مجلة جامعة دمشق للعلوم الهندسية
المجلد41 العدد(1) – 2025: 221-233

Damascus University Journal for engineering sciences
Vo 41 number (1) -2025: 221-233

تحسين تكامل إنترنت الأشياء والحوسبة السحابية باستخدام التشفير الهجين (ضمان الأمن والخصوصية)

عبير آصف منصور*[1] نديم شاهين[2]

*[1]. طالبة دراسات عليا (ماجستير)، مهندسة– قسم هندسة الاتصالات والالكترونيات–كلية الهندسة الميكانيكية والكهربائية–جامعة دمشق– دمشق– سورية.
mansour12.abeer@damascusuniversity.edu.sy

[2]. أستاذ، دكتور، مهندس– قسم هندسة الاتصالات والالكترونيات – كلية الهندسة الميكانيكية والكهربائية– جامعة دمشق– دمشق– سورية.
nchahin@scs-net.org

الملخص:

إحدى التقنيات المتقدمة التي تتوسع بسرعة في مجال الاتصالات هي دمج الحوسبة السحابية مع إنترنت الأشياء، مع ظهور الحوسبة السحابية أصبح من الممكن التغلب على مشاكل الحساسات التي تعاني من محدودية الموارد مثل التخزين والطاقة. يسعى تكامل إنترنت الأشياء (IoT) مع الحوسبة السحابية (CC) إلى تحقيق مستويات جديدة من الكفاءة في تقديم الخدمات ويعد الأمان والخصوصية من العوامل الرئيسية التي تعمل على إبطاء الاعتماد السريع والنشر الواسع لكل من إنترنت الأشياء والحوسبة السحابية. ونظراً لأن البيانات المرسلة معرضة للتهديدات والتسلل من خلال التنصت أو الوصول غير المصرح به، في هذه الورقة البحثية يتم استخدام تقنية التشفير الهجين لحماية المعلومات التي يتم إرسالها من أجهزة إنترنت الأشياء إلى الخادم السحابي. استخدام آلية التشفير الهجين يُمكّن من توفير مزايا أداء التشفير المتماثل وغير المتماثل من خلال تطبيق خوارزمية تشفير المنحني الإهليلجي ECC (Elliptic-curve cryptography) لتوليد المفاتيح واستخدام هذه المفاتيح لتشفير وفك تشفير البيانات باستخدام خوارزمية معيار التعمية المتطور AES (Advanced Encryption Standard) لتوفير بيئة حوسبة موثوقة. تم تنفيذ النظام المقترح وإظهار نتائج باستخدام المحاكي CONTIKI COOJA 3.0 وتوصيله بالسحابة، ودراسة مجموعة من مقاييس الأداء مثل استهلاك الطاقة ومعدل الحزم المستلمة وزمن تنفيذ الخوارزمية، إضافة للتحقق من إمكانية كشف وحصانة الشبكة ضد هجوم الثقب الأسود.

الكلمات مفتاحية: انترنت الأشياء، الحوسبة السحابية، أمن البيانات، التشفير الهجين، هجوم الثقب الأسود.

تاريخ الايداع:2022/11/11
تاريخ القبول:2023/1/18

Improving the IoT and Cloud Computing Integration using Hybrid Encryption

(Security and Privacy Guarantee)

Abeer Asef Mansour*[1] Nadim Chahin[2]

*[1]. Postgraduate Student (Master), Department of Electronics and Communication Engineering, faculty of mechanical and electrical engineering، Damascus University, Damascus, Syria. abeermn98@gmail.com
mansour12.abeer@damascusuniversity.edu.sy
[2]. Professor, Department of Electronics and Communication Engineering, Faculty of Mechanical and Electrical Engineering, Damascus University, Damascus, Syria.
nchahin@scs-net.org

Received: 11/11/2022
Accepted: 18/1/2023

Abstract:

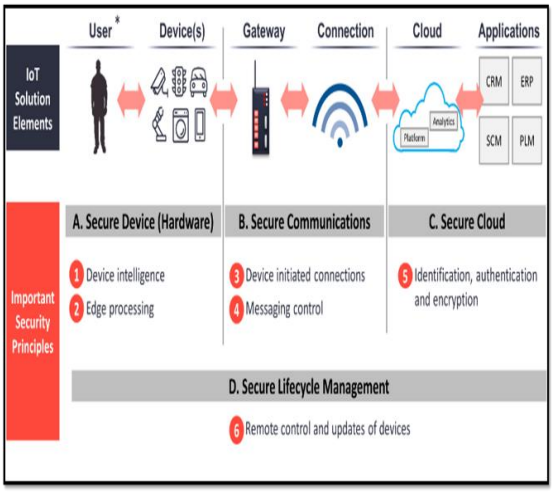
One advanced technology that is expanding quickly in the communications area is the integration of Cloud computing with the IoT, with the presence of cloud computing, it becomes possible to overcome the problems of sensor nodes that suffer from limited storage capacity and energy. The integration of the Internet of Things (IoT) with cloud computing (CC) seeks to achieve new levels of efficiency in service delivery. Security and privacy are key factors that slow down the rapid and widespread adoption and deployment of both IoT and cloud computing. Since the information sent between the sender and recipient is vulnerable to threats and attacks through eavesdropping or unauthorized, in this paper, encryption technology is used to protect the information that sent from the IoT devices to the cloud server. The security is achieved by using a hybrid encryption mechanism that provides the performance advantages of symmetric and asymmetric encryption algorithms. The Elliptic Curve Cryptography (ECC) algorithm is used for key generation and the AES (Advanced Encryption Standard) algorithm is used for encryption and decryption of the data to provide a reliable computing environment. We have implemented the proposed system and showed the results using CONTIKI COOJA 3.0 connected with the cloud service provider and evaluate a set of performance metrics such as power consumption, packet delivery ratio, algorithm execution time, and verify the network immunity against the blackhole attack.

Key words: Internet of Things, Cloud Computing, Data Security, Hybrid Encryption, Blackhole Att.

