مجلة جامعة حمص

سلسلة العلوم الهندسية الميكانيكية والكهربائية والمعلوماتية

مجلة علمية محكمة دورية

المجلد 47 . العدد 5

1447 هـ - 2025 م

د.محمد فراس رمضان	عضو هيئة التحرير
د. مضر سعود	عضو هيئة التحرير
د. ممدوح عبارة	عضو هيئة التحرير
د. موفق تلاوي	عضو هيئة التحرير
د. طلال رزوق	عضو هيئة التحرير
د. أحمد الجاعور	عضو هيئة التحرير
د. الياس خلف	عضو هيئة التحرير
د. روعة الفقس	عضو هيئة التحرير
د. محمد الجاسم	عضو هيئة التحرير
د. خليل الحسن	عضو هيئة التحرير
د. هيثم حسن	عضو هيئة التحرير
د. أحمد حاج موسى	عضو هيئة التحرير

تهدف المجلة إلى نشر البحوث العلمية الأصيلة، ويمكن للراغبين في طلبها الاتصال بالعنوان التالي:

رئيس تحرير مجلة جامعة حمص

سورية . حمص . جامعة حمص . الإدارة المركزية . ص . ب (77)

. هاتف / فاكس : 2138071 31 963 ++

. موقع الإنترنت : www.homs-univ.edu.sy

. البريد الالكتروني : journal.homs-univ.edu.sy

ISSN: 1022-467X

شروط النشر في مجلة جامعة حمص

الأوراق المطلوبة:

- 2 نسخة ورقية من البحث بدون اسم الباحث / الكلية / الجامعة) + CD / word من البحث منسق حسب شروط المجلة.
- طابع بحث علمي + طابع نقابة معلمين.
- **اذا كان الباحث طالب دراسات عليا:**

يجب إرفاق قرار تسجيل الدكتوراه / ماجستير + كتاب من الدكتور المشرف بموافقته على النشر في المجلة.

- **اذا كان الباحث عضو هيئة تدريسية:**

يجب إرفاق قرار المجلس المختص بإنجاز البحث أو قرار قسم بالموافقة على اعتماده حسب الحال.

- **اذا كان الباحث عضو هيئة تدريسية من خارج جامعة البعث :**

يجب إحضار كتاب من عمادة كليته تثبت أنه عضو بالهيئة التدريسية و على رأس عمله حتى تاريخه.

- **اذا كان الباحث عضواً في الهيئة الفنية :**

يجب إرفاق كتاب يحدد فيه مكان و زمان إجراء البحث ، وما يثبت صفته وأنه على رأس عمله.

- **يتم ترتيب البحث على النحو الآتي بالنسبة لكليات (العلوم الطبية والهندسية والأساسية والتطبيقية):**

عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1- مقدمة

2- هدف البحث

3- مواد وطرق البحث

4- النتائج ومناقشتها .

5- الاستنتاجات والتوصيات .

6- المراجع.

- **يتم ترتيب البحث على النحو الآتي بالنسـبة لكليات (الآداب – الاقتصـاد– التربية – الحقوق – السياحة – التربية الموسيقية وجميع العلوم الإنسانية):**
- عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1. مقدمة.
2. مشكلة البحث وأهميته والجديد فيه.
3. أهداف البحث و أسئلته.
4. فرضيات البحث و حدوده.
5. مصطلحات البحث و تعريفاته الإجرائية.
6. الإطار النظري و الدراسات السابقة.
7. منهج البحث و إجراءاته.
8. عرض البحث و المناقشة والتحليل
9. نتائج البحث.
10. مقترحات البحث إن وجدت.
11. قائمة المصادر والمراجع.

7- يجب اعتماد الإعدادات الآتية أثناء طباعة البحث على الكمبيوتر:

أ- قياس الورق 17.5×25 B5.

ب- هوامش الصفحة: أعلى 2.54- أسفل 2.54 – يمين 2.5- يسار 2.5 سم

ت- رأس الصفحة 1.6 / تذييل الصفحة 1.8

ث- نوع الخط وقياسه: العنوان . Monotype Koufi قياس 20

ـ كتابة النص Simplified Arabic قياس 13 عادي ـ العناوين الفرعية Simplified Arabic قياس 13 عريض.

ج . يجب مراعاة أن يكون قياس الصور والجداول المدرجة في البحث لا يتعدى 12سم.

8- في حال عدم إجراء البحث وفقاً لما ورد أعلاه من إشارات فإن البحث سيهمل ولا يرد البحث إلى صاحبه.

9- تقديم أي بحث للنشـر في المجلة يدل ضـمناً على عدم نشـره في أي مكان آخر، وفي حال قبول البحث للنشر في مجلة جامعة البعث يجب عدم نشره في أي مجلة أخرى.

10- الناشر غير مسؤول عن محتوى ما ينشر من مادة الموضوعات التي تنشر في المجلة

11- تكتب المراجع ضمن النص على الشكل التالي: [1] ثم رقم الصفحة ويفضل استخدام التهميش الإلكتروني المعمول به في نظام وورد WORD حيث يشير الرقم إلى رقم المرجع الوارد في قائمة المراجع.

