي تحدد طريقة إرسال البيانات و انتقالها عبر خطوط الاتصالات من كمبيوتر لأخر، و كيفية استقبال هذه البيانات عندما تصل إلى محطتها الأخيرة . و تنقسم البروتوكولات إلى ما يلي :[13]

1- بروتوكول مراقبة البث و بروتوكول الانترنيت IP/TCP و يشملان قواعد أساسية حول كيفية نقل البيانات عبر الشبكة و كسرها و يضمان العديد من التطبيقات المتنوعة التي تقدم الخدمات للمستخدمين .

2- بروتوكول HTTP: و هو اختصار لـ (Hypertext Transfer) و هو بروتوكول الانترنيت المسئول عن نقل و عرض صفحات الويب،و يكون النقل تشعبي يسهل تحويلات آمنة بين المستخدم و الخادم ، باستخدام نموذج إدخال البيانات.

3- بروتوكول نقل الملفات FTP : ميزته أنه يتيح للعميل إرسال الملفات إلى كمبيوتر بعيد و يفرغ ملفات منه و يوفر طريقة للولوج إلى حاسوب مزود في شبكة الانترنيت بهدف جلب ملفات مخزنة فيه أو إرسال ملفات إليه .

4- بروتوكول المحافظة على المورد RRP: و هو بروتوكول يحافظ على عرض الشريك بالنسبة لإرسال Multimedia مثل مؤتمرات الفيديو و نفس البروتوكول يمكن استخدامه لأولوية البريد الالكتروني .

5- جدار النار Fire wall: هو برنامج يمكن تشغيله على نفس حاسوب خادم الويب أو حاسوب آخر مرتبط بخادم الويب و يمارس جدار النار عمله عن طريق إجراء عملية فحص لبروتوكول IP الجوالة بين خادم الانترنيت و الزبون ، كما يمكنه إعاقة و منع جميع محاولات الدخول إلى الشبكة المحمية بهذا الجدار الناري .

ثانيا : بروتوكول الحركات المالية الالكترونية الآمنة (SECURE ELECTRONIC TRANSACTIONS)[14]

طورت مجموعة من الشركات العالمية الرائدة بروتوكولا لعمليات الدفع أطلقت عليه اسم بروتوكول الحركات المالية الآمنة للحفاظ على أمن البيانات و التحقق من وصولها إلى الجهة المطلوبة أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الانترنيت و يستخدم برمجيات تدعى المحفظة الالكترونية و تحوي رقم حامل البطاقة و الشهادة الرقمية التابعة له ، أما التاجر فتكون له شهادة رقمية صادرة عن أحد البنوك المعتمدة و يستخدم كل من حامل البطاقة و التاجر الشهادة الرقمية التابعة له مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الانترنيت . و لا يمكن للتاجر مشاهدة رقم البطاقة الائتمانية أثناء جلسة بروتوكول الحركات المالية الآمنة حيث ترسل الصيغة مشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر ، و تضمن بهذا عدم عرض الرقم كما تمنع أي تعديل غير مرخص به أثناء إرسال البيانات .

ثالثا : أنظمة تشفير العمليات المصرفية الالكترونية

تعتبر حماية و تأمين المعاملات المالية من بيانات متدفقة من و إلى العملاء و أيضا أموال و بيانات تخص وسائل الدفع للبنوك الالكترونية ، من أهم التحديات و التي استوجبت وضع أنظمة تشفير لمجابهة كل الأخطار المحدقة بها و التي تقلل من كفاءتها ،
مما ينعكس على سمعتها و مردودها المالي و توجد العديد من أنظمة التشفير نذكر منها[15] :

1- نظام الدفع الافتراضي :و هو أول نظام يقدم الربط بين المصارف و شركات بطاقات الائتمان، و الشركات التي تقوم بأعمالها عبر الانترنيت و زبائن الانترنيت، و يتحقق النظام من صحة التحويلات، ويتضمن أنظمة مراقبة لتقصي المشاكل ضمن:

NET CASH : طوره معهد علوم المعلومات التابع لجامعة كاليفورنيا الجنوبية ، و هو نظام يعتمد على القسائم التي يجري التعامل بها عبر البريد الالكتروني و يصدر ET BANK المرتبط بـ NET CASH القسائم و يحولها مقابل عمولة 2% .

NET SHEQUE: هو نظام دفع الكتروني يحاكي الشبكات العادية، و تتم الترتيبات مسبقا للاشتراك في هذا النظام و يمكن تحويل الشيكات باستعمال البريد الالكتروني أو البروتوكولات الأخرى للشبكات .

NET BILL: هو نظام يسمح بإجراء الدفعات الالكترونية عبر الانترنيت، و يقدم كوسيلة لكسب المال عن طريق دفعات صغيرة كل مرة باعتماد أعداد كبيرة من التحويلات .

DIGI CASH : هو نقد الكتروني يجمع ما بين تحويل النقد المؤمن و الخصوصية و الأمن، و يعتمد على نظام التشفير للتعرف على الشاري .

2- البصمة الالكترونية :

هي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال التمويه و تستطيع هذه البصمة تمييز الرسالة الأصلية و التعرف عليها بدقة، حتى أن أي تغيير في الرسالة سيفضي إلى بصمة مختلفة ، و من غير الممكن اشتقاق البصمة الالكترونية ذاتها من رسالتين مختلفتين، و الجدير بالذكر أن استخدام خوارزمية البصمة الالكترونية أسرع من القيام بعملية التشفير اللامتماثل و لهذا تستخدم خوارزمية البصمة الالكترونية كثيرا في إنشاء توقيعات الكترونية .