المقدمة

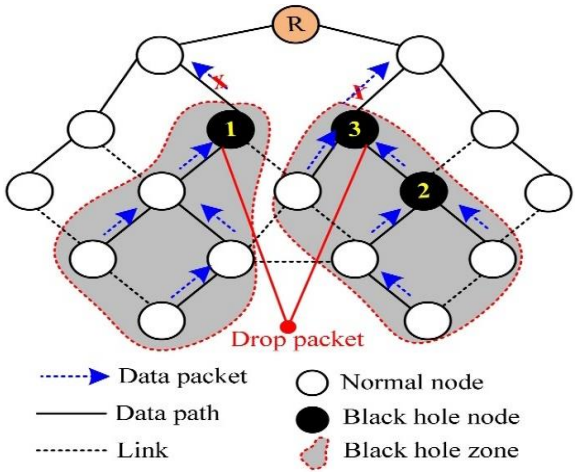
شهد كل من انترنت الأشياء IoT والحوسبة السحابية CC تطوراً مستقلاً في الأجهزة والبرامج الخاصة بهم لسنوات عديدة. تواجه إنترنت الأشياء العديد من المشكلات مثل سعة التخزين وكفاءة استهلاك الطاقة والقدرات الحسابية، ونظراً لأن CC لديها موارد وقدرات غير محدودة تقريباً، يمكنها دعم إنترنت الأشياء في تعويض القيود التكنولوجية مثل المعالجة والتخزين والطاقة. وكذلك، يمكن لإنترنت الأشياء أن يمنح CC الفرصة للتعامل مع كائنات العالم الحقيقي بطريقة أكثر ديناميكية لتقديم خدمات وتطبيقات جذابة جديدة في بعض التطبيقات العملية. بالنظر إلى الإمكانات الهائلة لهاتين التقنيتين والطريقة التي يكملان بها بعضهما البعض، فقد تم دمجهما لتشكيل ما يشار إليه عموماً باسم سحابة الأشياء (CoT-Cloud of Things). هذا التكامل مفيد لأن النظام الناتج يكون أكثر قوة وذكاء ويقدم حلولاً واعدة للمستخدمين. ومع ذلك، فإن (CoT) يواجه عدد كبير من التحديات مثل الأمن والخصوصية والموثوقية، وقابلية التوسع، وعدم التجانس، واستهلاك الطاقة، والتوحيد القياسي وغيرها [1].

تتم مناقشة الأمن والخصوصية بشكل متكرر في سياق إنترنت الأشياء. في كثير من الأحيان، يشير كل من الأمن والخصوصية– أو بشكل أكثر دقة، أمن وخصوصية المعلومات – إلى مفهومين مختلفين، حيث يشير أمن المعلومات إلى حماية البيانات من الوصول غير المصرح به (من قبل المتسللين) من خلال ضمان السرية والنزاهة والتوافر، وتشير خصوصية المعلومات إلى قدرة الفرد على التحكم فيمن يمكنه الوصول إلى بياناته في ظل أي ظروف ولأية أغراض. من الواضح أن كل من الأمن والخصوصية مفهومان مهمّان، مع الأخذ في الاعتبار كمية ونوع البيانات التي يحتمل أن تكون خاصة والتي تجمعها إنترنت الأشياء. فإن الأمن في سياق إنترنت الأشياء يتضمن أيضاً مفهوم السلامة، أي حماية البشر والبيئة والآلات من فشل النظام الذي قد يكون ضاراً [2]، يوضح الشكل (1) المفاهيم الأمنية الهامة في سياق تطبيقات انترنت الأشياء.



الشكل (1) الأمن والخصوصية في انترنت الأشياء [3]

تتكون السحابة من عدد كبير من المخدمات التي تستضيف التطبيقات المسؤولة عن تنفيذ عمليات المعالجة الحاسوبية الثقيلة على البيانات المجمعة من أجهزة انترنت الأشياء [4]، لذلك تكون الشبكة عرضة للعديد من الهجمات مثل هجوم الرجل في الوسط (Man in the Middle) MIM، Sinkhole attack، Vampire Attack، هجوم التشويش Jamming Attack، وأحد أهم الهجومات التي تعاني منها الشبكات محدودة المصادر هو هجوم الثقب الأسود Blackhole attack، الذي يُنفّذ على طبقة الشبكة بشكل أساسي بواسطة العقدة المهاجمة التي تقوم بإسقاط جميع الحزم المرسلة إلى عقدة أخرى الشكل (2)، بهدف سرقة المعلومات الهامة أو بهدف هدر موارد الطاقة بالشبكة[5]. على الرغم من أن هجوم الثقب الأسود يبدو بسيط من الناحية الهيكلية، إلا أنه من الصعب جداً ملاحظته لأن العقد التي تقوم بالهجوم لا تفعل شيئاً سوى إسقاط الحزم. يمكن أن تظل عقدة المهاجم غير ملحوظة في الشبكة لفترة طويلة أثناء تنفيذ إسقاط الحزمة.



الشكل (2) هجوم الثقب الأسود[7]

لحماية البيانات المتبادلة في الشبكة والمخزنة على السحابة يتم استخدام التشفير الذي يساعد على نقل البيانات بأمان عبر الوسيط اللاسلكي ويوفر الموثوقية والسرية وتكامل البيانات وعدم التنصل[6].

يتم تصنيف خوارزميات التشفير Encryption Algorithms في فئتين عامتين[6] هما خوارزمية التشفير المتماثل (Symmetric Encryption Algorithm) وتسمى تشفير المفتاح الخاص (Private-Key)، وخوارزمية التشفير غير متماثل (Asymmetric Encryption Algorithm) وتسمى تشفير المفتاح العام (Public-Key) الشكل (3).

تستخدم تقنية المفتاح المتماثل مفتاحاً واحداً يسمى المفتاح السري الذي يستخدم رياضيات أقل، وينتج عنه حساب أقل، من ناحية أخرى، تستخدم تقنية المفتاح غير المتماثل كلاً من المفاتيح العامة والخاصة، وتؤدي إلى مزيد من المعالجة وتستهلك المزيد من الطاقة لكن المفاتيح تكون أكثر قوة وأمان[8].

الشكل (3) تصنيف خوارزميات التشفير[8]

في إطار متطلبات الأمن والخصوصية وللتعامل مع تحديات أمان إنترنت الأشياء[8]، يمكن ذكر بعض البنود الأساسية لاختيار خوارزميات التشفير على النحو التالي:

1. حلول خفيفة الوزن ومتماثلة لدعم الأجهزة ذات الموارد المحدودة.
2. أنظمة إدارة مفاتيح خفيفة الوزن لتمكين إنشاء علاقات ثقة وتوزيع مواد التشفير باستخدام الحد الأدنى من موارد الاتصال والمعالجة، بما يتوافق مع طبيعة الموارد المحدودة لأجهزة انترنت الأشياء.
3. تقنيات التشفير التي تمكن من تخزين البيانات المحمية ومعالجتها ومشاركتها، دون أن يكون محتوى المعلومات في متناول الأطراف الأخرى.
4. تقنيات لدعم مفاهيم ("الخصوصية حسب التصميم")، بما في ذلك تحديد البيانات والمصادقة وإخفاء الهوية.

