طريقة مقترحة لتأمين المدفوعات الالكترونية باستخدام بروتوكول التشفير Kerberos

A Proposed Method for Securing Electronic Payments using the Kerberos Encryption Protocol

حسن عبدالازل عبدالرزاق السيقل **د.محمد مهدي حسيني**

وزارة المالية /الدائرة الادارية / قسم المحاسبة

Hasanalsaiqal77@gmail.com

hosseini_mm@yahoo.com

رقم التصنيف الدولي ISSN 2709-2852

تاريخ استلام البحث : ٢٠٢٤/٧/٢٢ **تاريخ قبول النشر: ٢٠٢٤/٨/١٩**

المستخلص

نظراً لزيادة استخدام وسائل الدفع الالكتروني عبر تطبيقات الهاتف المحمول والمؤسسات المالية والمصارف ، يعاني مقدمو الخدمات المالية باستخدام الطرق الالكترونية للدفع من خسائر مالية فادحة وذلك بسبب عدم توفر الامان اللازم في الشبكات الخاصة بالدفع الالكتروني ، في هذه الدراسة تم توظيف تقنية التشفير وفك التشفير باستخدام بروتوكول (Kerberos) ، حيث تم استخدام التشفير المتماثل بالاضافة الى مركز توزيع المفاتيح في بروتوكول (Kerberos) كونه يتطلب تفويـــضاً ذو موثوقية عالية من الجهة الخارجية وذلك عن طريق التحقق من هوية المستخدم شريحة (SIM) للمصادقة ، بعد ذلك يتم اخذ دور مدير الثقة للتـأكد من هوية الطــرف

مجلة العلوم المالية والمحاسبية
ACCOUNTING & FINANCIAL SCIENCES JOURNAL

مجلة العلوم المالية والمحاسبية
العدد التاسع عشر/ ايلول ٢٠٢٥
الصفحات ٢٧ــ ٤٨

الاخر الموثوق منه ، أظهرت الدراسة تفوق الطريقة المقترحة في السرية ووالموثوقية وعدم التنصل بالاضافة الى عدم قابلية اعادة الاستخدام بالاضافة الى انخفاض الوقت المستخدم عن الطرق السابقة الى ٢٢.٥%

الكلمات المفتاحيةKerberos : ، التشفير ، فك التشفير ، الهاتف النقال

Abstract:

Due to the increased use of electronic payment methods through mobile applications, financial institutions, and banks, financial service providers using electronic payment methods suffer significant financial losses due to the lack of necessary security in electronic payment networks. In this study, encryption and decryption techniques were employed using the Kerberos protocol. Symmetric encryption was used in addition to the key distribution center in the Kerberos protocol, as it requires highly reliable authorization from an external party by verifying the user's identity using the SIM card for authentication. After that, the role of trust manager is taken to verify the identity of the other trusted party. The study showed the superiority of the proposed method in terms of confidentiality, reliability, non-repudiation, and non-reusability, in addition to reducing the time used compared to previous methods by 22.5%.

Keywords: Kerberos, encryption, decryption, mobile phone.

المقدمة:

تعد عمليات الدفع الإلكتروني من خلال الهواتف المحمولة إحدى أهم وسائل تحويل الأموال وتبادل القيمة بين الأفراد والمنظمات في العالم وأكثرها شيوعًا. ومع نمو إستخدام هذه الأساليب، زادت أيضًا الحاجة إلى رفع مستوى أمن المعلومات ونقل البيانات المالية عبر شبكات الاتصالات المختلفة وبناءاً على ذلك تم اعتبار التشفير أحد الأدوات الرئيسية لزيادة الأمان في نقل البيانات المالية والمعلومات بصورة عامة. ومع ذلك، فإن استخدام التشفير وحده لا يمكن أن يلبي جميع الاحتياجات الأمنية

الإنترنت اليوم يختلف عما تخيلناه. لقد أفلست العديد من شركات الدوت كوم المبكرة أو تمكن بعضها من جني الأموال عبر الإنترنت. هناك العديد من الأسباب لهذا الفشل، ولكن من أهم الأسباب المتبقية هي مسألة الدفع عبر الإنترنت [١] . هناك طلب متزايد على أنظمة الدفع الجديدة والمحسنة للتسوق عبر الإنترنت اوجدت وخارجه، هنالك ثلاثة عوامل رئيسية خلقت مطالب جديدة[٢].الأول هو وجود التكنولوجيا ووسائل المعلومات والاتصالات الحديثة يرغب الناس في جميع أنحاء العالم في التجارة مع بعضهم البعض يومًا بعد يوم وأكثر من أي وقت مضى. وقد أدى ذلك قيام العديد من شركات الدعم والخدمات اللوجستية في العالم بنقل المنتجات عبر الحدود الدولية ومع ذلك واجهت عملية الدفع مشاكل في مثل هذه الحالات ثانياً اوجدت طرق الدفع الإلكترونية الجديدة العديد من الفرص لخفض التكاليف. ثالثاً، أدت الخسارة الناجمة عن زيادة المبيعات عبر الإنترنت في السنوات الأخيرة إلى زيادة الطلب على طرق الدفع البسيطة والآمنة عبر الإنترنت[٣].يعتبر الهاتف المحمول احد اهم الوسائل تحويل الاموال واكثرها شيوعاً في العالم ، حيث يتم تناقل الاموال بين الناس والمنظمات ، ومع تزايد استخدا هذه الوسائل في التعاملات المالية بين المنظمات والاشخاص ، ظهرت الحاجة الى زيادة مستوى الامان ، ويعتبر التشفير أحد اهم الادوات الرئيسية لزيادة الامان في نقل المعلومات ومع ذلك لا يمكن للتشفير وحده ان يلبي جميع الاحتياجات لهذا الغرض فلذلك يتم استخدام بروتوكولات الامان التي تحسن عملية التشفير في هذا البحث سيتم استخدام بروتوكول التشفير. (Kerberos)

١- المبحث الاول/ منهجية البحث

١.١- أهمية البحث:

نظرا لأهمية الدفع عبر الإنترنت واهتمام المؤسسات والشركات بإنشاء أندية العملاء وتقديم مهرجانات الخصم وأكواد وصناديق مختلفة لمرة واحدة ومتعددة الاستخدام في منصات مختلفة مثل الكوبونات الإلكترونية أو كوبونات الهاتف المحمول والخصومات الإلكترونية و نقاط الولاء ، ومن ناحية أخرى ، زيادة معدل انتشار الهواتف المحمولة

بين الناس، ويبدو أن هذا المجال ينمو كثيرًا. ولذلك فإن العمل في هذا المجال يمكن أن يساعد في زيادة أرباح المنتجين وتشجيع العملاء على شراء المزيد.