تكتب جميع المراجع باللغة الانكليزية (الأحرف الرومانية) وفق التالي:

آ . إذا كان المرجع أجنبياً:

الكنية بالأحرف الكبيرة ـ الحرف الأول من الاسم تتبعه فاصلة ـ سنة النشر ـ وتتبعها معترضة (–) عنوان الكتاب ويوضع تحته خط وتتبعه نقطة ـ دار النشر وتتبعها فاصلة ـ الطبعة (ثانية . ثالثة) . بلد النشر وتتبعها فاصلة . عدد صفحات الكتاب وتتبعها نقطة.

وفيما يلي مثال على ذلك:

–MAVRODEANUS, R1986– **Flame Spectroscopy**. Willy, New York, 373p.

ب . إذا كان المرجع بحثاً منشوراً في مجلة باللغة الأجنبية:

ـــ بعد الكنية والاسم وسنة النشر يضاف عنوان البحث وتتبعه فاصلة، اسم المجلد ويوضع تحته خط وتتبعه فاصلة ـــ المجلد والعدد (كتابة مختزلة) وبعدها فاصلة ـــ أرقام الصفحات الخاصة بالبحث ضمن المجلة.

مثال على ذلك:

BUSSE,E 1980 Organic Brain Diseases **Clinical Psychiatry News** , Vol. 4. 20 – 60

ج. إذا كان المرجع أو البحث منشوراً باللغة العربية فيجب تحويله إلى اللغة الإنكليزية و التقيد بالبنود (أ و ب) ويكتب في نهاية المراجع العربية: (المراجع In Arabic)

رسوم النشر في مجلة جامعة حمص

1. **دفع رسم نشر (50000) ل.س أربعون ألف ليرة سورية عن كل بحث لكل باحث يريد نشره في مجلة جامعة البعث.**
2. **دفع رسم نشر (200000) ل.س مئة الف ليرة سورية عن كل بحث للباحثين من الجامعة الخاصة والافتراضية .**
3. **دفع رسم نشر (200) مئتا دولار أمريكي فقط للباحثين من خارج القطر العربي السوري .**
4. **دفع مبلغ (15000) ل.س ستة آلاف ليرة سورية رسم موافقة على النشر من كافة الباحثين.**

المحتوى

اسم البحث	اسم الباحث	الصفحة
تحسين أمن الاتصالات والإدارة المثلى لبروتوكول Fieldbus في أنظمة التحكم الإشرافي باستخدام DNP3-OPC	د.مسعود الأتاسي	42-11
تأثير المعالجة الحرارية المسبقة T4 على خصائص الوصلة الملحومة بطريقة لحام المزج الاحتكاكي لسبيكة الألمنيوم AA-6082-	ريم قاص بولات د.محمود الأسعد	68-43
تقييم استهلاك الموارد لخوارزميات التعلم الآلي في كشف الشذوذ في شبكات سلاسل الكتل	علي عطية أ.د.ماهر عباس د.وسيم رمضان	108-69
تحديد العتبة المثلى للمعاملات الشاذة باستخدام التعلم الآلي لتحسين أمن سلاسل الكتل	علي عطية أ.د.ماهر عباس د.وسيم رمضان	142-109
دراسة تجريبية لتأثير نوع عملية الصقل على السلوك الميكانيكي للفولاذ الكربوني	محسن عدره	166-143

تصميم خوارزمية كشف الاحتيال في مواقع التجارة الإلكترونية بهدف تحسين الدقة والسرعة في عمليات الكشف	علي إبراهيم د.بسيم عمران	190-167

تحسين أمن الاتصالات والإدارة المثلى لبروتوكول Fieldbus في أنظمة التحكم الإشرافي باستخدام DNP3-OPC

د.م مسعود الأتاسي. استاذ مساعد في قسم هندسة الميكاترونك. جامعة حمص.

الملخص

تعتبر برتوكولات Fieldbus بأنواعها المختلفة أساساً لإدارة الشبكات الصناعية حيث تضمن نقل بيانات الشبكة الصناعية بشكل موثوق بين عقد الشبكة المتقاربة أو المتباعدة جغرافياً. ويرتبط أداء الشبكات الصناعيّة بمجموعة من البارامترات مثل زمن تأخير الإطار، استخدامية الشبكة، إنتاجية الوصلات، معدل ارسال الأطر في الثانية وغيرها، حيث تتأثر هذه البارامترات بعدة عوامل نذكر منها عدد العقد، حجم الإطار، طوبولوجيا الشبكة، نوعية خطوط النقل، نوعية الأجهزة البينية التي تربط بين عقد الشبكة وغيرها، ويعكس الأداء العالي للشبكة الصناعيّة قدرتها على تلبية مُتطلبات الزمن الحقيقي وجودة الخدمة التي تُلبي الاحتياجات المطلوبة.

