المجلة الليبية لعلوم التعليم – العدد الثاني عشر – فبراير 2024
ISSN202153
Website: https://laes.org.ly Email: alse9.2019@gmail.com

دراسة تأثير هجمات الأمان على أداء الشبكات ودور بروتوكولات التشفير في حماية الشبكات.

زينب عمر محمد [1] ليلى علي أحمد الحكنون[2]
(قسم الحاسوب، كلية التربية، جامعة طرابلس) طرابلس، ليبيا[1،2].
[1]Za.othman@uot.edu.ly

الملخص:

تتناول هذه الدراسة التحديات التي تواجه الشبكات نتيجة للتقدم التكنولوجي وارتفاع استخدام الشبكات الرقمية. تركز الدراسة على تأثير هجمات الأمان على أداء الشبكات ودور بروتوكولات التشفير في مكافحة هذه الهجمات. كما تقدم الدراسة إطارًا لفحص تأثير أنواع معينة من هجمات الأمان على بروتوكولات التشفير. الجزء التالي يسلط الضوء على دور بروتوكولات التشفير في حماية الشبكات، ويستعرض وظائفها الحيوية والآليات التي تجعلها جزءًا أساسيًا من استراتيجيات الأمان الشاملة. وفي الختام، يتم التركيز على تطوير استراتيجيات فاعلة لتعزيز جاهزية الشبكات من خلال اعتماد بروتوكولات التشفير، موفِّرًا تحليلًا لدور بروتوكولات التشفير في تحقيق توازن بين الأمان والأداء في مواجهة التحديات المستمرة للأمان السيبراني.

الكلمات المفتاحية: بروتوكولات التشفير، هجمات الأمان، الامن السيبراني

Abstract

This study addresses the challenges facing networks as a result of technological advancement and the increased use of digital networks. The study focuses on the impact of security attacks on network performance and the role of encryption protocols in combating these attacks. The study also provides a framework for examining the impact of certain types of security attacks on cryptographic protocols. The next part highlights the role of cryptographic protocols in protecting networks, and reviews their vital functions and the mechanisms that make them an essential part of comprehensive security strategies. In conclusion, the focus is on

developing effective strategies to enhance network readiness through the adoption of encryption protocols, providing an analysis of the role of encryption protocols in achieving a balance between security and performance in the face of ongoing cybersecurity challenges.

Keywords: encryption protocols , impact of security , cyber security.

مقدمة الدراسة:

في ظل تطور التكنولوجيا، واستخدام الشبكات الرقمية بشكل مستمر وواسع، ظهرت العديد من التحديات في هذا المجال، ومن بين هذه التحديات تبرز هجمات الاختراق كتحدي خطير يهدد أمان البيانات واستقرار الشبكات.(جون كانافان , 2015).(P.K.Malik ,2020)

" لقد أصبحت الهجمات الإلكترونية واحدةً من السُّبل المؤثرة من دون تكاليف كبيرة، بعد أن أصبح العالم أمام قوىً تتسلَّح بالتِّكنولوجيا الحاسوبيَّة، ويمكنها بكبسة زر الاختراق وارتكاب أفعالٍ تقنيَّةٍ مضرة بالآخرين عبر العالم الافتراضي، وثمَّة العديد من التَّطورات والتَّجاذبات والسِّجالات الميدانيَّة والنَّظريَّة، التي ألقت الضّوء على هذا المجال الجديد نسبيا "(خالد وليد محمود, 2013).

تسعى هذه الدراسة إلى تحليل مفصل بشأن تأثير هجمات الاختراق على أداء الشبكات، والتركيز على الأدوار الفعالة التي تلعبها بروتوكولات التشفير في مواجهة هذا التحدي، حيث يعتبر توفير الحماية للبيانات والاتصالات أمرًا حاسمًا ومهما.

في هذه الدراسة سنحدد ثلاث بنود رئيسية لدراستها:

1.فحص تأثير أنواع معينة من هجمات الأمان على بروتوكولات التشفير.