٢.١- مشكلة البحث:

تكمن مشكلة البحث في الافتقار الى الامان اللازم عند نقل الاموال والمعلومات بين المنظمات والافراد والمصارف المالية المختلفة.

٢- المبحث الثاني/ الجانب النظري

في هذا الحانب سيتم تعريف متغيرات الدراسة وتشمل كل (الدفع الالكتروني ، المصرفة أو المؤسسة ، العميل أو الدافع ، التجار أو المستقبلون ، المشرع ، وأخيرا بروتوكول التشفير(Kerberos

١.٢- الدفع الإلكتروني:

يشير الدفع الإلكتروني إلى الدفع الذي يقوم به شخص ما إلى شخص آخر أو منظمة أو مؤسسة أخرى من خلال شبكة كمبيوتر دون اتصال مباشر. تشمل كافة طرق الدفع الإلكتروني أربع مجموعات وهي [٤].

١. المصرف أو مؤسسة:

إنشاء منصة دفع إلكترونية لإجراء عمليات الشراء. بمعنى آخر، يتم فتح حسابات الدفع الإلكتروني من قبل هذه المؤسسات.

٢. العميل أو الدافع: هناك مشترين يقومون بالدفع الإلكتروني أثناء تبادل السلع أو الخدمات.

٣. التجار أو المستقبلون: هناك أشخاص يتلقون المدفوعات الإلكترونية أثناء التعامل مع السلع والخدمات.

٤.المشرع: الجهات الحكومية التي تتحكم في عملية الدفع الإلكتروني خلال عملية تنظيمية خاصة.

يمكن إجراء الدفعات الإلكترونية بشكل مباشر أو غير مباشر. ففي الطريقة المباشرة توجد علاقة مباشرة بين المشتري والبائع، أما في الطريقة غير المباشرة فيتم الدفع من

خلال حساب بنكي ومن خلال وسيط بنكي، ويمكن أن يتم ذلك بطريقتين. أحدهما هو أن المشتري قد قام بالفعل بإيداع دفعة مقدمة في حسابه ليتم سحبها في وقت الشراء، كما هو الحال مع العديد من حسابات الموظفين المشروعة والحسابات المودعة مسبقًا. النموذج الثاني هو شكل من أشكال الائتمان يقوم فيه البنك بالدفع للبنك عند الشراء دون إيداع المبلغ في حسابه البنكي حتى يتمكن البنك من إرسال الفاتورة إلى العميل.

٢.٢- بروتوكول التشفير Kerberos:

هو بروتوكول مصادقة شبكة تم تطويره بواسطة معهد ماساتشوستس للتكنولوجيا (MIT) [٥] تم تصميم Kerberos لتوفير مصادقة قوية للعميل/الخادم و التطبيقات باستخدام تشفير المفتاح السري. من وجهة نظر المستخدم، فإنه لا يختلف كثيرًا عن عملية تسجيل الدخول العادية. لا يزال Kerberos يعتمد على قيام المستخدم بتقديم شكل ما من أشكال أوراق الاعتماد للتحقق من هويتهم. يتم تشفير تبادل بيانات الاعتماد في جميع أنحاء عملية المصادقة بأكملها بحيث تصبح آلية المصادقة آمنة. الاختصاص الفرق هو أنه بعد إثبات الهوية، يتم إصدار تذكرة مؤقتة للعميل[٦]. هذا و تتيح التذكرة للمستخدم الوصول إلى الأنظمة والتطبيقات الأخرى الموجودة داخل دائرة الثقة، أو بشكل أكثر دقة، يستخدم بروتوكول Kerberos تذاكر بصورة فريدة (unique)الذي يوفر مصادقة أسرع و يوفر أيضًا خدمات الأمان التالية: المصادقة المتبادلة والتحكم في الوصول المفوض والخصوصية و امن البيانات ، يحتوي Kerberos على ثلاثة كيانات أساسية العميل والخادم اللذين يريدان المصادقة عليهما ومركز التوزيع الرئيسي (KDC) وهو اختصار[7] (Key Distribution Center) ، (KDC)اشارة الى عملية تتكون من الخدمات: خدمة المصادقة (AS) وخدمة منح التذاكر (AS) .بالاضافة الى ((TGS يُصدر تذاكر منح التذاكر (TGTs) لمديرين معتمدين (أي المستخدمين والآلات الخدمات) للقبول في .TGS تصدر TGS تذاكر الدخول إلى الخدمات الأخرى في نفس المجال (domain)أو TGS في مجال آخر (other domain)موثوق به ومعرف فيما بينهم . يمكن أن تقبل أي وحدة تحكم أو

تتحكم المجال طلبات المصادقة وطلبات منح التذاكر الموجهة إلى مركز التوزيع الرئيسي (KDC) الخاص بالمجال (٣).يتمتع Kerberos بمزايا مقارنة ببروتوكولات المصادقة الأخرى، حيث لا تنتقل كلمة المرور مطلقًا خلال الشبكة حتى في شكل مشفر (ولكنها تستخدم التشفير/ فك التشفير بين العميل (agent) ومزود الخدمة (service provider))، يتكون البروتوكول من الخطوات التالية[٨][٩]:

١. يرسل العميل رسالة إلى مركز التوزيع الرئيسي (KDC) يطلب فيها إصدار TGT. الطلب يتضمن اسم المستخدم في شكل نص عادي للعميل، لكنه لا يتضمن كلمة المرور الخاصة به.

٢. يُصدر (KDC) TGT للعميل. يحتوي TGT على مفتاح الجلسة في شكل مشفر.لتشفير مفتاح الجلسة، يستخدم مركز توزيع المفاتيح (KDC) مفتاحًا مشتقًا من كلمة مرور العميل. هذا يعني أن العميل فقط يمكنه فك تشفير TGT وجلب مفتاح الجلسة.

٣. يقوم العميل بفك تشفير TGT واستخراج مفتاح الجلسة منه. العميل ثم المؤلفين طلب تذكرة الخدمة. تذكرة الخدمة صالحة فقط للتواصل بين طرفين، أي بين العميل والخادم.

٤. يقوم KDC بتأليف تذكرة خدمة للخادم. تحتوي هذه التذكرة على معلومات العميل بيانات المصادقة ومفتاح تشفير جديد، يسمى مفتاح الجلسة الفرعية. مركز السيطرة على الأمراض يقوم بتشفير تذكرة الخدمة باستخدام المفتاح السري للخادم (المفتاح السري مشترك السر بين KDC والخادم). وهذا يعني أن الخادم فقط يمكنه فك تشفير الملف تذكرة الخدمة.