في شبكات الحساسات محدودة المصادر، يتطلب تشفير المفتاح المتماثل مزيداً من مساحة التخزين لتخزين المفتاح بين جميع عقد الشبكة، وفي تشفير المفتاح غير المتماثل، يلزم المزيد من وقت الحساب لتشفير البيانات وفك تشفيرها لذلك تم اقتراح نظام تشفير هجين في كثير من الدراسات والذي يدمج بين مزايا كل من خوارزميات التشفير المتماثل وغير متماثل لتوفير مزيد من الأمان على البيانات المراد تخزينها على السحابة.

تم تنظيم بقية هذه الورقة البحثية على النحو التالي:

تستعرض الفقرة (2) الدراسة المرجعية فيما يتعلق بتحقيق التكامل ومشاكل الأمن والخصوصية في أنظمة انترنت الأشياء وتقدم الفقرة (3) الطرق والمواد المتبعة لإنجاز البحث، بينما تصف الفقرة (4) النموذج المقترح لتحقيق التكامل الآمن بين انترنت الأشياء والحوسبة السحابية. كما يتم دراسة مجموعة من مقاييس الأداء ومقارنتها مع دراسات أخرى في الفقرة (5)، وأخيراً يتم ذكر بعض الاستنتاجات والتوصيات للنموذج المقترح في الفقرة (6).

1. الدراسة المرجعية:

أولى المحاولات لدمج شبكات الحساسات اللاسلكية مع السحابة عام 2009 [9]. يتألف النظام المعتمد مما يسمى بالأنابيب pipes والمرشحات filters مصممة من أجل النظام المستضاف على السحابة، الأنابيب عادة لا تنقل البيانات (القادمة من الحساسات) لكن بالعموم تقوم بتخزينها وتؤمن آلية اتصال موحدة لتوصيل المعلومات الى المرشحات. أما المرشحات تقوم بعمليات المعالجة ونقل المعلومات من الحساسات مثل التصفية (عمليات تخزين البيانات في قاعدة البيانات أو حذف البيانات عندما يتجاوز حدود عتبة ما).

يمكن تحقيق التكامل بين شبكات الحساسات اللاسلكية والحوسبة السحابية من خلال إنشاء نسخ احتياطية من الحساسات والمعلومات المخزنة عليها افتراضياً في السحابة، تتم عليها نفس العمليات الحسابية التي يتم اجراؤها على الحساسات الفعلية [9] من خلال نموذج بسيط يعمل على مبدأ الذاكرة الموزعة المشتركة (DSM-Distributed Shared Memory).

أو يمكن تحقيق التكامل بالاعتماد على مبدأ المعالجة متعددة المستويات حيث يتم تنفيذ وظائف محددة على كل مستوى من مستويات الشبكة، حيث يتم نقل البيانات المجمعة كل 30 ثانية في مستوى التحسس SPL (Sensor Processing Level) إلى مستوى تحليل البيانات DAL (Data Analysis Level) الذي يعتبر الواجهة المحلية بين الحساسات والمنصات الحوسبية والمستخدمين والاخصائيين ويتكون من خوارزميات محلية لتجميع البيانات وإنذار الأحداث التي يتم تشغيلها ومنه إلى السحابة حيث يسمح مستوى التنبؤ السحابي CPL (Cloud Prediction Level) بتخزين وترابط البيانات والتنبؤ، ويوفر حلولاً لضمان سرعة رد الفعل في حالة الطوارئ، إضافة إلى استخدام خوارزميات التنبؤ المعقدة. هذا النهج يحل مشكلة مركزية تخزين البيانات ومعالجتها في السحابة، الأمر الذي يتطلب عدد كبير من الموارد [10].

اقترح الباحثون في [11] بنية عامة تسمى إنترنت الأشياء كخدمة IoTaaS (IoT as a service) وتعالج التحديات التي تعيق التكامل بين انترنت الأشياء والحوسبة السحابية، وتقدم حلاً شاملاً لتطبيقات إنترنت الأشياء المختلفة. تستخدم البنية الخدمات السحابية الحالية وتقترح إضافة خدمات جديدة لدعم التطبيقات المختلفة وللتحقق من صحة البنية تم تطبيق بعض سيناريوهات المدينة الذكية، تدعم البنية الأمان من خلال توفير بوابة آمنة تربط نظام إنترنت الأشياء بالسحابة، ودعم تشفير البيانات التي يتم تمريرها من / إلى السحابة، ويقوم مدير المصادقة بضمان وصول الأطراف المصرح لها فقط إلى نظام إنترنت الأشياء والخدمات السحابية، وتم تفويض جميع عمليات قاعدة البيانات إلى مدير ومعالج البيانات لضمان تنفيذ العمليات الصحيحة فقط.

يتم تشغيل أجهزة إنترنت الأشياء الصغيرة في الغالب بواسطة طاقة البطارية، وتمتلك قدراً محدوداً من الذاكرة وقدرة المعالجة، وتصميم آلية أمنية يمكن أن تتناسب مع هذه الأجهزة الصغيرة مهمة شاقة كما أن هنالك مخاوف من مسؤولي مركز البيانات السحابية حيث يكون لهم في هذه الحالة القدرة على الوصول إلى البيانات التي تم جمعها وتعديلها، ومن أجل حماية هذه البيانات تم اقتراح تقنيات مختلفة مثل التشفير[4].

أظهرت نتائج محاكاة برنامج LabVIEW 2016 لدراسة عدة خوارزميات تشفير في [12] أن AES هي أفضل تقنية تشفير من حيث السرعة والإنتاجية والأقل من حيث استهلاك الطاقة، أي يمكن الحصول على كفاءة أعلى مع وقت أقل على الرغم من تعقيد تصميم AES-256، لأنه يمكنه تشفير كتلة بحجم 128 بت (وهو أكبر تشفير كتلة لخوارزميات التشفير) في 14 دورة فقط. ثم تأتي خوارزمية معيار تشفير البيانات DES (Data Encryption Standard) بالمرتبة

الثانية كأفضل أداء أثناء عمليات التشفير وفك التشفير، بينما كانت 3DES (Triple DES) و RC2 تقدم نفس مستوى الأداء، أما RSA(Rivest–Shamir–Adleman) أعطت أدنى مستوى أداء من حيث السرعة والإنتاجية.