يقوم هذا البند بتحليل تأثير هجمات الأمان مثل التصيد وهجمات الرفض الخدمي الموزع على بروتوكولات التشفير، حيث يتم تحديد كيف يؤثر تنفيذ هذه الهجمات على فعالية التشفير، مما يساعد في فهم كيفية تأثير تلك الهجمات على أمان الشبكات.

2. دور بروتوكولات التشفير في الدفاع عن الشبكات:

تعتبر بروتوكولات التشفير الركيزة الأساسية في الدفاع عن البيانات والتحصين ضد هجمات الاختراق. سنبين كيفية عمل هذه البروتوكولات وكيف يمكن أن تكون جزءًا من استراتيجية فعّالة للحفاظ على سلامة الشبكات.

3.تطوير استراتيجيات لتعزيز استعداد الشبكات باستخدام بروتوكولات التشفير:

تقدم الدراسة استراتيجيات عملية لتحسين امكانية الشبكات لمواجهة التحديات السيبرانية باستخدام بروتوكولات التشفير، ويستعرض كيفية تكامل هذه البروتوكولات في البيئات الشبكية بشكل يعزز الأمان ويحقق أداءً فعّالًا.

من خلال هذه الدراسة نسعى إلى الإجابة عن سؤال محدد وهو: "كيف يؤثر تنفيذ هجمات الأمان، على فعالية بروتوكولات التشفير وكيف يمكن لبروتوكولات التشفير أن تسهم في حماية الشبكات وضمان أمان البيانات؟

مشكلة الدراسة:

تتمثل المشكلة في الحاجة إلى فهم وتحليل مصادر التهديد والاختراقات التي تؤثر على أمان شبكات والمعلومات وبروتوكولات التشفير، بما في ذلك الخطر الداخلي والخطر الخارجي وسوء التصميم ومخاطر الأمان السيبراني.

تساؤلات الدراسة:

1. كيف يمكن تحديد وتصنيف مصادر الخطر الداخلي لشبكات المعلومات؟
2. ما هي أساليب وتقنيات الهجوم والاختراق السيبراني؟
3. ما هي العيوب المحتملة في استخدام التشفير لحماية الشبكات؟

أهداف الدراسة:

1. تحليل مصادر الخطر الداخلي والخطر الخارجي لتطوير استراتيجيات أمان فعّالة.
2. فحص أساليب وتقنيات الهجوم السيبراني والاختراق.
3. تقييم أهمية بروتوكولات التشفير وتحديد عيوبه المحتملة في تأمين الشبكات.

أهمية الدراسة:

تكمن أهمية الدراسة في أن مجال امان الحواسيب والشبكات أمر بالغ الأهمية للمنشآت لعدة أسباب مهمة منها. أولاً، يركز الأمان على حفظ الأصول الحيوية للشركة، بما في ذلك حماية المعلومات الحساسة وليس فقط الأجهزة والبرامج. ثانياً، يمكن لتبني سياسات أمان معلومات فعّالة منح المنشأة ميزة تنافسية في أسواق مثل الخدمات المالية عبر الإنترنت والتجارة الإلكترونية، مما يزيد من معدل القبول والاستجابة لديها. وأخيراً، يساهم التشفير في حماية البيانات أثناء انتقالها عبر الأجهزة، بينما تقلل إجراءات الأمان الإضافية مثل المصادقة المتقدمة من وصول المستخدمين غير المصرح لهم.

منهجية الدراسة:

استخدمت الباحثتان المنهج الوصفي في وصف وتحليل بيانات الدراسة والاجابة على تساؤلات الدراسة.

الإطار النظري:

مفهوم امن الشبكات هي مجموعة من الإجراءات التي يمكن من خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تهددها وتمت دراسة الوسائل والتجهيزات التقليدية المستعملة لحماية المستخدمين من الفيروسات والاختراقات التي تردهم عبر الانترنت، والتي من أهمها الجدران النارية (تاج الدين جركس، 2008).