٥. يقوم مركز التوزيع الرئيسي (KDC) بكتابة رسالة وتغليف تذكرة الخدمة بداخلها. مركز السيطرة على الأمراض أيضا نسخ مفتاح الجلسة الفرعية داخل الرسالة. لاحظ أن مفتاح الجلسة الفرعية موجود الآن

موجودة في الرسالة مرتين: مرة مباشرة في الرسالة ومرة أخرى داخل تذكرة الخدمة.

٦. يقوم KDC بتشفير الرسالة الكاملة باستخدام مفتاح الجلسة من الخطوتين ٢ و٣. وبالتالي، يمكن للعميل فقط فك تشفير الرسالة واستخراج مفتاح الجلسة الفرعية بالإضافة إلى ملف تذكرة الخدمة. لكن لا يستطيع العميل فك تشفير تذكرة الخدمة، ولا يستطيع ذلك إلا الخادم. ولذلك، لا يمكن لأي شخص آخر استخدام تذكرة الخدمة لأي غرض من الأغراض. ثم يرسل KDC الرسالة إلى العميل.

٧. يقوم العميل بفك تشفير الرسالة المستلمة من مركز توزيع المفاتيح (KDC) وجلب مفتاح الجلسة الفرعية داخل الرسالة وكذلك تذكرة الخدمة. يرسل تذكرة الخدمة إلى الخادم.

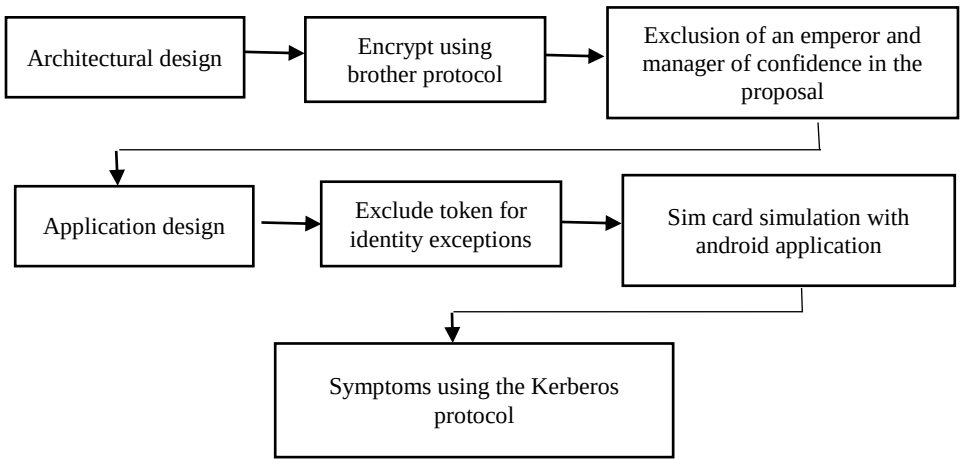
٨. يتلقى الخادم تذكرة الخدمة ويقوم بفك تشفيرها لجلب بيانات المصادقة الخاصة بها العميل الطالب وكذلك مفتاح الجلسة الفرعية. ثم يتعرف الخادم على طلب العميل، ويتم إنشاء جلسة آمنة جديدة بين العميل و الخادم. يمتلك كل من العميل والخادم الآن نفس مفتاح الجلسة الفرعية الذي يمكنهم استخدامه طلب العميل، ويتم إنشاء جلسة آمنة جديدة بين العميل و الخادم. يمتلك كل من العميل والخادم الآن نفس مفتاح الجلسة الفرعية الذي يمكنهم استخدامه من أجل التواصل الآمن مع بعضهم البعض.

يمكن للعميل تكرار الخطوات من أ إلى خ لتطبيق خادم آخر. هذا يعني ذاك يمكن استخدام خدمة Kerberos الخاصة بنا لمشاركة بيانات المصادقة وأن نفس العميل (الذي يمثل مستخدمًا واحدًا) يمكنه المصادقة باستخدام تطبيقات مختلفة. وهذا يتيح بشكل فعال الدخول الموحد.

٣- المبحث الثالث/ الجانب العملي

في هذا البحث، تم استخدام التشفير وفك التشفير باستخدام بروتوكول Kerberos والدفع عبر الهاتف المحمول مع كوبونات الهاتف المحمول. ولهذا الغرض، من خلال وضع مشغل الشبكة في دور مدير الثقة وإشراك بطاقة SIM للمصادقة، تمت محاولة زيادة الأمان مع الحفاظ على الكفاءة إلى حد كبير مقارنة بالطرق السابقة. يستخدم Kerberos تشفير المفتاح المتماثل ومركز توزيع مفتاح KDC يسمى مركز توزيع

المفاتيح. ولذلك، فإنه يحتاج إلى إذن طرف ثالث موثوق به لتأكيد هوية المستخدم. في هذا البحث، يتم أخذ دور بطاقة SIM في المصادقة ودور مدير الثقة للطرف الثالث الموثوق به. في هذا البحث، دعونا نستخدم مدير الثقة لتأمين كوبونات الهاتف المحمول. وبهذه الطريقة، يكون الشخص الثالث هو خادم مدير الثقة، أي بطاقة SIM. لذلك، فإننا نعتبر بطاقة SIM بمثابة وحدة آمنة ونقوم بتخزين المفاتيح فيها. باستخدام آلية المفتاح المشترك، يتلقى تجار التجزئة والعملاء مفاتيحهم المشتركة من المشغل ولا يقومون بإنشائها بأنفسهم. يوضح الشكل (٣-١) خطوات الطريقة المقترحة.



شكل (٣-١) خطوات الدراسة

١.٣- التصميم المعماري بالطريقة المقترحة

يتكون البروتوكول المقترح لهذا التصميم من أربع مراحل، باختصار هذه المراحل هي:

1) مرحلة الاتفاق والإعلان.

٢) مرحلة استلام نقاط الولاء وتحويلها إلى كوبونات للهاتف المحمول.

٣) مرحلة استخدام القسيمة.

٤) مرحلة تسوية الحساب.