3- التوقيع الالكتروني[16] :

هو توقيع مكون من حروف و أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني مرتبط برسالة الكترونية بنية توثيق أو اعتماد تلك الرسالة و التي تدل على شخصية الموقع دون غيره وأن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها .و هناك نوعين من التوقيع الرقمي ،التوقيع الرقمي " الكودي - ونجد استعمال هذا النظام في التعاملات البنكية وغيرها، وأوضح مثال عليه بطاقة الائتمان التي تحتوي على" رقم سري " لا يعرفه سوى العميل الذي يدخل البطاقة في ماكينة السحب، والتوقيع بالقلم الإلكتروني و الذي يتم عن طريق قلم إلكتروني حسابي يمكن عن طريقه الكتابة على شاشة الكمبيوتر، وهذا يتم باستخدام برنامج معين، هذا الأخير أي البرنامج يقوم بوظيفتين، الوظيفة الأولى تتمثل في خدمة التقاط التوقيع، أما الوظيفة الثانية تتمثل في خدمة التحقق من صحة التوقيع، ويطلق عليه التشفير البيومتري، وهو طريقة من طرق التحقق من الشخصية، عن طريق الاعتماد على الخواص

الفيزيائية والطبيعية والسلوكية للأفراد، وحاليا تستخدم هذه التقنيات بواسطة أجهزة الأمن والمخابرات كوسيلة للتحقق من الشخصية، وتحديد الاستخدام المرخص لها.

في أوروبا، تكثر المصارف التي تستخدم البطاقات البنكية الذكية مثل يوروباي وماستر كارد وفيزا وزودت عملاءها الذين يجرون المعاملات إلكترونياً بحلول لقارئ البطاقات الذكية. فمن خلال تمرير البطاقة في القارئ وتسجيل الرمز السري، تستطيع البطاقة أن تولّد كلمة سر لمرة واحدة فقط يستخدمها المستخدم النهائي ويسجل دخوله بها للتعريف عن نفسه أو التأكيد على معاملة إلكترونية.

يوفر هذا الحل مستوى الأمن نفسه الذي يوفره العالم الرقمي حيث يتعين على العميل أن يسجل رمزه السري لإجراء المعاملة بأمن في متجر أو عبر الصراف الآلي.وقد بات هذا النوع من الحلول مقبولا كثيرا في المناطق التي أصبحت فيها سوق البطاقات البنكية ناضجة. [17]

في المقابل، اختارت بعض مصارف المفاتيح الأمنية وهي أجهزة صغيرة تولد كلمة سر لمرة واحدة فقط عند الضغط على الزر مع الحرص على أن يكون الشخص الذي يجري المعاملة إلكترونياً صاحب الحساب المصرفي على اعتبار أنّه يحمل الجهاز. كما اختارت مصارف أخرى حل الرمز السري لمرة واحدة فقط بالرسائل النصية القصيرة حيث تُرسل كلمة السر لمرة واحدة إلى المستخدم في رسالة نصية قصيرة إلى هاتفه النقال . في الأشهر القليلة الماضية، لاحظنا زيادة نسبة الاهتمام في التطبيقات التي تخصّ العمليات المصرفية التي تتم عبر الهاتف النقال وتتضمّن مستوى عالياً من الأمن.

المحور الرابع :دور الحوسبة السحابية في تأمين العمليات المصرفية الالكترونية

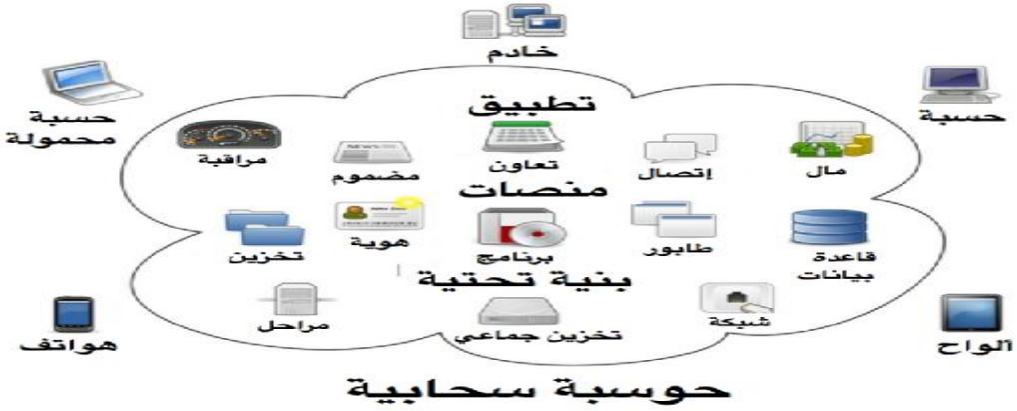
أولا :ماهية الحوسبة السحابية و خصائصها[18]

الحوسبة السحابية هي تقنية الخدمات الحاسوبية ضمن الانترنيت، و بتعريف أكثر وضوح و شمولية يمكننا القول أن تكون الملفات والجزء الأساسي من نظام التشغيل و البرامج على شبكة الانترنيت، و هو مصطلح يعكس مفهوما أو تصورا حول الخدمات و التطبيقات و البرمجيات soft ware و الأجهزة والعتاد hardware و المصادر التي تتوفر عن طريق الانترنيت و تدار من قبل طرف ثالث يدعى مقدم الخدمة provider في مراكز بياناته data centers ويحصل العميل و يسمى مشترك على كل ذلك أو بعضه وفق نظام الدفع بحسب الاستخدام و هو المعتمد غالبا، حيث تدفع الشركات لقاء حصولها على خدمة الحوسبة السحابية و يتم تقدير المقابل وفق ما يستهلكه كل عميل من إمكانيات المعالجة و مساحة التخزين و حجم الذاكرة و عدد العملاء المسموح لهم العمل و غير ذلك ، و بعبارة أخرى بدلا

من أن يستخدم الحاسوب للتواصل عبر الشبكة و تخزن عليها البرامج والملفات و غيرها ، يتم تخزين كل هذه الموارد على السحابة (أي مراكز البيانات) و يصبح الحاسوب أداة للتواصل مع هذه السحابة و هكذا الحال مع مختلف أجهزة الحاسوب الموجودة في شركة ما .