وطريقة دمج أنظمة التحكم الإشرافي SCADA (Supervisory Control And Data Acquisition) باستخدام بروتوكول اتصال المنصة المفتوحة OPC (Open Platform Communication) يسمح بتأمين إدارة مثلى للشبكة، حيث تربط الوحدات الفرعية RTUs لنظام السكادا مع الوحدة الأساسية Master عبر روابط الاتصالات الموزعة بعيدة المدى DNP3 (Distributed Network Protocol) ومن ميزاته أنه موثوق ضد البيئات الصاخبة وتداخل الإشارات. وهو بروتوكول اتصال يستخدم على نطاق واسع في محطات الطاقة الكهربائية والمياه والغاز، وخاصة في المراقبة والتحكم عن بعد في المعدات والأجهزة. ومن سيئاته انه معرض لعدد من الهجمات مثل العبث بالأجهزة أو هجوم الرجل في المنتصف، لذلك اقترحنا أول تحسين لأمن المعلومات DNP3 باستخدام خوارزمية Diffie-Hellman. تم محاكاة هذه الخوارزمية باستخدام لغة بايثون، ولاحظنا أن المستخدمين حصلوا على نفس قيمة المفتاح على الرغم من وجود متنصت

على الخط، وعلى الرغم من حصولها على قيم p، g، A، B، إلا أنها لم تستطع الحصول على المفتاح السري K، لأنها لم تعرف القيم السرية المختارة a(160، 212) وb(114، 601) من قبل المرسل والمستقبل. تم تحقيق التحسين الثاني باستخدام التشفير غير المتماثل من خلال تطبيقه على شبكة Modbus لتوقيع الشهادات الرقمية ومفاتيح التبادل باستخدام أداة OpenSSL. يوفر هذا النوع من التشفير وظائف آمنة في تبادل البيانات، مما يحل مشكلة القنوات غير الآمنة ويحمي من الاختراق.

وتم أيضاً بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus ذو الناقل التسلسلي وهو أحد أنواع برتوكولات Fieldbus الصناعية وباستخدام محاكي الشبكات OPNET، بإجراء عملية تحليلية للنتائج وبهدف تحديد القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات وعدد الأطر للوصول للإدارة المثلى لبروتوكولModbus .

وتوصلنا إلى أن زيادة استخدامية الناقل تكبر بزيادة عدد العقد في الشبكة وحجم الإطار المرسلة، ولكن بالمقابل يزداد زمن التأخير، لذلك لتحقيق متطلبات الزمن الحقيقي للقيمة الحدية 0.5 ثانية للشبكة الصناعيّة Modbus من أجل حجم البيانات المرسلة 256Byte، يجب عدم تجاوز عدد العقد لقيمة (1000 عقدة). أما أهمية البحث فتكمن أولاً في تحقيق أمن معلومات وحماية الشبكة وإزالة مخاطر الهجمات وثانياً في معرفة عدد العقد الأعظمي لأخذ مؤشر عن زيادة الاستخدامية للشبكة مما يُسبب زيادة في الأداء العام للشبكة.

الكلمات المفتاحية: SCADA، بروتوكولDNP3 ، أمن الشبكات الصناعية، خوارزمية ديفي–هيلمان، بروتوكولModbus ، استخدامية الشبكة، التشفير غير المتناظر،Openssl .

Improved communications security and optimal management of the Fieldbus protocol in SCADA systems using DNP3-OPC

Dr. Massoud ATASSI. Associate Professor at Mecatronics Engineering Department – Homs University

ABSTRACT

Fieldbus protocols of various types form the basis for industrial network management, ensuring reliable transmission of industrial network data between nearby or geographically distant network nodes. The performance of industrial networks relate with a set of parameters such as frame latency, network utilization, link throughput, frame rate per second, etc. Several factors affect these parameters, including the number of nodes, frame size, network topology, transmission line quality, and the type of interface devices that connect the network nodes. The high performance of an industrial network reflects its ability to meet real-time requirements and the quality of service that meets the required needs.

The integration of SCADA (Supervisory Control and Data Acquisition) systems using the Open Platform Communication (OPC) protocol allows for optimal network management, as SCADA sub-units (RTUs) connect to the master unit via DNP3 (Distributed Network Protocol) communication links. Its advantages include reliability in noisy environments and signal interference. It is a communication protocol widely used in power, hydraulic, and gas plants, particularly in the remote monitoring and control of equipment and devices. One of its disadvantages is that it is vulnerable to several attacks, such as hardware tampering or man-in-the-middle attacks. Therefore, we proposed the first improvement of DNP3 information security using the Diffie-Hellman algorithm. This algorithm was simulated using the Python language, and we noticed that users obtained the same key value despite the presence of an eavesdropper on the line, and although it obtained the values of p, g, A, B, it could not

obtain the secret key K, because it did not know the secret values chosen a(160, 212) and b(114, 601) by the sender and the receiver. The second improvement was achieved by using asymmetric cryptography by applying it on the Modbus network to sign digital certificates and exchange keys using the OpenSSL tool. This type of encryption provides a secure feature in data exchange, which solves the problem of insecure channels and protects against hacking.