كما أن لهذا البروتوكول أربعة أدوار رئيسية:

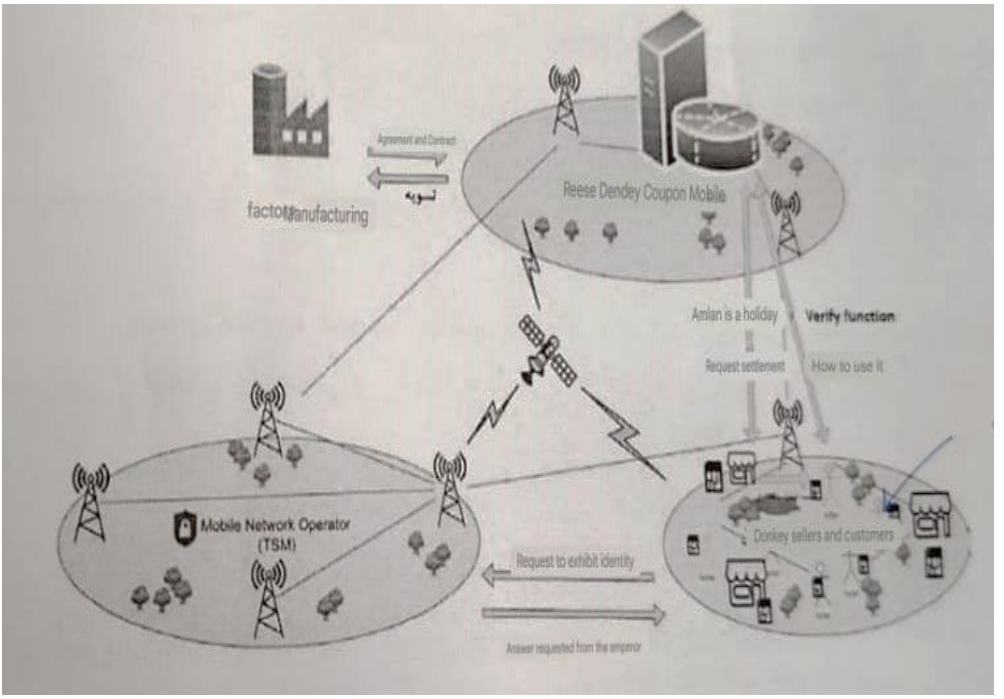
١) الموردين

٢) مزود خدمة القسيمة

٣) تجار التجزئة

٤) العملاء

ويتضمن التصميم الأولي نظام كسب نقاط الولاء وتحويل النقاط إلى كوبونات للهواتف المحمولة واستخدامها بطرق مختلفة. يتم إنشاء نقاط الولاء من خلال الجمع بين سلسلة من التجزئة على جانب واحد وسلسلة من التجزئة على الجانب الآخر. السلسلة الأفقية العلوية هي نفس السلسلة الأساسية الأصلية. لنفترض أن لدينا عدد n من العملاء ولا يتم إصدار أكثر من ٢٠ نقطة ولاء لكل عملية شراء. الصف الأول من المصفوفة هو القيمة الأولية للمولدw0 ، حيث يتم تطبيق وظيفة التجزئة الأولية على عدد العملاء. بعد الانتهاء من السلسلة الفرعية الأفقية الرئيسية، يأتي دور السلاسل الفرعية العمودية، حيث يتم تطبيق وظيفة التجزئة الثانوية عموديًا على المستويات على شكل تسلسل هرمي. وأخيرًا، أحد صفوف كل عمود من هذه المصفوفة يخص كل عميل قام بمعاملة ناجحة ويجب إرساله إليه:



الشكل (٣-٢) يوضح مصفوفة المستويات الهرمي

يتم الإعلان عن الخصومات. يتفاعل بائع التجزئة مع العميل من خلال إعلام العملاء بكيفية الحصول على نقاط الولاء وعروض الخصم. في الواقع، فإن بائع التجزئة، من خلال بيع سلع مخفضة، يدين للعميل بقسيمة من مزود الخدمة، وفي النهاية، سيقوم مزود الخدمة بتسوية مبلغ الخصم مع بائع التجزئة على فترات زمنية محددة في المستقبل. في المرحلة الثانية من البروتوكول ، بعد إتمام عملية الشراء لكل عميل من موقع البيع بالتجزئة الخاص بطرف العقد ، سيتم تخصيص عدد من نقاط الولاء للعميل. ويمكن للعميل تحويلها إلى قسيمة للهاتف المحمول من خلال توفير عدد معين من نقاط الولاء لمزود الخدمة. في المرحلة الثالثة يستخدم العميل كوبونات الهاتف المحمول ويلتزم تاجر التجزئة بقبول الاقتراحات التالية من العميل بعد التحقق من صلاحية الكوبونات. وأخيرًا، في المرحلة الرابعة، تتم التسوية بين مزود الخدمة وتاجر التجزئة، وينتهي برنامج الخصم.

٢.٣- تفاصيل تصميم النموذج:

١) اختيار الاتجاهات ونظام كسب نقاط الولاء: أولاً يقوم المستخدم بإدخال الاتجاه المطلوب من خلال الاطلاع على قائمة اتجاهات الخصم واختيار واحد منها. طريقة الحصول على نقاط الولاء هي أن يقوم بائع التجزئة أولاً بالاتصال بقاعدة البيانات. يتم فحص المصفوفة X بمؤشرينa ، b. بعد ذلك، يتم استلام المسار ذي الصلة بتنسيق السلسلة من خلال خدمة الويب كرقم درجة ولاء المستخدم من الرقم أ إلى الرقم ب من الدرجات في تطبيق المستخدم. هذا الخط هو في الواقع نفس رمز الخصم (نقاط الولا).

٢) تحويل النقاط إلى كوبونات للهاتف المحمول: يمكن للعملاء الاطلاع على قائمة نقاط الولاء المكتسبة. كما يمكنه أن يطلب من الخادم تحويل نقاطه إلى كوبونات في أي وقت. في الواقع، يتم إرسال طلب http يحتوي على سلسلة من رموز نقاط الولاء من العميل إلى الخادم. وبعد ذلك، من أجل التحكم، يتم إرسال طلب من الخادم إلى

بائع التجزئة ويتم التحقق من صحة الرمز. واستجابة لذلك، في حال تطبيق الرموز المقدمة، سيتم تفعيل زر استخدام الكوبون للعميل.

٣) استخدام قسيمة الهاتف المحمول: في تطبيق العميل، الضغط على زر استخدام القسيمة سيؤدي إلى تطبيق خصم على فاتورة العميل.

التشفير باستخدام بروتوكول:Kerberos

البروتوكول المقترح بإضافة دور المشغل الشبكة ومدير الثقة (SIM) الى خطوات العمل المقترحة.