و يعرف المركز القومي للمعايير و التكنولوجيا NIST [19]الحوسبة السحابية على نموذج لتوفير وصول مناسب و دائم و في أي وقت إلى الشبكة ،لمشاركة مجموعة كبيرة من مصادر الحوسبة (الشبكات، الخوادم، وسائط تخزين البيانات، التطبيقات، الخدمات ...الخ) والحوسبة السحابية ليست جديدة تماماً ولكنها في السنوات الأخيرة باتت متاحة للمستخدمين خارج مراكز الأبحاث والشركات العملاقة، ويعود الفضل لعالم الكمبيوتر الشهير جون مكارثي [20] في تشكيل تعريف أو تصور مبدئي لفكرتها في فترة الستينيات حيث قال: «الحوسبة يمكن أن تُنظم ذات يوم بحيث تُعد مثل مؤسسة منفعة عامة» على غرار مؤسسات الخدمات (الماء والكهرباء)، وفكرته هذه تم البناء عليها وتطورت حتى وصلنا إلى الحوسبة السحابية التي بين أيدينا اليوم.

الشكل 1- رسم تخطيطي توضيحي لمكونات الحوسبة السحابية



المصدر : http// cloud-wd.com/cw/ articles

وكان لشركة أمازون دور كبير في تشكيل خدمات الحوسبة السحابية التي نتعامل معها اليوم حين أطلقت في العام 2006 خوادم الويب الخاصة بأمازون (Amazon Web Services). وفي 2007 ظهرت تطبيقات غوغل السحابية عبر بريد غوغل وتقويمه ومستنداته وبقية حزمة التطبيقات. وفي العام 2008 ظهر برنامج نيبولا (Nebula Open) الذي كان أول برنامج

مجاني يسمح للشركات الراغبة بتقديم خدمات السحب الخاصة والهجينة عبر الحوسبة السحابية، وكان له أثر كبير في مسيرة وتطور خدمات السحب الإلكترونية.

و لقد حدد المعهد القومي للمعايير و التكنولوجيا خمسة خصائص أساسية للحوسبة السحابية[21] :

01-الخدمة الذاتية بناءا على الطلب on demand self service ، المستفيد يتلقى الخدمة عند طلبه دون تدخل من المورد .

- الوصول الواسع للشبكات brodd network access ، وصول المستفيد إلى تلك الموارد عبر قنوات و منصات مختلفة مثل الكمبيوتر المحمول و اللوحي و الهاتف الجوال .

02- حزم الموارد resource pooling ،تقديم موارد الحوسبة للمستفيدين مختلفين تبعا لطبيعة كل منهم و تطبيقاته بمعنى تلبية احتياجاتهم على اختلاف اهتماماتهم .

03- المرونة مع السرعة rapid elasticity أي الاستجابة للتغير في احتياجات المستفيدين و بسرعة في الأداء .

04- قياس الخدمة mesured service الوقوف على مستوى خدمة الحوسبة السحابية حيث توجد أدوات لقياس استخدام الموارد ووسائط التحزين و التطبيقات و عدد المستفيدين في كل لحظة.

ثانيا : مزايا و عيوب الحوسبة السحابية[22]

هناك العديد من المزايا للحوسبة السحابية غير خدمة تخزين الملفات و أهمها :

- إمكانية استخدامها في ميدان التعليم بتكلفة صغيرة أو بشكل مجاني (الفصول الافتراضية).

-مزامنة الملفات : عند رفع ملف أو تعديله يمكن أن تصل إلى هذا الملف من أي جهاز حاسوب أو لوحي أو نقال تستخدمه .

- مشاركة الملفات : أن حجم الرسالة الالكترونية لا يمكن أن يتجاوز 25MB و هذا يعتبر مشكلة للأشخاص الذين يرسلون ملفات كبيرة لهذا يمكن رفع الملفات الكبيرة على مواقع التخزين السحابي ثم نقوم بإرسال رابطها عبر البريد الالكتروني .

- لا تحتاج الشركات إلى شراء عتاد جديد و بذلك تقلص حجم قسم تكنولوجيا المعلومات لديها .

- الحوسبة السحابية تسمح بالوصول إلى جميع التطبيقات من أي مكان وزمان عبر الانترنيت،لأن المعلومة غير مخزنة على القرص الصلب بل على خوادم الشركة المقدمة للخدمة.

- الاستفادة من البنى التحتية الضخمة التي تقدمها الخدمات السحابية للقيام بالاختبارات و التجارب العلمية فبعض الحسابات المعقدة تحتاج إلى سنوات لإجرائها على أجهزة الكمبيوتر العادية ، بينما تتيح شركات مثل جوجل و أمازون سحاباتها المؤلفة من آلاف الخادمات المرتبطة بعضها البعض لإجراء مثل هذه العمليات الحسابية في دقائق أو ساعات .

أما عيوب التخزين السحابي فتتمثل في:

- حاجة التطبيقات السحابية إلى الاتصال بالانترنيت ، حيث سيؤثر الانقطاع عن الانترنيت على إمكانية انجاز العمل ، لكن الشركات بدأت تتدارك هذا ، و بفضل تقنيات HTML5 و جافاسكربت الحديثة بات بالإمكان بناء تطبيقات ويب يمكن أن تعمل دون اتصال بالانترنيت ثم القيام بالمزامنة لدى عودة الاتصال ، لكن مازلنا بحاجة إلى المزيد من الوقت كي تتطور هذه التطبيقات و التقنيات بشكل آمن.

- مخاوف أمنية : يخشى البعض من وضع كل المعلومات و الملفات لدى الشركات المقدمة للخدمات السحابية ، فلو تعرضت الخدمة لعملية اختراق ناجحة ، قد يتمكن المخترق من الحصول على معلومات المستخدمين ، إضافة إلى إمكانية بيع معلوماتك من طرف الشركة المقدمة للخدمة أو الاستفادة منها ستشكل مشكلة حقيقية ، فالضمان الوحيد إذن هو اللجوء إلى الشركات الكبيرة الموثوقة و ذات السمعة الجيدة في هذا المجال .