An industrial network model is realized using the Modbus serial bus protocol. Using the OPNET network simulator, the results were analyzed to determine the optimal values of the factors that affect the overall performance of the industrial field network when the data volume and the number of frames change, thus achieving optimal management of the Modbus protocol. We found that bus utilization increases with the number of nodes in the network and the size of the transmitted frame. However, the delay time also increases. Therefore, to achieve the real-time threshold of 0.5 seconds for an industrial Modbus network with a transmitted data size of 256 bytes, the number of nodes must not exceed 1,000 nodes. The importance of the research lies, firstly, in achieving information security and protecting the network to eliminate the risk of attacks. Secondly, it defines the maximum number of nodes to provide an indication of increased network utilization, which leads to an increase in overall network performance.

Keywords: SCADA, DNP3 Security, Diffie-Hellman Algorithm, Modbus, Modbus Protocol, OPNET, Network Uutilization. Asymmetric Cryptography, Openssl.

مقدمة

يعتبر برتوكول الشبكة الموزعةDNP3 أحد حلول أنظمة الاتصال بين الأجهزة التي تستخدم برتوكولات Fieldbus بأنواعها المختلفة وهذه الطريقة أساسية لإدارة الشبكات الصناعية في نظام SCADA، لأننا نضمن نقل بيانات الشبكة الصناعية بشكل موثوق بين عقد الشبكة المختلفة المتقاربة أو المتباعدة جغرافياً وخلال البيئات الصاخبة والإشارات المتداخلة. لكن هذه

الطريقة سيئتها أنها غير محمية ومعرضة للهجمات والتنصت على المعلومات، لذلك بروتوكول الاتصال الموزع DNP3يتطلب تحسيناً في أمن نقل معلوماتها.

في البدايات صمم DNP3 خصيصاً لتطبيقات الاتصالات في نظام الـ SCADAوتم استبداله لاحقاً ببروتوكول IEC61850 المحسن لاستخدامه في أوروبا. في بحثنا استخدمنا خوارزمية Diffie-Hellman والتشفير الغير متناظر asymmetric cryptography لتحقيق أمن المعلومات وحماية الشبكة من القرصنة وإزالة مخاطر الهجمات. وقمنا أيضاً باستخدام محاكي الشبكات OPNET لإجراء عملية تحليلية لنتائج شبكة صناعيّةModbus لمعرفة عدد العقد الأعظمي اللازم لتحقيق متطلبات الزمن الحقيقي ومعرفة أفضل استخدامية للشبكة من أجل زيادة أداء العام.

يتم استخدام DNP3-OPC Server في أنظمة الأتمتة واسعة النطاق والتحكم الصناعي، بمثل تلك الموجودة في محطات الطاقة، ومرافق معالجة المياه، وعمليات النفط والغاز. ويمكن استخدامها أيضًا في التطبيقات الأخرى التي تتطلب الوصول إلى البيانات ومراقبتها. ويعد DNP3-OPC Serverمن الحلول البرمجية التي توفر الاتصال بين الأجهزة من مختلف الشركات الصناعية باستخدام بروتوكول DNP3 وخوادم OPC .حيث يقوم خادم DNP3-OPC بتحويل البيانات من بروتوكول DNP3 إلى بروتوكول OPC وبالعكس. بدون هذه الحلول، لن تتمكن الأجهزة التي تستخدم بروتوكول DNP3 من الاتصال بالأنظمة والتطبيقات التي تستخدم بروتوكولات OPC. هذه الحلول المتكاملة السلسة بين الأجهزة والأنظمة المختلفة تعزز الكفاءة والوظائف الشاملة للنظام[2] .

1. هدف البحث

- تحسين أداء المنظومة الإشرافية والإدارة المثلى وذلك من خلال بناء نموذج لشبكة صناعية Modbusالصناعية باستخدام محاكي الشبكات OPNET، ثم القيام بتحليل النتائج بهدف تحديد القيم الأفضل والقيم الحرجة التي تُخرج الشبكة الصناعيّة عن تلبيتها لمتطلبات الزمن الحقيقي الأعظمي والذي يساوي 0.5 ثانية لبروتوكول Modbus[21].

- تحسين الأمان في أنظمة SCADA والتي تعتمد على بروتوكول الاتصالات الموزعة DNP3 وذلك من أجل التحكم في الزمن الحقيقي ومراقبة نظام واسع النطاق الموزع بواسطة بناء معمارية آمنة لبروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان وذلك أثناء تراسل البيانات بين محطات Modbusومن ثم استخدام شهادات رقمية موقعة ومشفرة باستخدام المفاتيح غير المتناظرة والتحقق باستخدام الأداة OpenSSL، وهذا يحل مشكلة القناة الغير آمنة والقرصنة. ونلخص أهم النقاط الواجب حلها في هذا البحث هي:

–حماية المعلومات في بروتوكول DNP3بين المرسل والمستقبل من مخاطر الهجمات وهجوم الرجل في المنتصف وأيضاً مصادقة الشهادات الرقمية وتوقيعها وتشفيرها باستخدام المفاتيح غير المتناظرة بين الوحدات الطرفية clients والمحطات الرئيسية servers داخل شبكةModbus

– معرفة عدد العقد الأعظمي لتحقيق متطلبات الزمن الحقيقي للشبكة الصناعيّة Modbus ذو الناقل التسلسلي مما ينعكس إيجابياً على الأداء العام للشبكة.