٣.٣- الجزء الأول: تأمين الاتصال بين بائع التجزئة وخادم القسيمة من خلال مدير الثقة بناءً على عملية مصادقة Kerberos ومشاركة نفس مفتاح الأمان بين العميل والخادم، ويتم ذلك على مرحلتين المصادقة وإنشاء الثقة.

المرحلة الأولى: التحقق من الهوية

فيما يلي العملية الموضحة باستخدام دور بائع التجزئة كعميل وخادم :

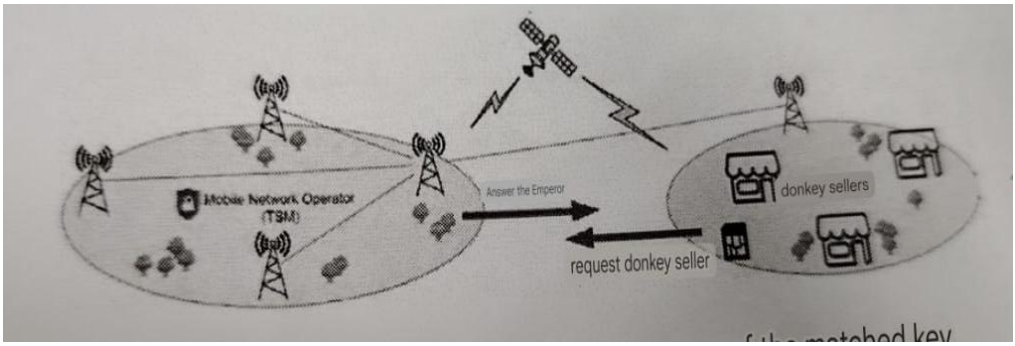
يتم من خلال العميل ينشيء اتصال آمن مع الخادم. يجب على كل من العميل والخادم استخدام بروتوكول مصادقة Kerberos للتأكد من هويتهما ، يستخدم Kerberos تشفير المفاتيح المتماثل. يتم استخدام مفتاح واحد للتشفير وفك التشفير. هنا يجب على الخادم التحقق من أن الرسالة التي أرسلها العميل مرسلة بالفعل من قبل نفس العميل. للقيام بذلك، يقرر العميل والخادم استخدام المعلومات الموجودة على مفتاح الأمان لمصادقة بعضهما البعض، لذلك يرسل العميل رسالة إلى الخادم. يرسل العميل رسالة تحتوي على اسم العميل بنص عادي والمصادقة مشفرة بمفتاح أمان. تحتوي رسالة التأكيد على بنية بيانات تتكون من حقلين. الحقل الأول هو اسم العميل والحقل الثاني هو وقت محطة عمل العميل. بعد أن يتلقى الخادم الرسالة، يستخدم نفس مفتاح الأمان لفك تشفير بنية بيانات المصادقة واستخراج معلومات العميل المطلوبة. بعد ذلك، يتحقق الخادم من الطابع الزمني مرة أخرى. إذا كان الاختلاف مقبولا. يدرك الخادم أن الرسالة ربما تم إرسالها من قبل العميل نفسه. إذا كان هناك اختلاف في

التوقيت، فسيرفض الخادم الرسالة تلقائيًا. عمليات التحقق من الصحة لها غرض آخر، وهو منع الهجمات المتكررة مثل هجمات إعادة التشغيل عندما يسرق أحد المهاجمين الرسائل أثناء الاتصال. من خلال تقديم نفسه كمستخدم رئيسي، يرسل رسالتين إلى الخادم. لكي يعرف العميل أن الخادم قد تلقى رسالته، يقوم الخادم بتشفير الطابع الزمني للعميل باستخدام مفتاح أمان ويعيده إلى العميل. نظرًا لأن الخادم يرسل فقط الطابع الزمني وليس جميع المعلومات الموجودة في مصادقة العميل، فيمكن للعميل التحقق من عدم تلقي أي شخص آخر غير الخادم رسالته لأن الخادم وحده هو الذي يمكنه فك تشفير معلومات الطابع الزمني واستخراجها. لذلك، في هذا البحث، ووفقاً للسيناريو المحدد لعملية المصادقة بواسطةKerberos ، فإن خطوات المصادقة لمتاجر التجزئة، وهو العميل، هي كما يلي.

أولاً: يقوم بائع التجزئة بتوقيع المفتاح العام استنادًا إلى المفتاح الرئيسي لبطاقة SIM بمساعدة مفتاحه الخاص، ثم يقوم بتشفيره بالمفتاح العام للمشغل وإرساله إلى المشغل كطلب أولي.

ثانياً: يتلقى المشغل طلب بائع التجزئة ويقوم بفك تشفيره بمساعدة مفتاحه الخاص ويستخرج المفتاح العام لبائع التجزئة. وبناء على ذلك، يقوم بإنشاء مفتاح متماثل ويضعه في حزمة آمنة، ويوقعه بمفتاحه الخاص، ويرسله إلى بطاقة SIM للبيع بالتجزئة.

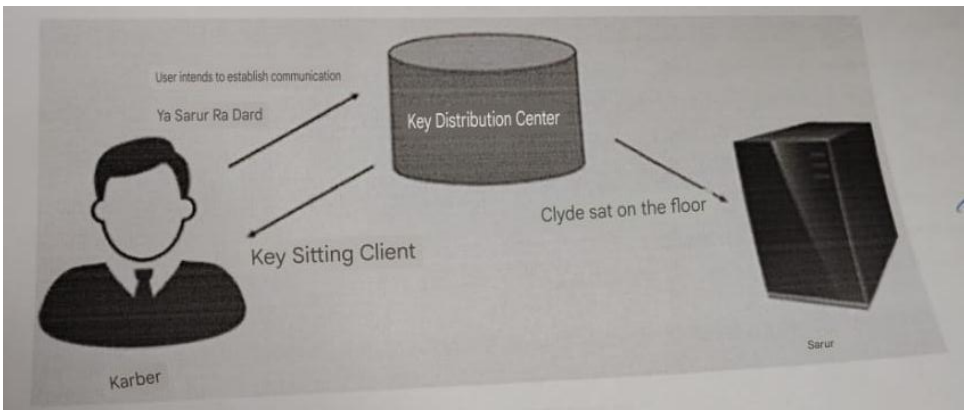
٤) تقوم بطاقة SIM الخاصة بتاجر التجزئة بفك تشفير الحزمة بمفتاحها الخاص وتحصل على المفتاح المتماثل الخاص بها والمشغل وتخزنه في بطاقة SIM. ويظهر ذلك في الشكل(٣-٣).