ثالثا : تأثير تطبيق الحوسبة السحابية على مستوى البنوك الالكترونية

يعتبر تطبيق الحوسبة السحابية قفزة نوعية قي عمل المؤسسات بحيث يختبر قدرتها على التكيف مع التطور المستمر في تكنولوجيا المعلومات و الاتصالات فبرغم ما تمنحه هذه التقنية من تسهيلات في العمل و تخفيض في التكلفة إلا أنها لا تخلو من المخاطرة .

فالخدمات المصرفية المتاحة عبر الإنترنت يمكن أن تساعد المصارف في اختصار العديد من المنافذ والقنوات للعملاء،وعلى القدر الذي تتيحه هذه التطورات التقنية والسوقية المستقبلية في الخدمات المصرفية المتاحة عبر الإنترنت فإنه من المهم جداً أن تتجنب الجهات الإشرافية كل السياسات والممارسات التي يمكن أن تحول دون تحقيق الفوائد التي من أجلها تم تطوير تلك التقنيات والخدمات.

الأمن المعلوماتي واحد من أهم الموضوعات التي تشكل هاجسًا لدى المؤسسات المالية و المصرفية لاسيما مع تسجيل العديد من الهجمات الإلكترونية التي تسبب خسائر مالية كبيرة و بحسب شركة سيمانتك [23]الأمريكية لحماية الشبكة الإلكترونية فإن المعدل السنوي لكلفة الجرائم الإلكترونية حول العالم يبلغ 114مليار دولار .وأصدرت تقريرًا بعنوان «نورتون سايبركرايم

2011» وهو أكبر تقرير من نوعه حول كلفة الجرائم الإلكترونية، خلصت فيه إلى أن 431 مليون بالغ حول العالم كانوا ضحية للتهديدات الإلكترونية أي ما معدله مليون ضحية يوميًا .

وتدرك لجنة خبراء المعلومات بالقطاع المالي جيدا أن حماية بنية تكنولوجيا الاتصالات والمعلومات بالقطاع المصرفي والأنظمة المقترنة به من أهم أولويات التي تم وضعها في الاعتبار عند إطلاق حملة توعية وطنية حول أفضل ممارسات السلامة لعملاء المصارف؛ ويتم خلالها توفير أحدث المعلومات الخاصة بالسلامة من التهديدات ومناطق الضعف للجمهور عبر الهواتف النقالة ، وشاشات الصراف الآلي، وكشوف الحسابات المصرفية، والمواقع الإلكترونية ومن ضمن أفضل الممارسات التي يمكن استخدامها لحماية البيانات المالية على الإنترنت، التأكد من أن المصرف الذي يمتلك أحدث تفاصيل الاتصال الخاصة مع الاحتفاظ بهذه المعلومات في مكان آمن و حماية الرقم السري الخاص خلال إجراء المعاملات المصرفية عبر الإنترنت .

و تعتبر البلدان العربية من بين دول العالم التي تعاني من خسائر مهمة بسبب القرصنة الرقمية، لكنها لا تزال متواضعة مقارنة بما يحصل في الدول المتقدمة، وتقدر خسائر دول مثل السعودية والإمارات مابين 1 و3 مليارات دولار، والنوع الغالب هو قرصنة البرمجيات، أما في دول مثل مصر وتونس والمغرب والأردن فالخسائر أقل لسبب وجيه هو أن هذه الدول أقل اعتماداً على الإنترنت في تعاملاتها، فحكومات هذه الدول تبدأ أولى خطواتها في الإدارة الإلكترونية بخلاف ما هو قائم في دولة مثل الإمارات، وأيضاً أغلب الشركات في هذه الدول لا تولي أهمية كبيرة للتعامل من خلال الإنترنت إلا في مجالات ضيقة وقليلة، وهذه الأسباب تحد دون انتشار كبير للقرصنة .

يثير موضوع أمن معلومات السحب الإلكترونية الكثير من الجدل، فالبعض يرى أن المعلومات لا تكون آمنة إلا عند إدارتها في شبكة داخلية، والبعض الآخر يرى أن السحب الإلكترونية تستطيع توفير الأمن اللازم لضمان حفظ المعلومات وسلامتها،كما يمكن القول أن مشاكل أمن المعلومات في السحب الإلكترونية تأتي من جهتين: موفر الخدمة والعميل، لكن الحمل الأكبر دائما يقع على عاتق موفر الخدمة، فهو الملزم بتوفير بنية تحتية قوية وأدوات ومستودعات تخزين آمنة، خصوصا إذا ما كان سيأخذ مقابلاً ماديا عليها.

تطور استخدام تقنيات الحوسبة السحابية بشكل ملفت للنظر، فحجم هذه الصناعة وصل إلى أكثر من ثلاثة أضعاف خلال الخمس سنوات الأخيرة، حيث كانت قيمة هذه الصناعة في عام 2008 حوالي 46 مليار دولار، ويقدر أن تصل في عام 2015 إلى أكثر من 150 مليار دولار. كما يرتقب أن يأتي حوالي 50% من أرباح الحوسبة السحابية من الولايات المتحدة فقط، كما نجد في إحصائية لـ 2013 أن حوالي 40% من أنظمة خدمات العملاء المباعة

كانت مبنية على أنظمة الحوسبة السحابية و رغم هذا النمو في استعمال هذه التقنية في البنوك إلا أنها تواجه الكثير من التهديدات منها :

1- سرقة البيانات Data Breachesأو ضياعها Data Loss:

إن سرقة بيانات البنك الحساسة من أسوأ المخاطر التي قد يواجهها ، ووصول معلومات سرية عن العملاء و أرصدتهم المالية قد يشكل كارثة للبنك .أو حتى ضياع البيانات سواء بسبب مشاكل أو أخطاء مقدم الخدمة، أو بسبب اختراق مقدم الخدمة أو حتى اختراق المستخدم، يمكن أن يؤدي إلى مشكلة كبيرة، فعند لجوء البنك إلى تخزين برامجه و بياناته على السحابة الالكترونية يجب أن تكون مؤمنة لأن خسارتها يمكن أن تؤدي حتى إلى التعثر المالي أو إلى المسائلة القانونية أو حتى إفلاس البنك .