الجميع الان يدركون أهمية بروتوكولات التشفير وازدياد الحاجة إليها خصوصاً في هذه الأيام مع الانتشار الواسع للأنترنت وكثرة سرقة المعلومات والبيانات الشخصية, وكلمات السر إذ, تكمن أهمُته بالحفاظ على سرية المعلومات الهامة والحساسة, وعدم وصولها إلى الأشخاص الغير مخولين بالاطلاع عليها, ويمكن عن طريق التشفير التقليل من حجم المعلومات أثناء انتقالها، وضمان هوية المصدر المرسل للرسالة, وأكبر دليل على أهمية بروتوكولات التشفير أنه في وقتنا الحاضر تم إنشاء العديد من الشركات المختصة بأمن المعلومات عامةً و بروتوكولات تشفير الرسائل والبيانات (صلاح الهادي غبيق, خاصة 2013 .) (Sura Fahmy February 2021)

ففي الولايات المتحدة الأمريكية، نجد وكالة الأمن القومي السرية الأمريكية التي تختص بالتشفير، ترتبط مباشرة بالرئيس الأمريكي ويرتبط بها حوالي 80,000 موظف، وتزيد نفقاتها السنوية عن 15 مليار دولار، وتضم عددا كبيرا من الحواسيب المتقدمة تقنيا (صلاح الهادي غبيق، خاصة 2013).

ومن هذا السياق نذكر بعض أنواع هجمات الأمان الشائعة:

1. هجمات التصيّد (Phishing):

- تستخدم لخداع الأفراد واستخراج معلومات حساسة عن طريق التنكر ككيان آخر، عادة من خلال رسائل بريد إلكتروني مزيفة.

2. هجمات الرفض الخدمي الموزع (DDoS):

- تستهدف زيادة الحمل على الخوادم أو الشبكات بشكل مفرط لتعطيل الخدمة للمستخدمين الشرعيين.

3. هجمات التسلل (Intrusion Attacks):

- تهدف إلى اختراق النظام أو الشبكة للوصول إلى معلومات حساسة أو لتدمير البيانات.

4. هجمات البرامج الضارة (Malware Attacks):

-هناك نمو كبير في الانترنت و الأجهزة الذكية المتصلة بالشبكة من ناحية, و من ناحية أخرى, هناك زيادة في عدد البرامج الضارة التي تهاجم الشبكات و الأجهزة و الأنظمة و التطبيقات و منها ما يشمل الفيروسات وبرامج التجسس وبرامج الفدية, وتستهدف التلف أو الاستلاء على البيانات (عمر شامل أحمد 2012,).

5. هجمات تصيّد الهوية (Identity Theft Attacks):

- تهدف إلى سرقة هويات الأفراد لاستخدامها في أنشطة غير قانونية.

6. هجمات التجسس (Spyware Attacks):

- تستخدم لمراقبة أنشطة المستخدمين دون علمهم، وغالبًا ما تكون متسللة عبر برامج خبيثة.

-تفضل الدول التصرف دون أن يلاحظها احد وبالتالي فإنه الهجمات الالكترونية اليوم مجرد تطورات جديدة في مجال التجسس أو العمليات الاستخبارية أو العمليات المغطاة، و تستخدم لمراقبة أنشطة المستخدمين دون علمهم, وغالبًا ما تكون متسللة عبر برامج خبُثة.

هذه مجرد أمثلة، ويتطور مجال هجمات الأمان باستمرار، مما يجعل الحماية والوقاية ضرورية للحفاظ على أمان البيانات والشبكات.