الشكل (٣-٣) فك التشفير بواسطة المفتاح المتماثل

١.٣.٣- المرحلة الثانية: بناء الثقة

نظرًا لأنه في عملية Kerberos ، يتم استخدام مشاركة نفس مفتاح الأمان بين العميل والخادم لإنشاء الثقة، لذلك في هذه المرحلة يتم وصف تشغيل Kerberos قد يرغب العميل في التواصل مع خوادم متعددة ويحتاج كل خادم إلى مفتاح. قد يتعين على الخادم أيضًا الاتصال بعدة عملاء، ويحتاج كل عميل إلى مفتاح. اذ من الصعب تخزين وحماية مفاتيح متعددة في العديد من الأنظمة. يعد مركز التوزيع الرئيسي KDC كوسيط موثوق به بمثابة حل من بروتوكول مصادقة Kerberos لحل هذه المشكلات. تحتفظ KDC بقاعدة بيانات تحتوي على معلومات حسابات جميع الأطراف الخاضعة لسيطرة النظام. تتضمن هذه المعلومات مفتاح التشفير الذي يتم الاحتفاظ به سرًا بين مركز توزيع المفاتيح (KDC) والأطراف الخاضعة للمراقبة. المفتاح أعلاه هو مفتاح طويل المدى وله صلاحية زمنية عالية ويستخدم في الاتصال بين مركز التوزيع الرئيسي والجهات المراقبة، وتظهر هذه العملية في الشكل (٣-٤).



الشكل (٣-٤) عملية بناء الثقة

الشكل (٣-٤). يوضح إذا أراد العميل الاتصال بالخادم، فإنه يرسل طلبًا إلى .KDC يقوم KDC بتوزيع مفتاح الجلسة على كل من جانب الخادم والعميل في نموذج مشفر. بعد أن يتلقى العميل مفتاح الجلسة هذا. وقد يرسل رسالة إلى الخادم على الفور أو بعد مرور بعض الوقت.

في هذه الحالة، ينبغي معالجة حالتين مهمتين. إذا قرر العميل. لتأسيس هذا الاتصال

لاحقًا، يجب على الخادم تخزين مفتاح الجلسة المستلم من KDC بناءً على طلب العميل. من ناحية أخرى، بسبب حركة مرور الشبكة، قد يقوم الخادم لا ينبغي استلام مفتاح الجلسة هذا من مركز التوزيع الرئيسي حتى وصول رسالة العميل. ولمنع ذلك، يجب إرسال مفتاح الجلسة إلى الخادم، ويرسل مركز توزيع المفاتيح (KDC) نسخة من هذا المفتاح إلى العميل على شكل تذكرة جلسة. في الرد بناءً على طلب العميل، تقوم KDC بإرجاع نسختين من مفتاح الجلسة إلى العميل نفسه.

٤.٣- الجزء الثاني: تأمين التواصل بين العميل ومزود خدمة القسيمة من خلال مدير الثقة تكرر خطوات القسم السابق للعملاء.

١.٤.٣- تصميم التطبيق

وبعد تصميم المصفوفة وقياس الاحتياجات، تم تنفيذ تطبيقين لنظام Android لمعلومات العملاء وتجار التجزئة. من خلال كتابة الأقسام الأمامية والخلفية ووظائف الاتصال مع الخادم في أقسام كود Java التي تتطلب الاتصال بالخادم، يجب كتابة الوظائف المطلوبة في نموذج غير متزامن. وبمساعدة بروتوكول http، فإنه يحدد بنية الطلب والاستجابة بين الخادم والتطبيق. ولهذا الغرض تم استخدام مكتبة volley في نظام Android وبروتوكول http. في الواقع، في تطبيق البيع بالتجزئة، بعد تسجيل الدخول، والذي يتضمن رقم الهاتف المحمول وكلمة المرور والبريد الإلكتروني الاختياري، يجب على بائع التجزئة إرسال طلب القيمة الأولية w0 إلى الخادم مرة واحدة في كل فترة خصم، وله مصادفة ثابتة حتى نهاية الاتجاه، يرسل إلى بائع التجزئة لإنتاج مصفوفة X بأكملها لنفسه. في كل مرة يقوم فيها أحد العملاء بإجراء معاملة ناجحة، ينتمي إليه عدد من نقاط الولاء، يرسل بائع التجزئة المصفوفة المقابلة للسلسلة الفرعية للعميل (member_id) وعمود عدد نقاط الولاء للعميل. يتم إرسال هذه التذكرة، وهي في الواقع نفس رمز الخصم، إلى العميل عبر رسالة نصية أو NFC. في المتابعة، في الشكلين (٣-٥) و (٣-٦)، يمكنك رؤية تصميم واجهة المستخدم لهذين التطبيقين. تتضمن قائمة خدمات تصميم الويب:

١) وظيفة المصادقة للعملاء وتاجر التجزئة بشكل منفصل

٢) تحميل برامج الخصم المتنوعة من الخادم

٣) عرض هذه الاتجاهات في تطبيق البيع بالتجزئة

٤) التحقق من صحة رمز نقاط الولاء

٥) تخصيص مبلغ معين لكل عميل

٦) تخصيص مبلغ معين لكل عميل

٧) معادلة العدد المحدد من نقاط الولاء للقسيمة

الشكل (٣-٥) تصميم التطبيق

الشكل (٣-٦) تصميم التطبيق

٥.٣- إضافة رمز مميز للتحقق من الهوية:

هناك طرق مختلفة لمصادقة المستخدم. في طريقتنا (Trust Manager) يوجد خادم ثالث وهو يوفر رمزًا لإرسال الطلب والتحقق من الميقوم المستخدم الذي يريد إرسال طلب إلى خادم قسيمة الهاتف المحمول بإحضار السلسلة المجزأة فقط بدلاً من المعلومات الأخرى في الطلب، ومن جانب الخادم، يتم البحث عن هذه السلسلة في قاعدة البيانات. إذا كانت هناك سلسلة في قاعدة بيانات الخادم، فسيتم إجراء المصادقةصادقة به. يتم تعيين سلسلة طويلة مكونة من ٧٤ بت لكل مستخدم وتكون عشوائية ولا يمكن تخمينها قلنا أنه لا يمكن تخمين سلسلة طويلة من الرموز المميزة، ولكن يمكن سماعها. ولحل مشكلة التنصت تم استخدام مفهوم المفتاح المشترك، وهو

التماثل بين جهاز الاستقبال والمرسل. يمكن الوصول إلى أي جزء من المفتاح بواسطة مدير المفاتيح لنفس المرسل أو المتلقي. لذلك إذا حدث التنصت، فإن الدخيل لديه جزء فقط من المفتاح ولا يمكنه استخدام هذا الجزء.