2- أخطار الموظفين Malicious Insiders:

أخطار الموظفين تشمل الموظفين الحاليين أو الموظفين السابقين، ممن لديهم صلاحيات الوصول إلى الأنظمة أو الشبكات الداخلية لمقدم الخدمة والمعرفة التامة لنقاط ضعفها، والذين قد يقومون باستغلالها بطريقة سيئة تؤدي إلى مضاعفات سلبية تؤثر على مقدم الخدمة وبالتالي المستخدم، سواء بقصد أو بدون قصد.

3- قلة الاهتمام والعناية Insufficient Due Diligence:

المميزات التي تقدمها الحوسبة السحابية جعلت الكثير من المنظمات تسارع إلى استخدامها بدون الفهم الكامل لما هم متوجهين له. هناك العديد من النقاط التي على المستخدمين فهمها قبل التحويل إلى الحوسبة السحابية، مثل إمكانيات التشفير، أنظمة الأمان، سرعة الاستجابة ... إلخ، وذلك للوصول إلى الاستخدام الأمثل والمقارب للتوقعات.

رابعا : تجربة البنوك السعودية في تطبيق الحوسبة السحابية

أسهمت مؤسسة النقد العربي السعودي بشكل فعال في إرساء قواعد البنية التحتية للمعاملات المصرفية الالكترونية في المملكة ، بحيث زادت الحاجة إلى تقديم خدمات مصرفية إلكترونية للزبائن ، و نتيجة النمو المتسارع في تكنولوجيا المعلومات و الخدمات الالكترونية ، عمدت مؤسسة النقد السعودي بالتعاون مع البنوك التجارية العاملة في المملكة إلى إيجاد أنظمة مدفوعات آلية متطورة و شاملة .

1- أنظمة المدفوعات الآلية في المملكة العربية السعودية[24]

أ- الشبكة السعودية للمدفوعات (span) : التي أنشئت عام 1990 و هي شبكة المدفوعات الآلية الوحيدة في المملكة العربية السعودية ، حيث تربط أجهزة الصرف الآلي و نقاط البيع في كافة أنحاء المملكة بشبكة مدفوعات مركزية تقوم بدورها بإعادة توجيه العمليات المالية إلى الجهة المصدرة للبطاقة سواء كانت بنكا محليا أو (visa) أو أمكس (AMEX)أو ماستر كارد (MasterCard)، و تسخر الشبكة السعودية للمدفوعات بأفضل التقنيات في سبيل تقديم خدمات آلية تمتاز بالسرعة و الدقة و الأمان .

ب- نظام المقاصة الآلية للشيكات الذي عرف ارتفاعا ملحوظا خلال السنوات الأخيرة و بناءا على التقارير المقدمة من مؤسسة النقد السعودي نجد أن عدد الشيكات المنفذة من خلال المقاصة الآلية في غرف المقاصة الرئيسية بلغ في سنة 2011ما قيمته 2.3 مليون شيك أي ارتفاع بنسبة 1.8 % لتصل في سنة 2014 إلى نسبة 2.8 % .

ج-النظام السعودي للتحويلات المالية السريعة (SARIE): تم تشغيل هذا النظام و المعروف اختصارا بسريع في 1997و هو من أحدث نظم المدفوعات و التسويات البنكية في المملكة العربية السعودية في مجال الأعمال المصرفية الالكترونية ، و هو نظام متكامل للتسويات الإجمالية الآنية لكافة المصارف المحلية فيما بينها بالريال السعودي بصورة فورية من خلال حساباتها لدى المؤسسة و لها حرية الوصول لحساباتها و ضمان انجاز الدفع مع عدم قابلية النقض و تسوية المدفوعات ذات الاستحقاق الآجل ، و يدمج نظام سريع نتائج المقاصة و التسوية لجميع الأنظمة القائمة و هي الشبكة السعودية للمدفوعات (Span) و نظام سوق الأسهم السعودية الآلي تداول (Tadawul) و غرف المقاصة الآلية (ACH) و في مركز موالي موحد يتم من خلال تنفيذ التسويات بين المصارف .و يعمل هذا النظام على مساندة تحويل الأموال على نطاق دولي بصياغة وسائل الدفع طبقا للمعايير الدولية المستخدمة في شبكة سويفت و يشمل عددا من المعايير و الإجراءات الأمنية المتقدمة .

د-نظام دفع الفواتير الكترونيا : قد بدأ العمل بنظام السداد في أكتوبر 2004 و هو نظام مركزي لعرض و دفع الفواتير و المدفوعات الأخرى الكترونيا في المملكة العربية السعودية ، مهمته تسهيل دفع فواتير الكهرباء ، فواتير المياه .

2- أهمية الحوسبة السحابية في البنوك السعودية

مثلت قيمة سوق الحوسبة السحابية [25]على مستوى العالم أكثر 1.9 تريليون دولار في سنة 2012 ، و لتصل للضعف في سنة 2014 أي نحو 3.8 تريليون دولار.أما في المملكة

العربية السعودية فقد استمر الإنفاق من قبل السلطات على الحوسبة السحابية في الزيادة بشكل ملحوظ من 26.34 مليون دولار في عام 2013 إلى 40.3 مليون دولار في عام 2014. ومع استمرار مقدمي الخدمات السحابية العالميين في توسيع تواجدهم بالمملكة، وبخاصة من خلال الشراكات، [26] استفادت قطاعات مثل التعليم والرعاية الصحية والخدمات المصرفية والمالية والتأمين وشركات الاتصالات في تبني الخدمات السحابية، بينما اعتبرت المنشآت الحكومية أكثر تردداً بشأن أمن تقنية المعلومات والجوانب الخاصة بالسيطرة على الخدمات السحابية.كما تطور سوق الاستعانة بخدمات المصادر الخارجية بالمملكة إلى 16.3% في عام 2014 مقارنة بـ2013، ، ومن المتوقع أن يرتفع الإنفاق على خدمات الحوسبة السحابية إلى 52.9% خلال السنوات القليلة القادمة ، وذلك على الرغم من ضعف القاعدة الأساسية، جاء ذلك في تقرير حديث صادر عن شركة IDC العالمية للأبحاث ، ويعود ذلك إلى تميز المنشآت السعودية ببطئها في الانفتاح على مفهوم الاستعانة بخدمات المصادر الخارجية والخدمات المدارة، وذلك بسبب رغبتها في الحفاظ على قدرتها على التحكم بمهام تقنية المعلومات الخاصة بها بشكل كامل، في ظل تزايد المخاوف بشأن أمن تقنية المعلومات .