كما اقترح الباحثون في [6] نموذج مصادقة معتمد على الهوية من أجل شبكات انترنت الأشياء الهجينة بالاعتماد على الشبكات المعرفة برمجياً SDN-Software Defined Network، تقوم وحدة التحكم المركزية في SDN بترجمة الهويات المختلفة الخاصة بالتكنولوجيا من الأجهزة المختلفة إلى هوية مشتركة تستند إلى العناوين الافتراضية IPv6(Internet Protocol v6)وتقوم بمصادقة الأجهزة والبوابات. يتم توليد المفاتيح باستخدام ECC للأجهزة والبوابة، أظهرت النتائج أن المخطط آمن ضد هجمات التنكر وهجمات MIMوهجمات الإعادة.

وفي سياق التشفير الهجين اقترح البحث [13] نظام تشفير هجين من خوارزميات مختلفة لتأمين محاسن من كل من التشفير المتماثل وغير متماثل باستخدام ECDH (Elliptic-curve Diffie–Hellman) لتوليد المفاتيح وإجراء التوقيع الرقمي لتحقيق المصادقة وبعد ذلك يتم استخدام AES للتشفير، وأثبتت العديد من البحوث الأخرى كفاءة التشفير الهجين في تأمين الحماية المطلوبة والحفاظ على مصادر الشبكة.

واقترح الباحثون في [16] نهج تشفير هجين بالدمج بين خوارزمية ECC وخوارزمية ElGamal حيث يتم تحميل المعلومات المشفرة في السحابة للتخزين، في قنوات مختلفة وبكلمات مرور مختلفة، إذا قام المستخدم بمصادقة الاستراتيجيات، فيمكن تنزيل البيانات المشفرة ويتم فك تشفير البيانات الأصلية بواسطة مفتاح متزامن باستخدام خوارزمية ECC-ElGamal وتم تنفيذ المحاكاة باستخدام MATLAB 2014a وحساب مقاييس الأداء المختلفة من حيث وقت التنفيذ ، ونسبة تسليم الحزم ،والتأخير ومقارنة هذه النتائج بالطرق التقليدية ووجد أنها تقدم 12%، 31% ، 8% فيما يتعلق بنسبة تسليم الحزم والتأخير ووقت التنفيذ.

سيتم في هذه الورقة اعتماد نهج التشفير الهجين في الخوارزمية المقترحة لتطوير تكامل آمن بين انترنت الأشياء والحوسبة السحابية.

2. مواد وطرق البحث:

تم استخدام جهاز حاسوب بمعالج core i5 (2.20 Ghz) – 8 GB RAM نظام تشغيل ويندوز 10 (64 Byte)، استخدمت الأداة الافتراضية VMware virtual Machine لتشغيل نظام Ubuntu (64 Byte) و (8 GB RAM) وتم تنفيذ المحاكاة علىCONTIKI COOJA 3.0 الذي يدعم شبكات انترنت الأشياء ويدعم جميع البروتوكولات في مجال الشبكات كما أنه يعتبر emulator وليسsimulator أي أن أداءه أقرب للواقع لأنه يقوم بتشغيل حقيقي للأجهزة الموجودة في الشبكة مما يجعل النتائج التي نحصل عليها دقيقة أكثر وتحاكي الواقع، تم العمل على عقد من نوع Skymote، لغة المحاكاة المستخدمة C.

تم تمكين مجموعة من عقد الحساسات اللاسلكية باستخدام شبكة (IEEE 802.15.4)، والتوجيه باستخدام بروتوكول RPL (Routing Protocol for Low Power and Lossy Networks) ويتم ربط الشبكة بالسحابة باستخدام بروتوكول MQTT (Message Queue Telemetry Transport Protocol) كبروتوكول طبقة تطبيقات، ثم يتم تأمين الاتصال بين كافة العقد بالشبكة مع المخدم السحابي باستخدام التشفير بالنموذج الهجين وفق ما يلي:

- توليد المفاتيح في العقدة المجمعة (Sink node) وتوزيعها على عقد الحساسات باستخدام ECC وهو نهج لخوارزمية تشفير المفتاح العام على أساس البنية الجبرية للمنحنيات الإهليلجية للحقول المحدودة يساعد بتأسيس مفتاح سري بين طرفي اتصال يتبادلان البيانات عبر شبكات عامة، يساعد على توليد مفاتيح بحجم مناسب للعقد محدودة

المصادر ومن الصعب تخمين المفاتيح الخاصة بهذه الخوارزمية.

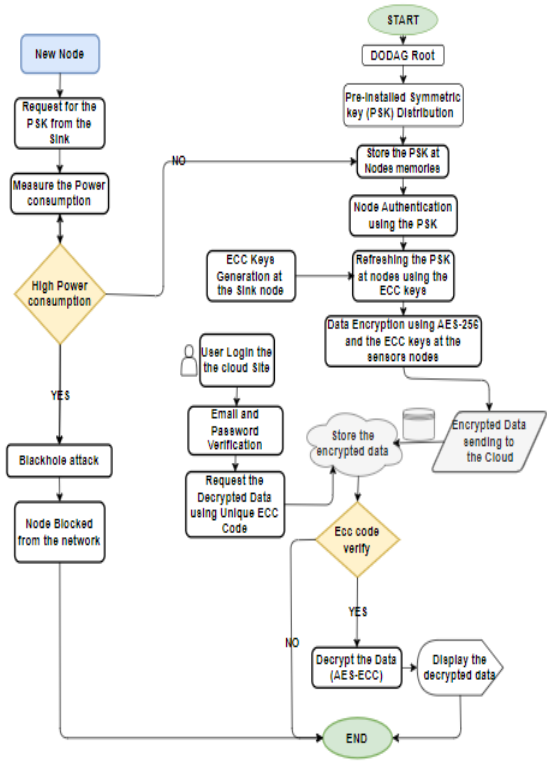
- استخدام خوارزمية AES في كل عقدة على حدى لتشفير بيانات الحساسات وإرسال البيانات مشفرة إلى السحابة، تؤمن الخوارزمية حماية فعالة للبيانات أثناء نقلها وتجنب تعديلها، لتوفير بيئة حوسبة موثوقة حيث يساعد النموذج المقترح في تحسين قوة عملية التشفير والأمان.