٦.٣- محاكاة بطاقة SIM مع تطبيق أندرويد

عند محاكاة بطاقةSIM ، يجب أن يكون التطبيق قادرًا على التفاعل مع المشغل دون تدخل المستخدم في خلفية الهاتف المحمول. الهدف هو أن يتفاعل تطبيقان من تطبيقات Android، العضو والمحاكي، مع بعضهما البعض في الخلفية. بمساعدة ثلاث طرق للنشاط وصفحات البث واستخدام الخدمة في Android ، أصبح هذا العمل ممكنًا. استخدمنا الخدمة. في تطبيق المحاكاة، وفقًا للشكل (٣-٧) قمنا بكتابة خدمة تسمى خدمة بطاقة SIM ، والتي ترسل خدمة ويب إلى المشغل وتستقبل رمزًا مميزًا. لاختبار الأداء الصحيح لتطبيق المحاكي، نرسل طلبًا لإنشاء المفتاح وتوزيعه على الخادم واختبار النتائج باستخدام برنامج ساعي البريد. تتم خطوات تنفيذ الطلب وفقًا لبروتوكول المرحلتين المقترح. إذا كان هناك تغيير في المفتاح المشترك، فلن يتم الوثوق به. تم إنشاء خطأ ولن يتم إرسال المفتاح المشترك لبطاقة SIM وموفر خدمة القسيمة إليهم. كما أنه في حالة النجاح أو الخطأ في إرسال الطلب، سيتم استقبال رسالة بناءً على ذلك على الخادم. كانت خدمة الويب هذه عبارة عن تطبيق لمحاكي المشغل الذي يمكننا توصيله بأي تطبيق آخر إلى جانب تطبيق Android لمحاكي بطاقة.SIM

الشكل (٣-٧) محاكاة نظام اندرويد

يحتوي هذا التطبيق على تطبيق aidl القياسي لمحاكي بطاقة sim، والذي يمكننا توصيله بأي تطبيق Android آخر يحتاج إلى التواصل مع المشغل إلى جانب خدمة الويب Python.

فك التشفير باستخدام بروتوكول Kerberos بعد تصميم قسم كوبونات الجوال على الهواتف المحمولة نناقش فك التشفير من خلال بروتوكول Kerberos. كما ذكرنا في الفصل الثاني، فإن تحديد الهوية والمصادقة هما المحوران الرئيسيان في معظم أنظمة التحكم في الوصول. التعريف هو عملية يستخدمها المستخدم لتقديم نفسه إلى نظام المعلومات، والتي عادة ما تكون على شكل معرف تسجيل الدخول. في الواقع، تحديد الهوية هو الرد على المستخدم للإجراءات التي يقوم بها على النظام.

باستخدام تشفير المفتاح المتماثل Kerberos، فإنه يتمتع بالقدرة على مصادقة العملاء وتقديمهم إلى الخدمات الأخرى ضمن الشبكة. يمكن وصف البنية ونمط العمل لبروتوكول Kerberos من خلال بنية العمل لبيئة المتجر. في مثل هذه البيئة، قد يكون هناك آلاف المواقع المختلفة لمحطات العمل والشبكات المحلية وأجهزة الكمبيوتر الشخصية والعديد من أجهزة الكمبيوتر الأخرى غير المؤمنة. لذلك، في مثل هذه البيئة، لا يمكن لأحد أن يدعي أن الكابلات آمنة تمامًا، والرسائل المرسلة على الشبكة آمنة من التلاعب، وحتى الخوادم ومواقع تخزينها لا يمكن اعتبارها آمنة تمامًا. ولكن في مثل هذه البيئة، يمكن تأمين عدد قليل من الخوادم أو عدد قليل من المواقع قدر الإمكان والادعاء بأن هذه الخوادم ومواقع تخزينها آمنة، ومع ذلك، يمكن هنا استخدام هذه الخوادم كآلية مصادقة آمنة موثوقة بين كل عميل وخدمة في الشبكة وتشكل هذه الخوادم المركزية معًا KDC وTGS وAS. من Windows Server 2000 والإصدارات الأحدث، يتم دعم بروتوكول Kerberos بواسطة أنظمة تشغيل Microsoft. القاعدة العامة لنشاط بروتوكول Kerberos في البيئات التشغيلية هي كما يلي:

١) تعرف KDC جميع المفاتيح الخاصة لعملاء وخوادم الشبكة.

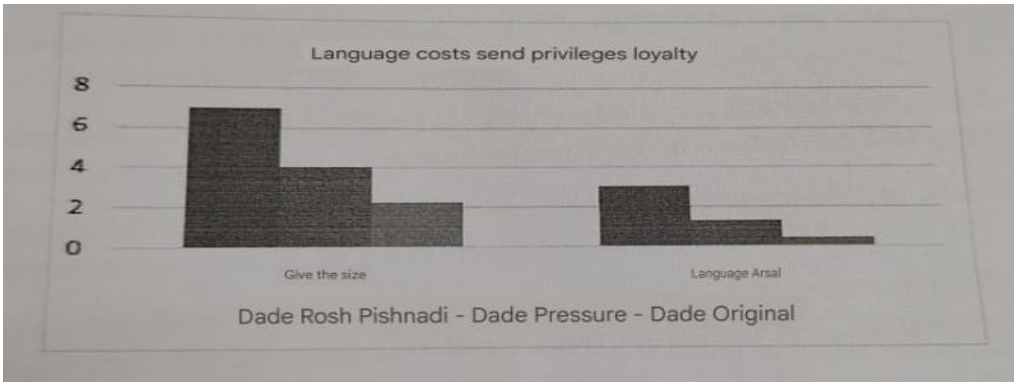
٢) يستخدم KDC هذه المفاتيح لتبادل المعلومات بين الخوادم والعملاء.
٣) يستخدم TGS rosKerbe للمصادقة أولاً على طلبات الخدمة من العملاء ولكل جلسة من الجلسات التي يتم إنشاؤها بين هذه الخدمات مثل العملاء وKDC والخادم وKDC بالإضافة إلى العميل والخادم، ينتج المفتاح المتماثل تسوية مؤقتة.
٤) في هذه اللحظة، يتم إنشاء الاتصال باستخدام المفاتيح التي تم إنشاؤها في الخطوة السابقة.