وعلى الرغم من أن المنشآت السعودية قد عبرت عن استمرار مخاوفها بشأن أمن تقنية المعلومات بتفضيلها لاستخدام حوسبة سحابية خاصة بداخلها، فقد لاحظت IDC[27] أن قلة فقط من هذه المنشآت قد أحرزت تقدماً بتحويل بنياتها التحتية الافتراضية إلى بيئات سحابية خاصة ومتكاملة،و أصبحت التوقعات التجارية وإدارة المخاطر واعتبارات تقليل التكلفة من أهم المخاوف على مستوى المؤسسات ، إلى حد أنها تدفع الرؤساء التنفيذيين السعوديين لتقنية المعلومات لوضع استراتيجيات خاصة بالحوسبة السحابية وتحديد أعباء العمل والنماذج الملائمة لمنشآتهم، في ظل بدء المنشآت السباقة بالحصول بشكل بطيء على المزايا التي توفرها خدمات الحوسبة السحابية.

إن مستقبل البنوك في المملكة السعودية بات مربوطاً بالتقنيات الحديثة كالحوسبة السحابية والحوسبة الذاكرية والحلول النقالة، في وقت توقعت فيه دراسة حديثة أن يصل إنفاق البنوك على تقنية المعلومات في نهاية عام 2015 إلى نحو 180 مليار دولار. وفيما لا تستحوذ الخدمات المستندة إلى السحاب الإلكتروني حالياً إلا على جزء يسير من هذا الإنفاق، تشير بعض التقديرات أنه خلال نفس السنة سيكون الإنفاق المتوقع من شركات الخدمات المالية على الحلول السحابية سواء كانت العامة أو الخاصة أو الهجينة، سيبلغ 26 مليار دولار . وقد دعمت هذه الفكرةَ دراسة استطلاعية حديثة أخرى أعدتها «برايس ووترهاوس كوبرز[28]» واستهدفت المديرين التنفيذيين في قطاع الخدمات المالية، إذ أن 71 % منهم إنهم سوف

يزيدون استثماراتهم في الحوسبة السحابية ، بعد أن كان 18% فقط من المستطلعة آراؤهم في دراسة 2012 قد قالوا الشيء نفسه. وإضافة إلى ذلك، قال نصف المشاركين في الدراسة إنهم يخططون للاستثمار في تقنيات السحابة الخاصة. إلا أن البنوك السعودية بحاجة إلى التعرف على الإمكانات الهائلة التي تتيحها التقنيات المبتكرة، بحيث أن الافتقار إلى المرونة، ونقاط الفشل المتعددة و البنى التحتية المعقدة، فضلاً عن التكاليف الكبيرة للصيانة والخبرة، أمور لا يمكن تجاهلها.

أي تكنولوجيا حديثة تقدم لنا الكثير من المزايا إلا أنه لا يمكن تطبيقها مباشرة دون تحليل حجم المخاطر التي يمكن تكبدها من جراء تبنيها و خاصة في القطاع البنكي باعتباره قطاع حساس يتأثر بسرعة و يؤثر في باقي القطاعات و دولة كالمملكة السعودية قد مرت بتجربة سيئة في هذا المجال و ذلك خلال سنة 2012 [29]بما سمي بهجمات "شمعون" على شركة "أرامكو" السعودية و "راس غاز" بحيث اعتبر بمثابة تحذير جدِّي. وأن قضية أمن تقنية المعلومات ستظل تشكل أولوية لمعظم المؤسسات ، و أمن تقنية المعلومات سيصبح ليس فقط مجالًا رئيسيًا للاستثمار للرؤساء التنفيذيين لتقنية المعلومات في المملكة السعودية ، وإنما عاملًا مؤثرًا كذلك على كافة قرارات الاستثمار على التقنية في السنوات المقبلة. وتتوقع IDC أن الإنفاق على برامج أمن تقنية المعلومات في المملكة سيرتفع بمتوسط نمو سنوي مركب 16.10% خلال الفترة من 2012 إلى 2017..و 40.37 % حتى العام 2018، بينما يتوقع نمو خدمات الحوسبة السحابية الخاصة بمعدل 40.7 % وخدمات الحوسبة السحابية الخاصة الافتراضية بمعدل 67.7 % خلال الفترة نفسها.

الخاتمة

لقد أتاحت الصيرفة الالكترونية للمصارف خدمات متطورة استطاعت من خلالها تخفيض التكلفة و زيادة حجم السوق المستهدف من خلال الخدمة المصرفية عن بعد بمختلف أنواعها، كما أثر ذلك على عملاء المصارف من خلال تخفيض تكلفة الخدمة المصرفية و السرعة و الفعالية، و بدون الانتقال إلى المصرف، كما صاحبت هذا التطور الحاصل على مستوى العمليات المصرفية الالكترونية مجموعة كبيرة من المخاطر كان على البنوك إيجاد الموازنة بين الأرباح التي تجنيها من تبنيها للتكنولوجيا الحديثة و المخاطر التي يمكن أن تقع فيها مما ينتج عنه من خسائر تضر بالبنك .

و من خلال هذه الدراسة تم التوصل إلى النتائج التالية :

· وجود تنوع و تعدد في الخدمات المصرفية الالكترونية التي تقدمها البنوك في الوقت الراهن مثل بطاقات الدفع الالكترونية بأنواعها و الخدمات المصرفية عن بعد .،و خدمات الصيرفة المنزلية ، سواء على المستوى العالمي أو حتى على المستوى العربي لكن بدرجة تطور أقل .