كما تم تصميم موقع لتقديم خدمة التخزين السحابي وإضافة خوارزمية التشفير الهجين المقترحة على الموقع بحيث يمكن التحقق من عمل الخوارزمية وأن البيانات مخزنة بطريقة آمنة ومحمية على السحابة ويمكن فك تشفيرها للمستخدمين المخولين بالدخول فقط.

3. النموذج المقترح لتطوير التكامل:

في النموذج المقترح المبين وفق المخطط التدفقي في الشكل (4)، يتم التنفيذ وفق المراحل التالية:

1. عند تأسيس الشبكة يقوم بروتوكول RPL بتأسيس مسارات التوجيه وتعيين العقدة الجذر Sink وفق مخطط DODAG (Destination Oriented Directed Acyclic Graphs) والتي تقوم بتوزيع المفاتيح PSK (Pre-installed Symmetric Key)، حيث تقوم العقد بتخزين المفاتيح في ذاكرتها الخاصة لتقوم بحماية رسائل التحكم المتبادلة بالشبكة لإجراء عملية المصادقة، يتم بشكل دوري تحديث المفاتيح بغرض الحماية.
2. توليد المفاتيح في العقدة sink باستخدام خوارزمية ECC وتوزيعها على العقد في الشبكة.
3. تحديث المفتاح المتناظر المخزن (PSK) بالمفتاح الذي يتم توليده في العقدة Sink باستخدام خوارزمية ECC لضمان الموثوقية وتأمين مفتاح التشفير.
4. تطبيق خوارزمية AESفي العقد لتشفير البيانات.
5. نقل بيانات كافة العقد بالشبكة مشفرة إلى المخدم السحابي.
6. فك تشفير البيانات عند الطلب من قبل المستخدم وفق استراتيجيات التحكم بالوصول.
7. تطبيق واكتشاف هجوم الثقب الأسود على الشبكة للتحقق من حصانة الشبكة وفعالية الآلية المقترحة.



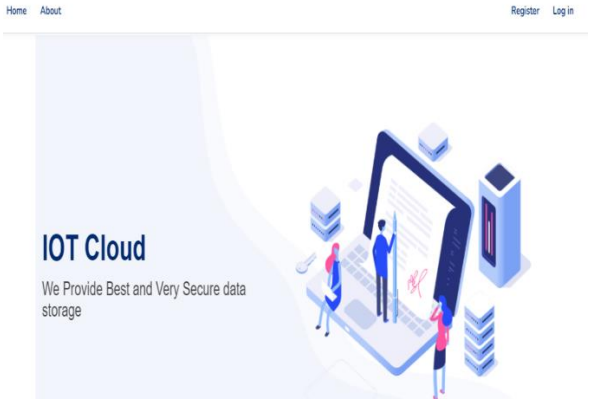
الشكل (4) المخطط التدفقي للنموذج المقترح

وتم تنفيذ العمل في ثلاث سيناريوهات على عدد متزايد من العقد بهدف دراسة تأثير عمل الخوارزمية على تزايد كمية البيانات المتبادلة (من أجل 10–15–20 عقدة بالترتيب) بمساحة شبكة ($100*100\ m^2$):

- السيناريو الأول (النموذج الأساسي): دراسة شبكة انترنت الأشياء متصلة بالمخدم السحابي دون تطبيق أي خوارزميات تشفير.
- السيناريو الثاني (سيناريو التشفير): دراسة تطبيق خوارزمية التشفير الهجين المقترحة على نفس الشبكة في السيناريو الأول ومقارنة النتائج لكل من معدل تسليم الحزم واستهلاك الطاقة وزمن تنفيذ الخوارزمية المقترحة للتشفير.

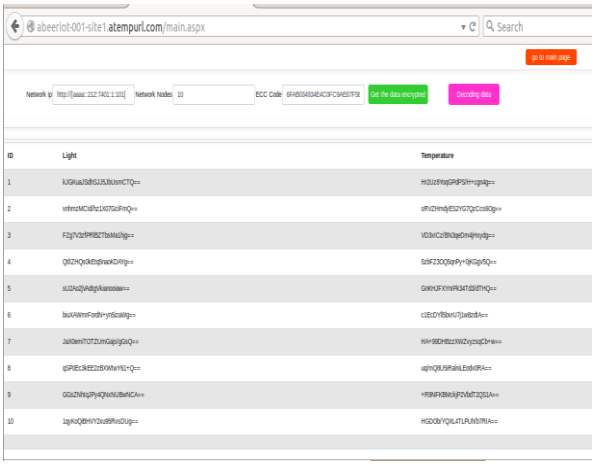
• السيناريو الثالث (سيناريو الهجوم): تطبيق هجوم الثقب الأسود على الشبكة وكشف الهجوم مع توضيح فائدة وسيلة الحماية المقترحة.

تم توصيل المحاكي COOJA مع موقع سحابي smarterasp.net الذي يعطي إمكانية بناء سحابة خاصة الشكل (5) وحجز وتعديل الخوارزميات حسب الحاجة عن طريق مجموعة من الخدمات المتنوعة.



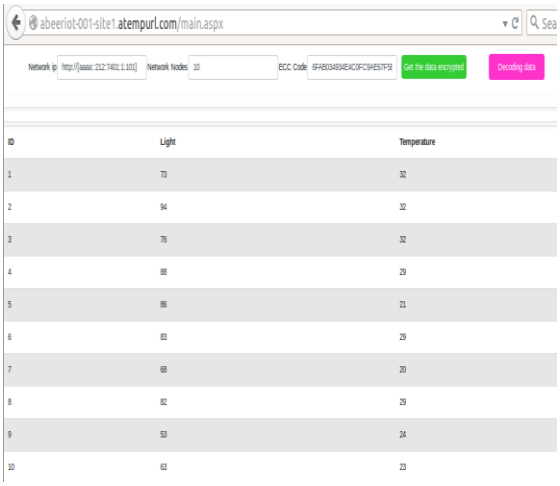
الشكل (5) واجهة الموقع السحابي

عرض قيم الحساسات المرسلة إلى الموقع السحابي للتخزين مشفرة وإجراء عملية فك التشفير فقط من قبل المستخدمين المخولين بالدخول الذين لديهم كود فك التشفير الخاص بالشبكة مما يؤمن السرية والموثوقية.