2. مواد وطرق البحث

1.2 أدوات البحث

تمّ استخدام أداة محاكاة الشبكات OPNET، ولغة البرمجة Python والأداة OpenSSL من أجل إنجاز هذا البحث:

1) محاكي الشبكات OPNET: هي أداة محاكاة للشبكات واختصار لـ Optimized Network Engineering Tools، أي أداة هندسية الشبكات المحسنة .ساعدت هذه الأداة في بناء نماذج شبكات صناعيّة واقعية وأخرى افتراضية من أجل تحديد العوامل المؤثرة في الأداء بهدف تحسينه. [3]
2) لغة Pythonلبرمجة خوارزمية Diffie Hellman (DH) كطريقة لشرح تبادل مفاتيح التشفير بشكل آمن عبر قناة الاتصالات لبروتوكول DNP3 والمخصص لتطبيقات أنظمة SCADA.[4, 5, 6]

3) OpenSSL هو تطبيق مفتوح المصدر يحتوي على أدوات التشفير ويستعمل بروتوكولات طبقة النقل الامن .مكتبته الأساسية مكتوبة بلغة البرمجة C لإجراء اختبارات بين خادمClient وعميل SSL/TLS-Server، إصداراته متاحة لمعظم أنظمة التشغيل، وفعال لتوقيع وتشفير الرسائل[27] .

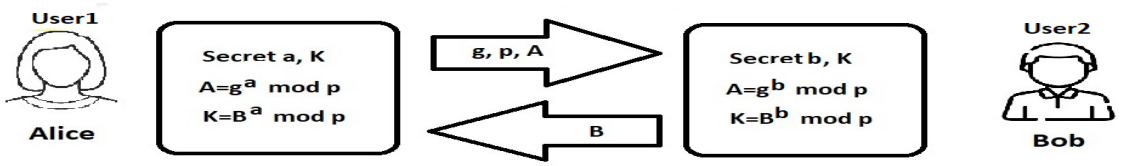
2.2محاكي الشبكات OPNet:

هو أحد أشهر المحاكيات الشبكية وأكثرها شعبية بسبب استخدامه الكبير والواسع في مجالي الصناعة والأبحاث الشبكية، وهو نظام هندسي قادر على محاكاة شبكات الاتصال الضخمة مع نمذجة تفصيلية للبرتوكولات، والتطبيقات، والأجهزة وتحليل الأداء. ميزته أنه يمتلك واجهات رسومية قوية جداً للنموذج، ومحاكاة ديناميكية، ونواة محاكاة معتمّدة على جدولة للأحداث، وأدوات تحليل متكاملة مضمنة داخله، وهرمية للبيانات، ببساطة هو أداة محاكاة للشبكات تتيح تعريف طوبولوجيا الشبكة، العقد، التوصيلات، التطبيقات وغيرها. كما يمكن للمستخدم أن يُعرّف العمليات التي يمكن أن تحدث في عقدة جزئية وخصائص توصيلات الإرسال، وبعد ذلك تنفذ المحاكاة وتحلل النتائج لأي عنصر في شبكة المحاكاة. كما أنّ OPNET هو بيئة محاكاة غرضيّة التوجّه يحقّق كل المتطلبات ويعدّ محاكي الشبكة الأكثر فعالية للأغراض العامة، ويشمل أيضاً على أدوات التحليل المخصصة لتفسير وتركيب الخرج ويعتمّد محاكاة الأحداث المتقطعة. علاوةً على ذلك فإنّه يتضمن دعم للغة الـ C مزوداً بالقدرة على تحقيق أي مهمة أو برتوكول اتصال ولمجال واسع من أنظمة الاتصال بدءاً من شبكات LAN البسيطة حتى شبكات الأقمار الصناعيّة مدعومة من قبل OPNET [7, 8].

3.2 خوارزمية تبادل المفاتيح ديفي-هيلمان(D-H) Diffie-Hellman key exchange

بروتوكول ديفي–هيلمان هو بروتوكول لتبادل المفاتيح في علوم الكمبيوتر يسمح لطرفين بمشاركة مفتاح سري بشكل آمن عبر قناة غير آمنة دون الكشف عن المفتاح نفسه. يتضمن استخدام خوارزمية تبادل المفاتيح ديفي–هيلمان D–H الأعداد الصحيحة الأولية والعشوائية الكبيرة والحسابات المعيارية لإنشاء مفتاح سري مشترك بين الطرفين.