هجمات الأمان المستهدفة في هذه الدراسة:

- هجمات التصيد (phishing):

في البداية يقوم المهاجم بأنشاء موقع تصيد احتيالي والذي يكون مشابه لحد كبير ويب المعروف ومحلة ثقة بين المستخدمين ورواده حيث في غالب الأحوال يتعمد المهاجمون اختيار عنوان (URL) قريب ومشابه في حروفه الابجدية للموقع الأصلي، يتبع ذلك ارسال بريد الكتروني يطلب من المستخدمين النقر على رابط او فتح ملف مرفق بعد تن يدخل المستخدم على الموقع المزيف يطلب منه ادخال بيانات حساسة على سبيل المثال: كلمات المرور / والمعلومات البنكية.

التصيد الاحتيالي هو شكل من أشكال الجرائم الإلكترونية حيث يقوم المهاجم بتقليد شخص / مؤسسة حقيقية من خلال الترويج له كشخص أو كيان رسمي من خلال البريد الإلكتروني أو وسائل الاتصال الأخرى. في هذا النوع من الهجمات السيبرانية، يرسل المهاجم روابط أو مرفقات ضارة من خلال رسائل البريد الإلكتروني التصعيدية التي يمكنها أداء وظائف مختلفة، بما في ذلك التقاط بيانات اعتماد تسجيل الدخول أو معلومات حساب الضحية. تؤذي رسائل البريد الإلكتروني هذه الضحايا بسبب فقدان الأموال وسرقة الهوية.

المصدر: لندوة الدولية السادسة لعام 2018 حول الطب الشرعي والأمن الرقمي (ISDFS)

- هجمات الرفض الخدمي الموزع (DDOS):

بمجرد اختراق القراصنة حاسوبا أو جهازا ذكيا، فإنه يمكنهم استدعاؤه للتنفيذ في أي لحظة، وكل ما يحتاجه المهاجم لاستغلال الشبكة هو تشغيل برنامج صغير يتواصل مع كافة الحواسيب المخترقة التي تخضع لسيطرته، ويتمكن المهاجم عندها من أمر هذه الحواسيب بالبدء بالاتصال عبر الإنترنت مع خادم أو موقع ويب معين بهدف إغراقه وزيادة الحمل بعشرات آلاف من الطلبات والاوامر في فترة زمنية قصيرة، مما يصيبه بالشلل وتعطيل الخدمة للمستخدمين الشرعيين.

تكون هجمات رفض الخدمة بمحاولة صريحة من قبل المهاجم لمنع المستخدمين الشرعيين من استخدام الموارد. قد يحاول المهاجم القيام بما يلي: "إغراق" الشبكة وبالتالي تقليل النطاق الترددي لمستخدم شرعي، أو منع الوصول إلى خدمة ما، أو تعطيل الخدمة لنظام معين أو مستخدم معين. نحن نصف الأساليب والتقنيات المستخدمة في هجمات رفض الخدمة،

المصدر: وقائع مؤتمر SMC 2000 المؤتمر الدولي حول الأنظمة والإنسان وعلم التحكم الآلي. "علم التحكم الآلي يتطور إلى الأنظمة والبشر والمنظمات وتفاعلاتهم المعقدة"

دور بروتوكولات التشفير في التصدي لهجمات الامان المستهدفة في هذه الدراسة:

- دور بروتوكولات التشفير في التصدي لهجمات التصيد:

1. استخدام بروتوكول HTTPS: يستخدم HTTPS (Hypertext Transfer Protocol Secure) لتأمين اتصالات الشبكة بين المتصفح والخادم. يتم تشفير بيانات المرور بين الجهاز الشخصي والموقع الذي يتم الاتصال به، مما يحمي من تسريب المعلومات الحساسة.

"Phishing in the Security Context: A Review" - مقالة علمية نشرت في مجلة International Journal of Computer Applications،

2. شهادات SSL/TLS: تستخدم الشهادات الرقمية للتحقق من هوية الخادم وتأمين التواصل بين المتصفح والخادم. يتم استخدام بروتوكول SSL (Secure Sockets Layer) أو بروتوكول TLS (Transport Layer Security) لتشفير البيانات وحمايتها من الاعتراض أو التلاعب.