الشكل (6) عرض قيم الحساسات مشفرة على الموقع السحابي

عرض قيم الحساسات بعد عملية فك التشفير باستخدام كود فك التشفير الخاص:



الشكل (7) عرض قيم الحساسات بعد فك التشفير على الموقع السحابي

4. النتائج والمقارنة:

تم اختبار وتحليل أداء النموذج المقترح ومقارنته مع النموذج المرجعي ثم مقارنة النتائج مع الأبحاث الحالية.

5-1 معدل تسليم الحزم (PDR%):

يشير معدل تسليم الحزم PDR (Packet Delivery Ratio) إلى نسبة عدد حزم البيانات الإجمالية المستلمة في الوجهة إلى العدد الإجمالي لحزم البيانات الكلية المرسلة أثناء المحاكاة[7]، يتم التعبير عنه وفق المعادلة:

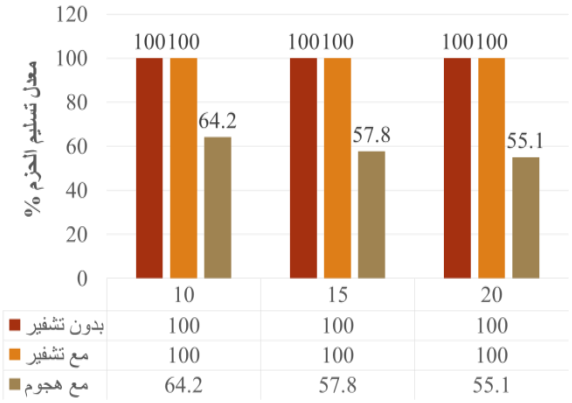
$$PDR\ \% = \frac{\sum_{i\varepsilon S} npacketsReceived(i.d)}{\sum_{i\varepsilon S} npacketsSent(i.s)}$$

حيث S عبارة عن مجموعة من الجلسات التي تم إنشاؤها أثناء المحاكاة و(i.d) npacketsReceived هي عدد الحزم المستلمة في الوجهة d و(i.s)npacketsSent هي عدد الحزم المرسلة من المصدر خلال الجلسة i.

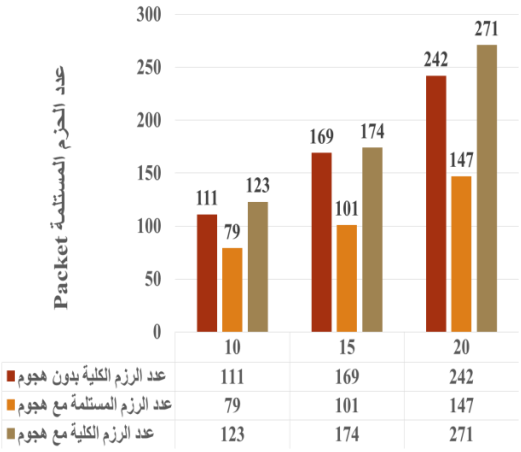
نلاحظ أنه من أجل السيناريو الأول والثاني لا يوجد أي خسارة بالحزم حيث معدل التسليم 100% أي أن الخوارزمية المقترحة لم تسبب أي خسارة في الحزم في الشبكة، أما بالنسبة لسيناريو الهجوم نجد أنه من الواضح أن العقدة المهاجمة تسبب ضياع كبير بالحزم بالشكل (8).

كما يمكن من المخطط في الشكل (9) مراقبة عدد الحزم المستلمة، وملاحظة الزيادة الملحوظة في العدد الكلي

للرسائل المتبادلة في العقد بالشبكة عند تطبيق هجوم الثقب الأسود والزيادة تكون بسبب زيادة عدد رسائل التحكم التي ترسلها العقد التي تعرضت للهجوم محاولة إعادة الانضمام للشبكة.



الشكل (8) معدل تسليم الحزم PDR



الشكل (9) عدد الحزم الكلية في حالة الهجوم

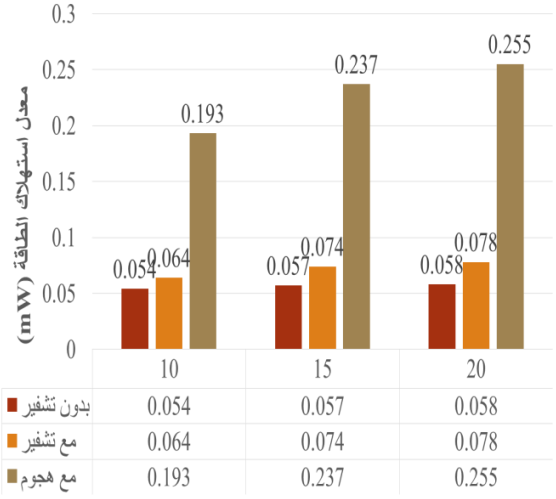
5-2 معدل استهلاك الطاقة:

يعطي المحاكي مجموعة من القيم المتعلقة باستهلاك الطاقة بواحدة (mW) من قبل كل عقدة على حدى وبشكل تفصيلي (CPU power، LPM power، Listen power، Transmit power) ونتيجة نهائية لاستهلاك الطاقة بكل عقدة وهي مجموع كل القيم السابقة، وبشكل وسطي لكامل عملية المحاكاة، ويتم التعبير استهلاك الطاقة في الشبكة وفق المعادلة[15]:

$$power\ (mW) = \frac{Energest_{value} \times current \times voltage}{RTIMER\_SECOND \times Runtime}$$

Voltage, Current, Energest value قيم الطاقة والتيار والفولط يتم أخذها من المحاكي SECOND, RTIMER هو تردد ساعة.

ومن الشكل (10) نجد أن التزايد القليل في الطاقة المستهلكة بسبب عملية التشفير تزايد مقبول بسبب عملية توليد المفاتيح والتشفير ولا يؤثر على عمل الشبكة، لكن عند تطبيق هجوم الثقب الأسود يمكن ملاحظة الزيادة الملحوظة لاستهلاك الطاقة والزيادة ناتجة عن رغبة العقد الضحية في إعادة الانضمام إلى الشبكة فترسل المزيد من رسائل التحكم.