· على الرغم من الخدمات المتطورة التي تقدمها المصارف الالكترونية إلا أنها لم تحض بالثقة الكاملة من قبل العملاء بسبب التشكيك في أمن المعلومات و مدى قدرة هذه المصارف للمحافظة على خصوصيات بيانات العملاء .

· تقنية الحوسبة السحابية تعطي للبنوك القدرة على الاستجابة بسرعة لتغيير السوق و العملاء و الاحتياجات الالكترونية، و فكرة توسيع أو تضييق نطاق التكنولوجيا متوقفا على متطلبات البنك وتكون القدرة على الاستجابة في حد ذاتها ميزة تنافسية ، فتطبيقات الحوسبة السحابية تسمح بالقيام بمختلف العمليات المصرفية الالكترونية من أي مكان و من أي حاسوب و بسعة تخزينية كبيرة و تكلفة أقل .

· تتعدد المخاطر عند تبني الخدمات المصرفية الالكترونية بحيث تضم مخاطر الصيرفة التقليدية إضافة إلى مخاطر أخرى تتمثل في المخاطر التقنية و الأمنية ،المخاطر القانونية ، مخاطر السمعة و مخاطر التشغيل و مخاطر الحوسبة السحابية .

· من المهم على المستخدمين معرفة عيوب ومخاطر خدمات الحوسبة السحابية بالإضافة إلى مميزاتها، ووضعها في الحسبان وقت اتخاذ القرار بالانتقال. الوقت الذي يستغرقه الشخص لمعرفة وفهم المخاطر التي قد يواجهها وكيفية تفاديها أو التصرف في حالة حدوثها قد يوفر عليه الكثير من الوقت والجهد والمال في حال حدوثها. هذه المعرفة قد تكون الفارق ما بين خسارة جزء بسيط من الاستثمار أو خسارة كامل الاستثمار.

· اعتمادا على حجم الأعمال المرتبط بالحوسبة السحابية، يمكن تفنيد ثلاثة عوامل رئيسية تعد هي العماد الرئيسي لعمليات التأمين الالكترونية لأي خدمة للحوسبة السحابية و هي :

× تشفير البيانات أثناء نقلها أو أثناء تخزينها هي العامل الرئيسي الأول، وينسلخ من هذا العامل بالضرورة حتمية وجود مفتاح رئيسي لفك التشفير حتى يمكن إعادة البيانات إلى وضع الاطلاع والقراءة وتشفير البيانات هي حائط الصد الرئيسي لهجمات المتطفلين .

× وفقا لمدى حساسية أي جزء من البيانات المخزنة في الحوسبة السحابية لابد من وضع نظام لتوثيق الدخول باستخدام كلمة مرور واسم مستخدم بمنتهى الدقة ودون ترك احتمالات لإنشاء كلمات مرور يمكن تخمينها أو اختراقها .

× يجب أن تكون هناك قائمة بأسماء الموظفين أو العملاء المسموح لهم بدخول بيانات الحوسبة السحابية ، ويجب أن يكون هناك لائحة صريحة بالتراخيص والصلاحيات الخاصة بكل موظف ومراجعة مدى تطابقها مع طبيعة عمله في المؤسسة.

بناءا على الاستنتاجات التي تم التوصل إليها يمكن تحديد عدد من التوصيات التي نعتقد بأنها ستساهم في دفع عملية التحول نحو الصيرفة الالكترونية و تضمن أمن العمليات المصرفية الإلكترونية في ظل تطور التقنيات التكنولوجية الحديثة :

· يتعين على المؤسسات المصرفية أن تراعي اتخاذ الإجراءات اللازمة للتحقق من الهوية و تفويض العملاء ممن يقومون بإجراء العمليات مع المصرف عن طريق الانترنيت .

· اتخاذ الإجراءات اللازمة الهادفة لحماية سلامة المعلومات الخاصة بالتعاملات المصرفية الإلكترونية و السجلات و المعلومات المرتبطة بها .

· العمل على إيجاد سبل تكنولوجية جديدة من أنظمة وبرمجيات ومعدات توفر الحماية الكافية من المخاطر التي تصاحب استخدام التكنولوجيا المصرفية وإجراء العمليات المصرفية عبر شبكة الانترنيت؛

· يتعين إعادة النظر في التشريعات القانونية و المالية العربية و توحيدها بما يتناسب مع طبيعة الصيرفة الالكترونية كما يجب وضع قواعد الإثبات القانونية للوقوف على مدى توافقها أو عدم توافقها مع المستجدات التكنولوجية الحديثة في ميدان المعاملات التجارية، حيث أن النصوص القانونية ما زالت تتعامل مع عناصر الكتابة والمستندات والأوراق والتواقيع والصور طبق الأصل من منظور يدوي بحت، وبالتالي فإنها لا تنطبق على الوصائل ذات المحتوى الالكتروني، ولا تعزز وتشجع عمليات التجارة الالكترونية.

· ضرورة إدراج عمليات الصيرفة الالكترونية في الأسواق المالية، وخاصة . في ظل تحول العديد من عمليات السوق إلى عمليات إلكترونية يؤدي المصرف دورا مهما في إتمام تنفيذها.

· يجب المحافظة دائما على أمن البيانات إذ تحتاج البنوك إلى المطالبة باتخاذ إجراءات السلامة الصارمة من الموردين وضمان تطبيقات جديدة تتوافق مع أحدث وأدق المعايير الأمنية. و هو ما يسمى باتفاقيات مستوى الخدمة ،بحيث تتأكد البنوك بأن التطبيقات والبيانات متوفرة دائما في حال وقوع كارثة طبيعية أو حدث لا يمكن التنبؤ به. فالبنوك في حاجة إلى اتفاقيات مستوى الخدمة تكون صارمة مع الضمانات.

الإحالات والمراجع:

[1] ليث محمود أحمد الحاج ،نظام الخدمات المصرفية الالكترونية عبر (sms) و دوره في تحقيق ولاء العملاء في البنوك التجارية الأردنية ، رسالة ماجستير ، جامعة الشرق الأوسط ،2012.