"Phishing Attacks and Countermeasures: A Survey" - مقالة علمية نشرت في مجلة International Journal of Computer Science and Security (IJCSS)

- دور بروتوكولات التشفير في التصدي لهجمات الرفض الخدمي الموزع:

1. تشفير الاتصالات: استخدام بروتوكولات التشفير مثل SSL/TLS في اتصالات الشبكة يحمي بيانات المرور بين المستخدمين والخوادم. هذا يضمن سرية المعلومات ويمنع المهاجمين من التقاط أو تعديل البيانات المرسلة والمستقبلة.

"DDoS Defense Mechanisms: A Survey" - مقالة علمية نشرت في مجلة International Journal of Network Security & Its Applications

2. اكتشاف ومنع هجمات DDoS: بروتوكولات التشفير يمكن أن تساهم في اكتشاف ومنع هجمات DDoS. من خلال مراقبة حركة المرور الشبكية وتحليل أنماط الاختناق، يمكن لأنظمة الحماية المتقدمة تحديد هجمات DDoS واتخاذ إجراءات لمنعها أو تقليل تأثيرها.

هذه الإجراءات والتقنيات لا توفر حماية مطلقة ضد هجمات DDoS، ولكنها تعزز قدرة الشبكة على مقاومة وتحمل هذه الهجمات. تكون استراتيجية الدفاع المناسبة تعتمد على نوع الشبكة ومتطلبات الأمان الخاصة بها.

الدراسات السابقة:

1. تهدف هذه الدراسة إلى تعزيز أمان نقل البيانات عبر شبكات الاتصال، حيث تم اقتراح وتصميم نظام يجمع بين تقنيات التشفير وإخفاء البيانات. تم استخدام تقنية تشفير مثل DES أو TDES لتأمين البيانات، ومن ثم تم إخفاء البيانات المشفرة في صور BMP باستخدام تقنية الخلية الثنائية الأقل أهمية. الدراسة قد قامت بتطبيق هذا النظام على بروتوكولات مختلفة مثل SIP وSDP وRTP وRTCP عبر شبكة الإنترنت، واستخدام القنوات المخفية لإرسال البيانات. تم استرجاع المعلومات المخفية بنجاح. أظهرت الدراسة أن الإخفاء في خلية ثنائية يقلل من قيمة الخطأ ويمكن استخدام مفاتيح متعددة لزيادة سرية الإخفاء. الدراسة استخدمت لغة البرمجة Visual C#، وبيئة Matlab7.6 (R2008a) البرمجية، (منار يونس كشمولة,2011) .
2. هدفت هذه الدراسة إلى تقييم هجمات استعادة مفتاح التشفير في بروتوكول الحماية WEP في الشبكات اللاسلكية. توصلت الدراسة إلى تسليط الضوء على نقاط الضعف في بروتوكول WEP وسهولة اختراقه. وقد قامت بتقديم نتائج التقييم ومقارنة الهجمات المختلفة، مؤكدة على أهمية استخدام بروتوكولات حماية أكثر قوة لضمان أمان الشبكات اللاسلكية، (رزق غانم ,2019) .

3. تستهدف هذه الدراسة حماية البيانات في تقنية D2D، من خلال تطوير بروتوكول لتبادل المفاتيح وخوارزمية تشفير باستخدام توابع Logistic Map. يتناول الهدف الرئيسي تأمين اتصالات D2D من

هجمات القرصنة والنسخ، حيث تسعى الدراسة إلى بناء منظومة تشفير متقدمة مخصصة لتقنية D2D (عصام محمد اسعد ,2023) .

