1.1 مقدمة البحث:

إن التجارة الإلكترونية والمعاملات المصرفية تتطلب التدابير الأمنية الصارمة والمشددة، ومن المعروف بأن استخدام الشركات للإنترنت كمنصة لممارسة أنشطتها التجارية سيرفع معدل نجاحهم لكن هناك المخاطر التي ستواجهها الشركة و أهمها انتحال الشخصيات وتغيير المعلومات الحساسة المتناقلة عبر الإنترنت أو التجسس عليها و هنا تظهر أهمية وجود بروتوكولات أمنية مشددة لحماية مصالحهم ، والخصوصية ،وتوفر الاتصالات الآمنة ، وقيمة التبادل ، وأصول المعلومات.

يعتبر رفع مستوى ثقة العملاء واحد من أهم مقومات التطبيق الناجح لخدمات البنوك الإلكترونية، ويأتي ذلك من خلال توفير وسائل تصديق إلكترونية عالية الكفاءة تمكن المتعاملين إلكترونياً من التحقق من هوية الطرف الآخر ، وتوفر الحماية لحقوق المتعاملين ، وذلك فإن آليات التصديق الإلكتروني بمختلف أنواعها ومستوياتها تلعب دوراً أساسياً لا غنى عنه ضمن منظمة البنوك الإلكترونية، وعليه فإنه من المهم فهم آلية عمل وسائل التصديق الإلكترونية وأساليب إدارتها بكفاءة حتى يُمكن توفير تعاملات آمنة للمواطنين والمؤسسات عبر الإنترنت.

بالرغم من وجود العديد من تقنيات التحقق من الهوية وخصوصا أساليب التحقق البيولوجي من الهوية (بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص)، تبقى كلمات السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعا للتحقق من الهوية، رغم أن هذه الأساليب بدأت تصبح أضعف وأضعف بتطور التقنيات التي يستخدمها الهكرز (مخترقي المواقع) لكشفها وخرقها. ومع ذلك، فهنالك الكثير من الوسائل التي يمكن استخدامها للحد من قدرة الهكرز على اختراق واكتشاف هذه الرموز. وتعتمد هذه الوسائل أساسا على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم. ولكن هذه التقنيات، ورغم قوتها، ليست حلولاً سحرية، إذ أنها تتطلب الكثير من المهارة والتخطيط الواعي قبل تطبيقها كي تحقق النجاح. وتتكون نظم التحقق من الهوية من ثلاث تقنيات هامة هي :

i. خدمات الأدلة Directory Services
ii. هيكلية المفاتيح العامة Public Key Infrastructure
iii. الشبكات الافتراضية الخاصة Virtual Private Networks

وتشكل هذه التقنيات الثلاث هيكلية شاملة للتحقق من هوية المستخدمين، وضمان تحديد حقوق النفاذ.

2.1 مشكلة البحث:

تتلخص مشكلة البحث في تأمين الأنظمة المصرفية لضمان سرية المعلومات وضمان عدم انتحال الهوية من قبل أشخاص غير مخول لهم لإجراء أي معاملات مصرفية داخل المؤسسة. الأمر الذي قد يؤدي إلى عدم ثقة العملاء بالجهة المصرفية وربما تلاعب أحدهم بحسابات بعض العُملاء.

3.1 أهداف البحث:

1. تصميم نظام صرافة و معاملات مالية.
2. حماية البيانات من العرض والتعديل الغير مصرح به أثناء التخزين والنقل.
3. تأمين النظام عن طريق الشهادة الموقع عليها من قبل طرف ثالث.
4. التحكم في الوصول وتوفير سبل الوصول إلى أطراف معينة دون غيرها.
5. تمكين المستخدم من التعامل الآمن في الإنترنت للنظام.

4.1 أهمية البحث:

تتضمن أهمية البحث في توفير الحماية والخصوصية والتكاملية لهذه المعلومات للوقاية من مخاطر تحريفها، باستخدام وسائل حماية أكثر فاعلية للمحافظة على تكاملية البيانات الإلكترونية للمؤسسات المصرفية

1. تتم عملية الحوالات المصرفية وإرسال المال عبرالإنترنت بصورة آمنة.
2. ألغى استخدام المفتاح العام (PKI) والمفتاح الخاص الخوف من مشكلة انتحال الشخصية، الأمر الذي وفر السلامة والأمن بالنظام.
3. تحقيق السرعة في القيام بالأعمال.
4. التحقق من هوية الشخص حسب ما تم تسجيله في شهادات السلطة (CA).

5.1 حدود البحث:

في هذا البحث يتم التركيز على تكاملية وسرية المعلومات والمعاملات المالية لضمان صِحتها وحِمايتها من أي تعديل بإستخدام الشهادات الرقمية .بالاضافة إلي التحقق من هوية المستخدم.

6.1 منهجية البحث:

يتّبع البحث المنهج الوصفي التحليلي حيث سيتم تحليل جميع العمليات المصرفية الخاصة داخل الصرافات والبنوك كمثال عملية تسجيل دخول الموظف للنظام وتحويل مبلغ نقدي من حساب شخص

لشخص آخر و تخزين البيانات الخاصة بهم ، وسيتم أولاً التحقق من الهوية وبعدها إجراء المعاملة بكل سرية وأمان.

7.1 هيكلية البحث:

يحتوي الباب الأول على مقدمة عن المشروع، توضيح المشاكل الموجودة في الأنظمة السابقة، الحلول والأهداف وأهمية البحث، إضافة إلى هيكلية البحث .

كما يتناول الباب الثاني وصف تفصيلي لمفهوم الصرافات ،وأمن المعلومات ،كما أنه يشتمل على تفصيل للبنية الأساسية للمفتاح العام.

يحتوي الباب الثالث الشهادات الرقمية ومكوناتها وأنواعها وحالاتها، كما يحوي التوقيع الإلكتروني، والفرق بين الشهادة الرقمية والتوقيع الرقمي .

كما يحتوي الباب الرابع على الدراسات السابقة التي تضمنت نظام الشهادة الرقمية أو استخدمت التوقيع الرقمي بأي شكل من الأشكال.

يحتوي الباب الخامس الأدوات والتقنيات المستخدمة في إنشاء النظام المقترح.

يحتوي الباب السادس على فصلين الفصل الأول به مقارنة بين النظام الحالي والنظام المقترح من حيث السرية التكاملية والسهولة وضمان سرية المعلومات بالنظام، أما الفصل الثاني فيتناول تحليل للنظام المقترح وعملياته.

كما يتناول الباب السابع تطبيق النظام المقترح.

يسرد الباب الثامن النتائج والتوصيات والخاتمة.