مثال خطوات خوارزمية ديفي-هيلمان[9]: هناك شخصان معروفان (user1)Alice و (user2)Bobوعدد أولي **p** وجذر بدائي**g**. نفرض أنBob و Alice يريدان تبادل مفتاح حسب الشكل (2.1):



الشكل (2.1):Diffie-Hellman key exchange Protocol

- يختار أليس وبوب معًا، على سبيل المثال،**g=7 p=11** .
- تختار أليس(**A**) **a= 3** لحساب g^a:

$$A= g^3 \text{mode } p$$

$$A = 7^3 \text{ mod } 11$$

$$A=343 \text{ mod } 11$$

$$A=2$$

- يختار بوب(**B**) **b= 5** لحساب g^b:

$$B=g^5 \text{ mode } p$$

$$B = g^y= 7^5= 16807 \equiv 15 \text{ mod } 11$$

$$B=10$$

- تبادل القيم **A=2** و **B=10** لحساب قيمة المفتاح السري **K**

$$K=B^a \text{ mod } p=10^3 \text{ mod } 11=10 \quad : \text{Alice}$$

$$K=A^b \text{ mod } p=2^5 \text{ mod } 11=10 \quad : \text{Bob}$$

نلاحظ أن المستخدمين حصلوا علة نفس قيمة المفتاح رغم وجود المتصنت على الخط ورغم أنه حصل على قيم **p, g, A, B** لكنه لن يستطع الحصول على المفتاح **K** الصحيح لأنه لا يعرف قيم المختارة a, bمن قبل اليس وبوب ولو حسابياً. لذلك طريقة ديفي-هيلمان D-Hتحترم السرية التامة المستقبلية (PFS: Perfect Forward Secrecy)، وهي إحدى

ميزات بروتوكولات اتفاقية المفاتيح المحددة التي تقدم ضمانات بأن مفاتيح الجلسة لن يتم المساس بها حتى في حالة المساس بالأسرار طويلة الأمد المستخدمة في تبادل مفاتيح الجلسة، مما يحد من الضرر. ولأن طريقة D-H تقوم بتوليد القيم السرية a ,b بكل جلسة جديدة وهذا ما يسمى DHE والذي يشير إلى " ديفي-هيلمان المؤقتEphemeral " وهذا يعني أن المفتاح المستخدم في تبادل المفاتيح يتم استخدامه مرة واحدة فقط ثم يتم حذفه.

4.2 دراسة مرجعية

– الدراسة المرجعيّة [11] تمّ فيها تحليل أداء برتوكول الاتصال Modbus/TCP الصناعي وركّز البحث على تقييم الأداء من خلال زمن الاستجابة T مُرتبطاً بعدد العقد والطوبولوجيا، وأظهرت النتائج أنّ الطوبولوجيا النجميّة ذات زمن استجابة ثابت تقريباً مع زيادة عدد العقد وبتالي مُناسبة لنظم الزمن الحقيقي. هذا البحث لم يحدد عدد العقد الأعظمي بحيث زمن التأخير لا يتجاوز الزمن الحقيقي 0.5 ثانية في بروتوكول Modbus ذو النقل التسلسلي[21] من أجل حجم البيانات المرسلة 256Byte، وهذا ما تم دراسته وتحليله في بحثنا.

– الدراسة المرجعيّة [12] قدمت تحليل لأداء شبكات ايثرنت الصناعيّة باستخدام برنامج المحاكاة OPNET، ففي البداية تمّ التأكد من قابلية برنامج OPNET في نمذجة الشبكات الصناعيّة من خلال مقارنة نتائج تجارب شبكة عملية مع نتائج المحاكاة ومن ثمّ تمّ دراسة تأثير عدد من العوامل على الأداء مثل طول الحزمة وعدد العقد ومعدل إنتاجية العقد ، وقدمت هذه الدراسة فائدة كبيرة حيث أثبتت قابلية برنامج OPNET في محاكاة الشبكات الصناعيّة من خلال مقارنة نتائج المحاكاة مع قيم تجريبية إلا أنّها عانت أيضاً من العموميّة فلم تعرض آلية نمذجة العقد المُستخدمة في الشبكة المدروسة و خصائص كل منها وحجم البيانات وعدد الأطر وهذا تم في بحثنا من خلال بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus وباستخدام محاكي الشبكات OPNET بهدف تحسينها ومعرفة خصائصها وزيادة استخدامية الناقل بشكل كبير بزيادة عدد العقد في الشبكة لعدد محدد تم معرفته بفضل الاختبارات.

– هدفت الدراسة [13] إلى التحقق من القيود والعيوب التي تعيب بروتوكول الاتصالات DNP3المستخدم بشكل شائع في SCADA، والتحقيق في الهجمات الإلكترونية التي تستغل نقاط الضعف في هذا البروتوكول، وتقديم توصية لحماية شبكات SCADA ومنع العواقب المدمرة.

– أما الدراسة المرجعية [14] قدمت اختبار لمعالجة تحليل الثغرات الأمنية واختبار الاختراق الذي يشمل على هجوم رجل في المنتصف وتحليل مختلف التهديدات ونقاط الضعف في بروتوكول DNP3 الذي يعمل في تطبيق SCADA. النتائج التي حصل عليها الباحث تبين أنه يمكن اكتشاف هذه الهجمات بنجاح باستخدام بنية تستند إلى خوارزمية (DCA: Dendritic Cell Algorithm) المعتمدة على نظام المناعة الاصطناعي (AIS: Artificial Immune System)، وأن اهم نقاط الضعف في DNP3 هي: هجوم رجل في الوسط، تعديل حزمة DNP3 وتعطيل الرسائل.