[2] مصطفى كمال السيد طايل ، الصناعة المصرفية في ظل العولمة ، اتحاد المصارف العربية ، 2009 ص66.

[3] رحيم حسين، هواري معراج، الصيرفة الالكترونية كمدخل لعصرنة المصارف الجزائرية أعمال الملتقى الوطني حول المنظومة المصرفية الجزائرية التحولات الاقتصادية- الواقع والتحديات- جامعة الشلف 14 ديسمبر 2004.

[4] بن عياد محمد سمير و سماحي أحمد .التكنولوحيا الالكترونية البنكية ضرورة أم حتمية بالنسبة للمؤسسات المصرفية الجزائرية، مقال منشور من خلال الموقع الالكتروني :

http//:*lbassair.net/Centre%20de%20téléchargement/../7.PD...*

[5] نبيل ذنون جاسم،مثال مرهون مبارك ، معيقات تطبيق الصيرفة الإلكترونية في القطاع المصرفي الحكومي،معهد الإدارة، بغداد، 2009/2008، ص06

[6] طه طارق ،ادارة البنوك و نظم المعلومات المصرفية ، الإسكندرية ، مصر ،2000.

[7] Capon , N., The marketing of Financial service Columbia University , (prentice hall Inc.,) 1992.

[8] فياض ملفى القضاة، ، مسؤولية البنوك عن استخدام الكمبيوتر كوسيلة وفاء، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة الإسلامية والقانون – جامعة الإمارات العربية المتحدة، 1 يوليو، 2000 .

[9] طوبيا، بيار أميل، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، دراسة تحليلية مقارنة منشورات الحلبي الحقوقية، بيروت، لبنان، 2000 .

[10] جلال عايد، وسائل الدفع الإلكتروني، دار الثقافة للنشر والتوزيع، رسالة ماجستير منشورة، الطبعة الأولى، عمان، الأردن، 2008.

[11] بن علي بلعزوز ، عبد الكريم قندوز، عبد الرزاق حبار ، إدارة المخاطر، الوراق للنشر والتوزيع ، الطبعة الأولى، عمان ،الأردن ،2013.

[12] أحمد السيد كردي مقال منشور بعنوان تحديد و إدارة المخاطر في الأعمال المصرفية الالكترونية من خلال الموقع الالكتروني : http:// kenanaonline.com/users/ahmedkordy/posts/283562

[13] طارق عبد العال حماد ، التجارة الالكترونية ، الدار الجامعية ، مصر 2005/2004 ص 732.

[14] عبد النافع ، بروتوكول الطبقات الأمنية ، الجزء الأول ، الاطلاع عليه على الموقع الالكتروني : http://www.startimes.com/f.aspx?t=10598934بتاريخ 2015/04/15.

[15] طلال عبود التسويق عبر الانترنيت ، دار الرضا للنشر ، سوريا ، الطبعة الاولى ،2000، ص103.

[16] منير الجنبيهي ، ممدوح الجنبيهي ، البنوك الالكترونية ، دار الفكر الجامعي ،الاسكندرية ،2005 ص 45.

[17] محمد إسماعيل ،مقال منشور بعنوان الحماية المصرفية في وجه الجرائم الالكترونية من خلال الموقع http://arabic.arabianbusiness.com/technology/electronics/2015/388405

[18] رشيد التلواتي ،مقال منشور بعنوان ماهو التخزين السحابي و أدواته ، كيف نستخدمه في التعليم ؟من خلال الموقع www.new-educ.com/% d8%a7%d9

[19] جودي منذر، مقال منشور بعنوان مفهوم الحوسبة السحابية ، المزايا و المساوئ من خلال الموقع www.syr-res/com/article/1809.htm

[20] جون مكارثي (1927 -2011) هو عالم أمريكي في مجال الحاسوب حصل عام 1971 على جائزة تيورنج لمساهماته الكبيرة في علم الذكاء الاصطناعي وله الفضل في اختيار لفظ الذكاء الاصطناعي .

[21] شريهان نشأت المنيري ، مقال منشور بعنوان الحوسبة السحابية، من خلال الموقع http://alabdulrazaq.blogspot.com/2012/04/blog-post.html

[22] مشاعل علي الزهراني، الحوسبة السحابية، بحث تخرج مقدم من قسم علم المعلومات جامعة أم القرى 2013

[23] شريف عبد الباقي ،طفرة تكنولوجية في حماية بيانات عملاء البنوك والتصدي لمحاولات القرصنة مقال منشور على الموقع الالكتروني http://www.ahram.org.eg/Index.aspx

[24] تقرورت محمد ، متطلبات تطوير المعاملات المصرفية الالكترونية في الدول العربية بالإشارة إلى حالة الجزائر ، أطروحة دكتوراه في العلوم الاقتصادية ، جامعة حسيبة بن بوعلي الشلف ،2014.

[25] 5 مليون دولار حجم الإنفاق السعودي على خدمات الحوسبة السحابية خلال عام 2015 مقال منشور من خلال الموقع الالكتروني :http://swiftnewz.com/?cat=17

[26] 52.9نسبة نمو الحوسبة السحابية في المملكة خلال 2014، مقال منشور على الموقع الالكتروني : www.alriyadh.com/914057

[27] 77.5 مليون دولار حجم الإنفاق السعودي على خدمات الحوسبة السحابية خلال عام 2015 ، مقال منشور على الموقع الالكتروني .http://swiftnewz.com/15462/

[28] برايس ووتر هاوس كوبرز أو PWC تعتبر واحدة من أكبر شركات الخدمات المهنية في العالم. تأسست في 1998. تكونت الشركة إثر اندماج برايس ووتر هاوس مع كووبر وليبراند ،كان إجمالي إيرادات PWC للسنة المالية 2008 ما يقارب 28 مليار دولار أمريكي، وتوظف ما يقارب 164 ألف موظف في 150 دولة.

[29] توقعات عام 2014 لقطاع تقنية المعلومات و الاتصالات في السعودية مقال منشور على الموقع الالكتروني : http://www.themenatech.com/mena- ws/%D8%AA%D9%88%D8%A9. 3pYt.dpuf