1.4 تطوير البنية التحتية للمفتاح العام في المعاملات المصرفية عبر الانترنت.

هدف البحث إلى تطوير بنية المفتاح العام التحتية بصورة كبيرة و مميزة و تأمين المعاملات المصرفية عبر الإنترنت. وحرص على تطوير خدمات التجارة الإلكترونية و زيادة القبول على استخدامها و زادت انتاجيتها و كفاءتها حيث انتشرت التجارة الإلكترونية بصورة كبيرة في دول العالم.

وهدف البحث أيضا إلى تطبيق النظام في السودان بصورة خاصة و ذلك بهدف تطوير التقنيات الإكترونية في المعاملات المصرفية بين البنوك على قطاع محلي و دولي، حيث حرص على توضيح كيفية بناء المفتاح العام و كيفية توثيقه والتأكد منه ومن مستخدمه باستخدام الشهادات الإلكترونية المصدقة من قبل جهات معينة باعتبارها طرف ثالث في عملية التأمين. وكان له الدور الأكبر في هذا البحث حيث تمت الاستفاده منه في إنشاء الشهادات الإلكترونية والمفاتيح الخاصة بها المستخدمة في الولوج إلى النظام .

Software SecurityModule Ssm (2010) 2.4

هدف البحث إلى توفير وسيلة تأمين أمن مقبولة ورخيصة وإعداد نماذج لخدمات تامين المُعاملات الإلكترونية و تمكين النماذج من التحكم في مُستويات أمن وحِماية البيانات. عن طريق تصميم نماذج التأمين البرامجية التي توفر مجموعة من الخدمات لتأمين المُعاملات المصرفية وتم تطبيقها وإستخدامها في بيئة الصراف الآلى من خلال نظام تراسل يربط بين مخدم التراسل يمثل البنك و بيئة إفتراضية للصراف الآلى (Client) نتج عن ذلك الأتي:

تأمين التراسل بين البيئة الإفتراضية للصراف الآلى والبنك حيث تم توفير الخدمات التالية:

- تشفير الرسائل وفك تشفيرها.
- توليد قيمة هاش.
- توليد شهادة رقمية
- التحقق من الشهادة .

تم إضافة المرونة في إستخدام الخدمات السابقة علي النحو التالى:

- إمكانية التشفير فقط .
- إمكانية التوقيع فقط.
- إمكانية أن يكون التوقيع مرتبط مع الرسالة.

- إمكانية أن يكون التوقيع غير مرتبط مع الرسالة.
- إمكانية التشفير والتوقيع.

ركزت هذه الدراسة على تأمين المعلومات والمُعاملات الإلكترونية عن طريق تطبيق آليات مناسبة لحِماية المُعاملات الإلكترونية، و تطرقت إلى توليد الشهادات الرقمية دون الخوض في البنية التحتية للمُفتاح العام، كذلك لم يتم إستخدام الشهادات الرقمية في التشفير والتوقيع، و طُبقت الدراسة علي شبكة محلية. و لكن هذه الدراسة تتفق مع الإطار المقترح في تأمين المُعاملات عن طريق تشفير الرسائل وفك تشفيرها، توليد قيمة هاش، توليد شهادة رقمية و التحقق من الشهادة.

3.4 نموذج لتأمين صفحات الإنترنت (2009)

هدفت الدراسة إلى تصميم وتطوير إطار عمل بسيط وفعال لتأمين الصفحات الإلكترونية، ومن ثم تطبيق هذا الإطار على صفحة شركة بتروناس. من خلال تطبيق بروتوكول أمن الإتصال (SSL) لتوفيرالموثوقية عن طريق عملية تبادل الشهادات بين العميل والمُخدم، ففي التطبيق على حالة الدراسة (بتروناس) تم إنشاء الشهادة من دون الإستعانة بطرف ثالث، أما تكاملية البيانات فتم توفيرها بواسطة بروتوكول أمن الإتصال عن طريق عملية التشفير التي يقوم بها بواسطة الخوارزميات الموجودة فيه؛ ففي حالة الدراسة (بتروناس) تم التطبيق الفعلي للتشفير بخوارزمية (AES)، أما التشفير غير المُتماثل فقد تم بواسطة خوارزمية (RSA). وخِدمة السرية الثالثة التي يوفرها بروتوكول أمن الإتصال وهي تكاملية البيانات تم الحصول عليها بإرسال مَستخلص للرسالة (MAC).