–في الدراسة المرجعيّة [22] قام الباحث بإجراء اختبار الاختراق باستخدام سيناريوهات الهجوم المختلفة في بيئة افتراضية من خلال محاكاة تتضمن بروتوكول DNP3. تم معالجة تحليل الثغرات الأمنية واختبار الاختراق الذي يشمل على هجوم رجل في المنتصف (MITM). تضمنت تقنيات الفحص الذي استخدمها الباحث إجراء فحص صحي للشبكة، ثم إجراء تقييم نقاط الضعف في DNP3 والهجمات الأمنية والاكتشافات والوقاية والتدابير المضادة. قام الباحث بتحليل مختلف التهديدات ونقاط الضعف في بروتوكول DNP3 الذي يعمل في تطبيق SCADA كجزء من الشبكة الذكية باستخدام النماذج الأولية والبيئات الافتراضية، كما تم إجراء اختبار كفاية الأمان باستخدام أربعة سيناريوهات للهجوم الأساسي بما في ذلك نوع هجمات رفض الخدمة (MITM). لاحظ الباحث أن استخدام النماذج النظرية لهجمات الشبكة الذكية باستخدام نظرية اللعبة أدت إلى تحسين استراتيجيات الكشف وذلك من خلال الحد من التهديدات الالكترونية في بيئة DNP3.

–أما الدراسة المرجعية [23] ناقش الباحث الهجمات التي تستهدف الشبكات الذكية التي تستخدم بروتوكول DNP3، وكيف يمكن اكتشاف هذه الهجمات باستخدام الإصدارات الحتمية لخوارزمية الخلايا الجذعية (DCA) والتي تعد خوارزمية قائمة على نظام المناعة الصناعي (AIS) لتقييم فعالية DCA. عمد الباحث إلى إنشاء مجموعة بيانات اختبار من خلال تنفيذ هجمات متنوعة ثم تنفيذها في بيئة الشبكة الذكية DNP3.

في الدراسة المرجعيّة [28]تقدم نهجًا توضيحيًا لدمج تقنية توزيع المفاتيح الكمومية (QKD) في مكتبة .Openssl ومعرّفًا التشفير غير المتماثل كأحد تقنيات التشفير الرئيسية المستخدمة في الاتصالات والأنظمة. على الرغم من فوائد هذه الطريقة وفعاليتها، إلا أن لها بعض المشكلات

المعقدة المتعلقة بتوزيع المفاتيح الكمومية، لذلك في التشفير الغير متناظر لا يتم نقل المفتاح السري عبر الشبكة وحتى إذا سُرق المفتاح الخاص، لا يمكن فك تشفير الجلسات السابقة وهو سهل التطبيق وحماية مناسبة

بعض الأبحاث السابقة أكدت أنه من الأفضل دمج عدة استراتيجيات للأمان بدلاً من استخدام استراتيجية واحدة أو استخدام طرق مثل DCA، MITM وAIS مما يعطي أمان أكثر للنظام ولكن على حساب تعقيد الخوارزميات. أما خوارزمية ديفي هيلمان فهي طريقة معيارية أثبتت فعاليتها في العديد من بروتوكولات الانترنت. مثل (Internet Protocol Security)، (Secure Shell) و Transport Layer Security (TLS). ويعتبره البعض الحل الأكثر كفاءة وسهل التنفيذ. لكن لا يزال البعض الآخر يفضل خوارزميات أخرى نظراً لكونها أوسع استخداما منه، مثل RSA التي تستخدم إلى جانب تبادل المفاتيح البصمات الإلكترونية.

في هذا البحث عملنا على تحسين أمن الاتصالات لبروتوكول DNP3 باستخدام خوارزمية سهلة وفعالة وهي ديفي هيلمان لمنع هجوم رجل في الوسط، وتم تحسين أمن شبكةModbus بمصادقة الشهادات الرقمية وتوقيعها وتشفيرها باستخدام المفاتيح غير المتناظرة بين Clients وServers. وتم تحديد أيضا القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات Byte256 بالإطار ومن أجل 1000 عقدة محققاً متطلبات الزمن الحقيقي (0.5) ثانية، من خلال بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus وباستخدام محاكي الشبكات OPNET بهدف تحسينها ومعرفة خصائصها.