٧.٣- مقارنة زمن التنفيذ:

المفاتيح التي أنتجها المشغل في هذا البحث تحتوي على ٧٤ حرفًا كحد أقصى. نظرًا لأن كل حرف يتم تمثيله بـ ٣٢ بت ويلزم ٩ عمليات تبادل للمفاتيح، فإن حجم البيانات لدينا يبلغ ١٨٤٣٢ بت، وهو ما يعادل ٤٦٠٨ بايت وبالتالي ٢٥.٢ كيلو بايت. يتم الحصول على وقت الإرسال من إجمالي أوقات الاستجابة لطلبات http. ويبين الجدول (١-٤) التكلفة الزمنية لإرسال نقاط الولاء مقارنة بالمادة الأساسية. الشكل (٤-١) رسم بياني للتكلفة الزمنية لإرسال نقاط الولاء، جدول (٤-٢) التكلفة الزمنية للتشغيل على الهاتف الذكي، الشكل (٤-٢) التكلفة الزمنية للتشغيل على الهاتف الذكي .

الجدول (١-٤) التكلفة الزمنية لإرسال نقاط الولاء مقارنة بالمادة الأساسية

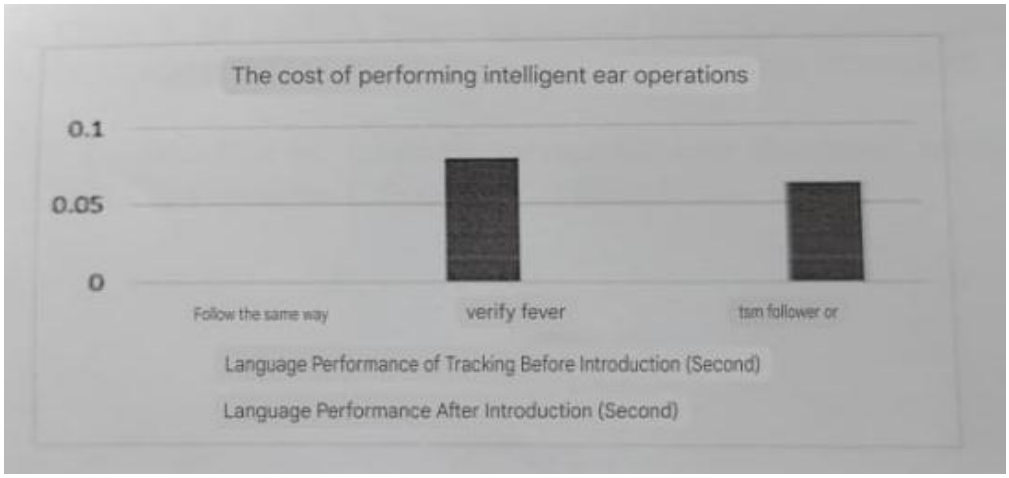
	البيانات الأصلية	البيانات المضغوطة (المادة الأساسية [٢٤])	بيانات البحث (بعد تطبيق الطريقة المقترحة)	معدل التحسن	تحسن النسبة المئوية
حجم البيانات	٧ كيلو بايت	٤ كيلو بايت	٢٥ ، ٢ كيلو بايت	١.٧٥	٤٣.٧٥ %
وقت الشحن	٣ ثوان	١.٣ ثانية	٠.٤٨٢ ثانية	١ ٠.٨	٦٢.٩ %



الشكل (٤-١) رسم بياني للتكلفة الزمنية لإرسال نقاط الولاء

جدول (٤-٢) التكلفة الزمنية للتشغيل على الهاتف الذكي

	زمن تنفيذ المعاملة قبل الطريقة المقترحة (بالثواني)	زمن التنفيذ بعد الطريقة المقترحة (بالثواني)	نسبة التحسن في الطريقة المقترحة
وظيفة التجزئة أحادية الاتجاه	٠.٠٠٠١٥	٠.٠٠٠٠١٥	%٩
وظيفة التحقق	٠.٠٨ ثانية	٠.٠٠٠٢٢	%٣٦
وظيفة مع TSM	لا يمتلك	٠.٠٦٣	



الشكل (٤-٢) التكلفة الزمنية للتشغيل على الهاتف الذكي

٤- المبحث الرابع/الاستنتاجات والتوصيات

في هذه الدراسة تم استخدام تطبيق بروتوكول Kerberos لغرض المصادقة على العمليات التبادل المالي الالكتروني من خلال الهاتف المحمول باستخدام التشفير وفك التشفير للمفتاح المتماثل ، وتم استخدام مشغل الشبكة بطاقة ال (SIM) كمدير للثقة لتعزيز الامان من خلال عمليات تبادل المعلومات والدفع المالي الالكتروني ويبقى هذا الحقل من الدراسات واعداً نظراً لزيادة المخاطر المحتملة لامن الشبكات والمعلومات ويوصي الباحث باستخدام تقنيات تشفير اخرى واستخدام اساليب الذكاء الاصطناعي ومقارنة النتائج في الدراسات المستقبلية.

المصادر

[1] Jalili R, Taherian M. 2017. Security and trust in electronic commerce. Proceedings of the 4th E-Commerce Conference, Vice Presidents of Planning and Economic Affairs of the Ministry of Commerce, print.

[2] Walczuch R, Duppen R. (2002). Payment Systems for the InternetConsumer Requirements, Department of Accounting and Information Management. University of .

[3] Mehboob Jahangard, Amir. "Asymmetric cryptography of electronic signature certificate of e-commerce gateway", Kanon, August 2019, No. 107.

[4] Hashemi M, Soroush A. 2014. An overview of the security of electronic payment and mobile payment. Proceedings of the Third National E-Commerce Conference, Deputy Planning and Economic Affairs, first edition.

[5] Maastricht, The Netherlands Steiner J. 1992. The Kerberos network authentication service overview. MIT project Athena RFC 1520.

[6] Hsueh, S. C., & Chen, J. M. (2010). Sharing secure m-coupons for peer-generated targeting via eWOM communications. Electronic Commerce Research and Applications, 9(4), 283-293.

[7] Hsueh, S. C., & Chen, J. M. (2010). Sharing secure m-coupons for peer-generated
targeting via eWOM communications. Electronic Commerce Research and Applications, 9(4), 283-293.
[8] Kizza J. M.)2017(. Security in wireless networks and devices," in Guide to Computer Network Security. Cham, Switzerland: Springer, 397-427.
[9] Hassan M. Al-Jawahry,& d Sahar Adill Kadum,(2023), Kerberos Protocol: History, Steps, and Security Analysis , Journal of Science And Engineering Application ISSN 2521-3911.