4. هدفت هذه الدراسة إلى تحليل وتصميم مفتاح جديد للشبكة الافتراضية الخصوصية باستخدام تقنية البعثرة (Scrambling). أظهرت الدراسة أن هذا المفتاح يسهم في تعزيز فعالية الحماية في شبكات الخصوصية الافتراضية، من خلال إنشاء جدار ناري، وتشفير البيانات، وتحسين عرض حزمة نقل البيانات، مع تقليل تأثير الضوضاء، (A.I.A.Jabbar,2005) .
5. هدفت هذه الدراسة إلى استعراض تأثير نمو شبكة الإنترنت والتقدم في الحوسبة السحابية وتطور تطبيقات الأعمال والتجارة الإلكترونية على تبادل المعلومات بين المؤسسات. كما ناقشت التحديات الأمنية المتزايدة نتيجة للهجمات الإلكترونية والحاجة إلى وسيط آمن لتأمين بيانات المؤسسات. قدّمت الورقة تقنية الشبكة الافتراضية الخاصة (VPN) كوسيلة فعالة وموثوقة لتأمين البيانات والأجهزة والموارد. ركزت الدراسة على تأثير VPN في حماية البيانات والخصوصية أثناء النقل عبر الإنترنت، مشددة على السمات الأمنية وأنواع هذه التقنية، بالإضافة إلى استعراض التحديات والتدابير الأمنية والبروتوكولات المستخدمة(فيصل الهادي محمد ,2022).

نتائج الدراسة ومناقشتها:

تمت دراسة "أمان الشبكات وبروتوكولات التشفير" بهدف فهم التحديات والتأثيرات الناجمة عن هجمات الأمان على أداء الشبكات. فيما يلي تلخيص لنتائج الدراسة ومناقشتها:

- أهمية أمان الشبكات:

تشير الدراسة إلى أن الحفاظ على أمان الشبكات يمثل أساسًا أساسيًا للحفاظ على سلامة المعلومات والبيانات، حيث تُعد الإجراءات الوقائية والدفاعية أساسية لمواجهة التحديات السيبرانية.

- دور بروتوكولات التشفير:

تتعامل هذه الدراسة مع دور بروتوكولات التشفير باعتبارها العنصر الأساسي في تأمين البيانات والاتصالات في الشبكات. توفر هذه التقنيات حماية فعّالة من الوصول غير المصرح به.

- تأثير هجمات الأمان على أداء الشبكات:

1. هجمات التصيّد (Phishing):

- أظهرت دراستنا أن هجمات التصيّد قد تؤدي إلى استخدام غير مصرح به للمعلومات الحساسة، مما يبرز أهمية التوعية وتحسين آليات التحقق.

2. هجمات الرفض الخدمي الموزع (DDoS):

- كشفت الدراسة أن هجمات DDoS يمكن أن تؤثر سلبًا على أداء الشبكات وتعطيل الخدمات، ولذلك يجب تبني حلول فعّالة للتصدي لهذه الهجمات.

- دور بروتوكولات التشفير في حماية الشبكات:

1. التشفير كأساس للأمان:

- أكدت الدراسة أن بروتوكولات التشفير تعتبر الركيزة الأساسية للدفاع عن البيانات والاتصالات، وتسهم بشكل كبير في الحماية من هجمات الأمان المتقدمة.

2. فحص تأثير هجمات الأمان على بروتوكولات التشفير:

- أجرت الدراسة تحليلًا لتأثير هجمات معينة مثل التصيد على فعالية بروتوكولات التشفير، وهو ما يساهم في تعزيز التصدي لهذه الهجمات.

- تطوير استراتيجيات باستخدام بروتوكولات التشفير:

1. تحسين جاهزية الشبكات:

- اقترحت الدراسة استراتيجيات فاعلة لتعزيز جاهزية الشبكات، من خلال تبني وتكامل بروتوكولات التشفير بشكل فعّال.

2. تحقيق توازن بين الأمان والأداء:

- قدّمت الدراسة تحليلًا شاملاً لكيفية يمكن لبروتوكولات التشفير أن تلعب دورًا فعّالًا في تحقيق توازن بين الأمان والأداء.