الشكل (10) معدل استهلاك الطاقة(mW)

5-3 زمن تنفيذ الخوارزمية:

تم الحصول عليه عن طريق استخدام حاسوب بمواصفات معالج Core i5 من الجيل السابع و(8RAM) وهارد SSD لكون النتائج في سرعة التشفير تتغير تبعاً لحالة الجهاز جميع القيم مقاسة ms بالطبع يتم توزيع المفاتيح بعد اكتشاف sink لجميع العقد المحيطة بها، وفق الآلية:

حساب زمن تنفيذ الخوارزمية:

يتم حساب زمن تنفيذ الخوارزمية عن طريق استخدام كود js (Java Script) حيث يقوم script بحساب زمن عمل كل عقدة وفق عدة مراحل، من أجل 10 عقد كمثال.

حساب زمن توزيع المفاتيح:

عداد الحلقة مساو لعدد عقد الشبكة المراد التوزيع عليها

```
while(counter<10){
انتظار وصول الرسالة
YIELD_THEN_WAIT_UNTIL(msg. equals "get")
في حال وصول رد تخزينه في plugin
plugin=mote. Get Simulation(). Get Cooja (). Get Startd Plugin)"org. conti kios. cooja. plugins. Log Listener"
في حال وصول رد يتم زيادة العداد للانتقال للعقدة الثانية:
{ if (plugin != null)
++؛counter
++؛plugins
log.log("LogListener: Setting filter: " +
؛plugin.getFilter() + "\n")
if (plugin.getFilter() == null ||
} !plugin.getFilter().equals("Contiki"))
else{ }؛plugin.setFilter("Contiki")

} }؛plugin.setFilter("MAC")
```

عند انتهاء الحلقة يتم طباعة رسالة sink بالانتهاء من توزيع المفاتيح على العقد مع زمن تنفيذ العملية حيث id هو معرف عقدة sink

```
؛log.log(time + ":" + id + ":" + msg + "\n")
()؛YIELD
```

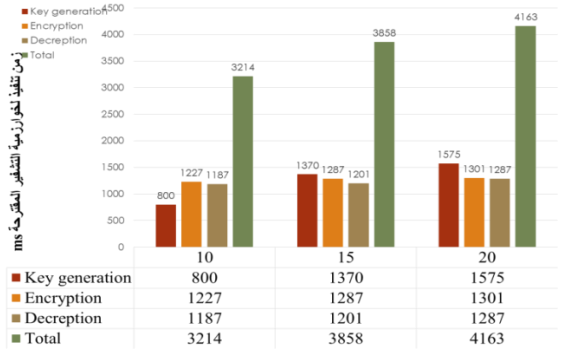
- حساب زمن التشفير داخل العقدة: يتم انتظار رسالة انتهاء التشفير من قبل عقدة ما ولتكن 3

```
؛log.log("waiting for output from mote 3\n")
؛WAIT_UNTIL(id == 1 && msg.equals("F"))
```

- حساب زمن فك التشفير داخل sink:
- يتم وضع قيد زمني لإنهاء الانتظار ومن ثم يتم الحصول على قيمة الزمن الإجمالي من عقدة sink التي لها (ID=1)

```
TIMEOUT(50000, log.log("last message: " + msg)
(؛+ "\n")
؛WAIT_UNTIL(msg. equals('finish')
() ؛log.testOK
```

يبين الشكل (11) الزمن اللازم لتنفيذ الخوارزمية من أجل عدد عقد متزايد 10–15–20 عقدة بالترتيب، نلاحظ أن زمن تنفيذ الخوارزمية يتزايد مع تزايد حجم البيانات في الشبكة وذلك لتزايد عدد العقد المراد تأمينها وكمية البيانات اللازم تشفيرها.

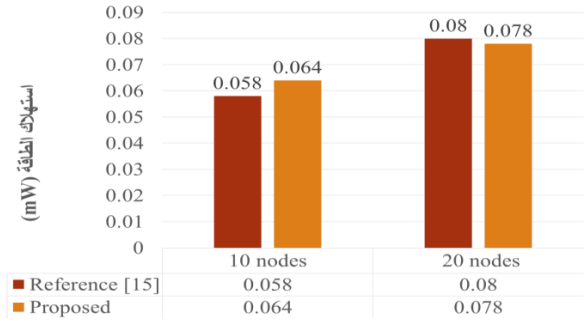


الشكل (11) زمن تنفيذ الخوارزمية (ms)

4-5 مقارنة نتائج النموذج المقترح مع دراسة سابقة:

- **مقارنة استهلاك الطاقة:**

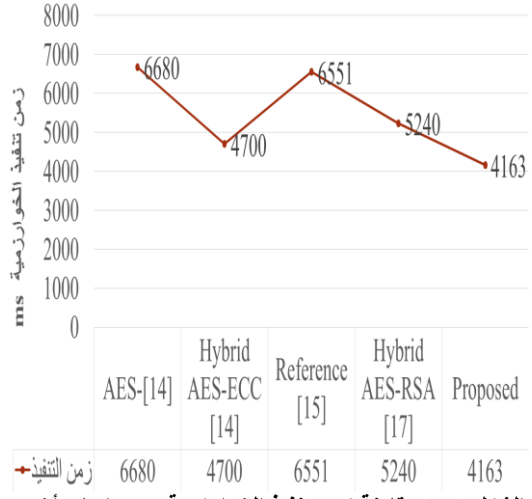
اقترح الباحثون نموذج تشفير هجين في [15] باستخدام خوارزمية AES لتشفير البيانات معECDH لتوليد المفاتيح والمصادقة ونلاحظ أن النموذج المقترح يقدم حلول مناسبة وأفضل لاستهلاك الطاقة كلما زاد معدل تبادل البيانات في الشبكة.



الشكل (12) مقارنة معدل استهلاك الطاقة مع دراسات أخرى[15]

- **مقارنة زمن تنفيذ الخوارزمية:**

ساهم النموذج المقترح في تقليل زمن تنفيذ الخوارزمية مما يؤدي تأخير أقل واستهلاك طاقة أقل، وبذلك نجد أن النموذج المقترح يقدم حل أمني خفيف الوزن وسريع مقارنة مع الدراسات [14]، [15]،[17] .