أما في تطبيق سرية خدمات الويب على حالة الدراسة (نموذج لتأمين الصفحات حالة دراسة (بتروناس))، فقد تم تصميم نموذج مقترح للحِماية وذلك بإستخدام بروتوكول ال (SSL) و تطبيق خوارزمية (AES)، الذي يتيح بفتح إتصال آمن (Secure Connection) بين طرفي الإتصال – بالإضافة إلى الحِماية التي تدعمها بيئة العمل (Zend Framework) الذي يوفر حِماية من عدد من الهجمات (Attacks) حيث أنه في حالة الدراسة هذه تم إختبار الهجمة المسماة ب (SQL Injection) وفي هذا البحث أيضا تمت محاولة لتطبيق إحدى وسائل ال (web services security) وفيها تم التوصل إلى مرحلة توليد الطلب والاستجابة (Request and Response) وتوليد ختم الوقت (Time Stamp) مُتضمنة (Token) والتي بواسطتها يمكن إضافة التوقيع الرقمي (Digital signature).

ولكن هذا الإطار يختلف عن الإطار المقترح في أنه تم إستخدام نظام التشغيل Windows server 2003، ولم يستخدم طرف ثالث في التوقيع علي الشهادة، كما انه يُركز علي تأمين الويب؛ عن طريق تطبيق

آليات مناسبة للحِماية. وكذلك يتطرق للشهادات الرقمية بصورة عامة دون التخصص في البنية التحتية للمُفتاح العام. ولكنه يتفق مع الإطار المقترح في نقطة تأمينه للإتصال بإستخدام بروتوكول أمن الإتصال.

4.4 البنية التحتية للمفتاح العام (2009)

توضح الدراسة مفهوم البنية التحتية للمُفتاح العام حيث مثلتها بمجموعة من البرمجيات وتقنيات التشفير والخدمات التي تضمن للمؤسسات والشركات والجهات المختلفة أمن إتصالاتها وتعاملاتها على الإنترنت وذلك بتقديم وإنشاء مقترح أو إطار عمل يُمكن من تطبيق البنية التحتية للمُفتاح العام في السودان، وهذا المقترح تضمن:

- موقع إلكتروني آمن يعمل ببرتوكول (HTTPS) يمكن لأي شخص الدخول عليه والتسجيل فيه لطلب شهادة رقمية موقعة من سلطة الشهادات (Root CA).
- توليد شهادات رقمية للمُستخدمين
- إنشاء التواقيع الإلكترونية لأي ملف من قبل الأشخاص مالكي الشهادات الرقمية (مُستخدمي document signer).
- إستخدام أي من الشهادات الموجودة ضمن قائمة الشهادات الصالحة للإستخدام مع أي منها في التعاملات الإلكترونية.
- توفير حوار إلكتروني آمن (Secure Chatting) لأصحاب الشهادات الإلكترونية.

تختلف هذه الدراسة عن الإطار المقترح في إستخدام نظام التشغيل Windows XP، لم يتم التعامل مع مخدم خاص للتحقق من حالة الشهادة الرقمية ببروتوكول (OCSP)، كما أنه لم يتم إستخدام صلاحيات سلطة الشهادات (Root CA) في إعادة توقيع و إلغاء الشهادة ويختلف كذلك في التطبيق حيث تم توفير حوار إلكتروني آمن (Secure Chatting) لأصحاب الشهادات الإلكترونية في هذه الدراسة، بينما في الإطار المقترح تم إستخدام الشهادات الرقمية في توفير معاملات بنكية آمنة بين البُنوك و بين البُنوك والعُملاء و تضمين بنك السودان المركزي كسلطة لإصدار الشهادات (Root CA).