- **مقارنة الدراسة مع الأبحاث السابقة:**

تتيح نتائج هذه الدراسة مقارنة مع الأبحاث والدراسات السابقة التي تمت الاشارة اليها هنا. إلى أن الدور الحيوي لبروتوكولات التشفير في حماية الشبكات والتصدي لتحديات الامان قد تم تسليط الضوء عليه بشكل أكبر، كما أظهرت النتائج إلى ضرورة توجيه الاهتمام إلى مواضيع محددة مثل هجمات التصيد وتأثيراتها على فعالية بروتوكولات التشفير، وهو جانب لم يتم التطرق إليه بنفس التفصيل في الأبحاث السابقة .

الخلاصة:

توضح نتائج الدراسة أهمية تكامل بروتوكولات التشفير في استراتيجيات أمان الشبكات. كما تؤكد الدراسة من أن تبنى حلول متعددة لمواجهة هجمات الامان أمر ضروري مع الحفاظ على توازن فعال بين الامان والاداء، وهذا يعزز قدرة الشبكات على تحقيق حماية متكاملة وفعالة ضد التهديدات السيبرانية المتزايدة، مما يساعد ذلك في تعزيز قدرة المنظمات على حماية بياناتها الحساسة والمعلومات الحيوية ويزيد من استقرارها ونموها في بيئة التشغيل الرقمية المتطورة.

التوصيات:

- دراسة تأثير هجمات الأمان على تكنولوجيا محددة مثل الحوسبة الحيوية.
- توسيع الدراسة لاستكشاف تقنيات تشفير مبتكرة وفعّالة.
- تحليل التطورات في هجمات الأمان وتقديم استراتيجيات مستجدة للدفاع.

مراجع الدراسة:

أولاً: المراجع العربية:

1. تاج الدين جركس، عدنان معترماوي & ,زياد الشر يقي. (2008). طريقة متكاملة لحماية الشبكة الحاسوبية.(3)*Tishreen University Journal-Engineering Sciences Series, 30* .
2. خالد وليد محمود. (2013). الهجمات عبر الإنترنت ساحة الصراع الإلكتروني الجديدة .*سياسات عربية* ,(5)*1* , 115-125.
3. د. م. رزق غانم د. م. محمد الحسين. (2019). تقييم هجمات كورك لاستعادة مفتاح تشفير بروتوكول الحماية WEPفي الشبكات اللاسلكية .*مجلة جامعة دمشق للعلوم الهندسية* .(2)*35* ,
4. عصام محمد أسعد، & عبدالكريم السالم. (2023). تطوير خوارزمية لتشفير البيانات لتعزيز الأمن في اتصالات D2Dعن طريق التبادل الآمن للمفاتيح .*مجلة العلوم الهندسية و تكنولوجيا المعلومات*.47-22 ,(2) ,*7* ,
5. مدني، شعيب التجاني، المشرف، & محمود علي أحمد عم. (2015) .(*ترجمة الصفحات (5-40) كتاب:" أساسيات أمن الشبكات" تأليف: جون. إ. كانا فان* ,(Doctoral dissertation جامعة السودان للعلوم والتكنولوجيا.

ثانياً: المراجع الانجليزية:

1. Badir Mahmood, A., & Jabbar, A. I. A. (2005). Analysis and design of a novell vpn switch. *Al-Rafidain Engineering Journal (AREJ)*, *13*(4), 11-25.
2. Design and implementation of the 2011) .منار يونس كشمولة & ,رشا عواد حسن hybrid system for encryption and hiding the text file in the Voice over Internet Protocols. *IRAOI JOURNAL OF STATISTICAL SCIENCES*, *11*(2).

3 P.K.Malik,D.S.Wadhwa,andJ.S.Khinda, ,2020 “Asurvey of device to device and cooperative communication for the future cellular networks,” International Journal of Wireless Information Networks, pp.1–22

4 Sura Fahmy February 2021, “Secure voice cryptography based on Diffie-Hellman algorithm, University of Diyala” , Article in IOP Conference Series Materials Science and Engineering · DOI: 10.1088/1757-899X/1076/1/012057