الشكل (13) مقارنة زمن تنفيذ الخوارزمية مع دراسات أخرى

5-5 كشف هجوم الثقب الأسود:

في هجوم الثقب الأسود تهدف العقدة المهاجمة إلى تعطيل الخدمة وسرقة المعلومات الهامة والخاصة بالمستخدمين، في النموذج المقترح يمكن كشف الهجوم عند محاولة عقدة جديدة الانضمام إلى الشبكة والحصول على المصادقة سوف تسبب استهلاك مرتفع في الطاقة كما في الشكل (10) وأيضاً يمكن كملاحظة عدد الحزم المتزايد بشكل كبير مع محاولة عقدة مهاجمة الانضمام الى الشبكة من الشكل (9)، وعند كشف القعدة المهاجمة سيتم منعها من الانضمام إلى الشبكة وإعادة توزيع مفاتيح التشفير بشكل فوري من عقدة sink.

كما أن العقدة المهاجمة لن تكون قادرة على فك تشفير البيانات في الشبكة وذلك بسبب عملية التشفير وقوة المفاتيح المستخدمة ولن تتمكن العقدة المهاجمة من الحصول على المفاتيح أو تخمينها.

5. الاستنتاجات والتوصيات:

ساعد النموذج المقترح في هذا البحث على تحقيق تكامل آمن بين انترنت الأشياء والحوسبة السحابية باستخدام نموذج التشفير الهجين(AES-ECC) في تأمين اتصال موثوق بين عقد الحساسات في الشبكة والسحابة وتخزين بيانات الحساسات بشكل آمن ومشفر وذلك من دون التأثير على معدل تسليم الحزم، واستهلاك الطاقة وبزمن تنفيذ أقل مقارنة بدراسات أخرى. كان التأثير المشترك لكل من ECC وAES مناسب للتقنية المقترحة في التخزين السحابي للحصول على النظام الآمن.

الهدف من البحث هو الدمج بين توافرية المصادر والحفاظ على الموثوقية والخصوصية عند تحقيق التكامل بين انترنت الأشياء والحوسبة السحابية مما جعله يتفوق على دراسات أخرى، وبما أن لكل تطبيق متطلباته وشروطه لذلك فإن هذه الدراسة موجهة بشكل أساسي لشبكات انترنت الأشياء بعقد غير متحركة وعشوائية النشر في حقل دراسة يتم فيه جمع البيانات من الحساسات وإرسالها إلى السحابة لتخزينها بسرية وإجراء بعض العمليات الحسابية عليها ونظراً لسرعة أداء النموذج المقترح واستهلاك الطاقة المنخفض مقارنة بدراسات أخرى يمكن استخدام النموذج في العديد من تطبيقات انترنت الأشياء التي تحتاج السرعة ومراعاة محدودية المصادر والسرية في نقل وتخزين البيانات الحساسة.

ومع ذلك، لا تزال هناك حاجة إلى قدر كبير من الأمان في المستقبل لتوسيع مفهوم الحوسبة السحابية من خلال تقنيات التشفير. في المستقبل، يمكن تحسين هذا البحث عن طريق زيادة أمان النهج الهجين بإضافة طبقات أمان متعددة لتعزيز إنتاجية وكفاءة النظام.

التمويل: هذا البحث ممول من جامعة دمشق وفق رقم التمويل(501100020595).

References:

1- Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroiu, A. M. (2019), "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges" Applied Computing and Informatics, Vol. ahead-of-print No. ahead-of-print, page3.

2- Sunyae, A., 2020, "Internet Computing Principles of Distributed Systems and Emerging Internet-Based Technologies" © Springer Nature Switzerland AG.

3- https://metrolush. com/key-enabler-for-iiot- applications, Posted on April 11, 2019-YOLANDO B. ADAMS /Retrieved by 28 Aug 2019.

4- Rayes, A., and Salam, S., 2019, "Internet of Things from Hype to Reality_ the Road to Digitization" Second Edition, © Springer Nature Switzerland AG.

5- Sokat, B., 2020, "Blackhole Attacks In Iot Networks" Master Thesis, Computer Engineering, Engineering and Sciences of İzmir Institute of Technology, İZMİR, 43p.

6- Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A.,and Kayssi, A., 2016,"Identity-Based Authentication Scheme for the Internet of Things", 978-1-5090-0679-3/16/$31.00 ©2016 IEEE.

7- Ahmed, F., and Young-Bae Ko, 2016, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1684.

8- HASSAN, A., ISMAIL, A., 2017, "Evaluation of encryption algorithms for IOT security" Bachelor of Science in Communication Engineering, Communication Engineering Department, University of almughtaribeen, Khartoum, Sudan, 49p.

9- Langendoerfer, P., Piotrowski, K., Díaz, M., and Rubio, B., 2012, "Distributed Shared Memory as an Approach for Integrating WSNs and Cloud Computing" IEEE.

10- Chenaru, O., Mihai, V., Popescu, D., and Ichim, L., 2018, Member, IEEE "Integration of WSN, IoT and Cloud Computing in Distributed Monitoring System for Aging Persons in Active Life" 26th Mediterranean Conference on Control and Automation (MED) Zadar, Croatia.

11- Othman, M. M., El-Mousa, A., 2020, "Internet of Things & Cloud Computing Internet of Things as a Service Approach", 2020 11th International Conference on Information and Communication Systems (ICICS), Amman, Jordan.

12- Latif, I.H., 2020, "Time Evaluation Of Different Cryptography Algorithms Using Labview" 2020 IOP Conf. Ser.: Mater. Sci. Eng. 745 012039View.

13- Kunchok, T., Prof. Kirubanand V.B., 2018 "A Lightweight hybrid encryption technique to secure IoT data transmission"- International Journal of Engineering & Technology, 7 (2.6) 236-240.

14- Rehman, S., Bajwa, N.,Shah, M., Aseeri , A., and Anjum, A.,2021, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage" Electronics 2021, 10, 2673.

15- Alzahrani,S.M.,2022 Secure Authenticated Key Exchange For Enhancing The Security Of Routing Protocol For Low-Power And Lossy Networks ,Master thesis of Science in Cyber Security, Wright State University.

16- Kumari C. S., Asha C. N., Rajashekhar U., K. Viswanath, 2022, "Performance Analysis of Cloud-based Health Care Data Privacy System Using Hybrid Techniques", INTERNA-TIONAL JOURNAL OF BIOLOGY AND BIOMEDICAL ENGINEERING, Volume 16.

17- Al-Bayati, A. S., 2021, Enhancing Performance of Hybrid AES, RSA and Quantum Encryption Algorithm , Master thesis of Philosophy, Anglia Ruskin University.