3. الناقل الحقلي(Fieldbus):

هو عبارة عن ناقل اتصال رقمي ثنائي الاتجاه بين الأجهزة الحقليّة الذكية، وتُعد بمثابة شبكة محلية مُخصّصة للأتمتة الصناعيّة، حيث تُستبدل شبكات التحكّم المركزية بشبكات التحكّم الموزّعة والتي تربط الأجهزة الحقليّة. هناك العديد من أنواع البرتوكولات الحقليّة المُستخدمة اليوم، ويعتمّد النوع الذي سيتمّ استخدامه على نوع المصنع، ونذكر منها (Foundation Fieldbus وPROFIBUS وDeviceNet وControlNet وInterbus وHART وAS-i وMODBUS وCAN Bus وEthernet وLon Works وWorldSIM). إنّ تطبيق برتوكول الناقل الحقلي في أتمّتة العمليات الصناعيّة له ميزات عديدة، فهو يؤدي لتحكم أفضل في

العملية إلى جانب زيادة إنتاجية المنتج[10]. وأهم الخصائص التي تميّز شبكات (Foundation Fieldbus) الصناعيّة هي:

- برتوكول أتمتة وتحكم بالعمليات الرقمية ثنائي الاتجاه.
- تمتلك المنظومة ثلاث طبقات: (طبقة فيزيائية – طبقة اتصال بيانات – طبقة التطبيقات) كما تمتلك طبقة إضافية ثامنة تدعى طبقة المستخدم (USER LAYER).
- لديها بنية ثنائية المستوى مكوّنة من مستوى منخفض (H1) ومستوى أعلى (H2)، ويعمل المستوى (H1) بسرعة ([Kbps] 31.25) بينما (H2) يعمل بسرعة (12.5 [Mbps]).
- يدعم الاتصالات المجدولة وغير المجدولة.
- تدعم التوافقية ويمكن للأجهزة المختلفة الموجودة من قبل مصنعين مختلفين أن تتصل بسلاسة مع بعضها.

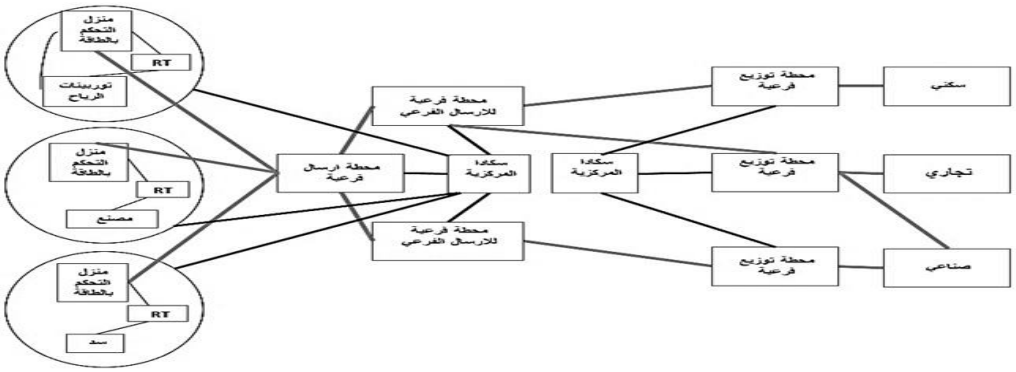
تعتمد شبكات Foundation Fieldbus على نموذج OSI (Open Systems Interconnection) المرجعي، ويتكون نموذج Fieldbus من ثلاث طبقات:(PHL ، DLL، APL)، فبالنسبة للطبقة السابعة APL (Application Layer) تُقسم إلى طبقتين فرعيتين هما: طبقة مواصفات رسائل FMS (Fieldbus Message Specification) وطبقة الوصول الفرعي FAS (Fieldbus Access Sub-layer)، وهناك طبقة فوق الطبقة السابعة تسمى طبقة تطبيق المستخدم، وهذه هي الطبقة الثامنة من نموذج Foundation Fieldbus، ولا يتمّ استخدام الطبقات من 3 إلى 6 الموجودة في OSI. تستقبل الطبقة الفيزيائية PDU (Physical Data Unit) البيانات من طبقة اتصال البيانات حيث يتمّ تحويلها إلى إشارة فيزيائية ونقلها على ناقل Fieldbusبوسيلة كهربائية أو ضوئية. [15]

4. لمحة عن بروتوكول DNP3 المستخدم في البحث:

DNP3 أو بروتوكول الشبكة الموزعة النسخة الثالثة هو معيار اتصال يعرف الاتصالات بين المحطة الرئيسة ووحدات القياس البعيدة RTUs وغيرها من الأجهزة الالكترونية الذكية IEDs. تم تطويره لتحقيق التوافقية بين الأنظمة في المجالات الصناعية، فجاء مخصصاً

لتطبيقات أنظمةSCADA، هذا يتضمن تحصيل المعلومات وإرسال تعليمات التحكم بين حاسوبين منفصلين فيزيائياً، وصمم لإرسال رزم صغيرة نسبياً من البيانات ولكن بطريقة موثوقة من خلال رسائل تصل بتسلسل قطعي، وهذا الاختلاف الأساسي عن بروتوكولات الأغراض العامة كـ FTP، والذي هو جزء من بروتوكول TCP/IP الذي يستطيع إرسال ملفات كبيرة الحجم ولكن بطريقة ليست متوافقة مع نظم سكادا. أهم مميزات بروتوكول DNP3 هي المعايير المفتوحة التي تمكن من عمل توافق بين تجهيزات من مصنعين مختلفين، هذا يعني أن المستخدم يستطيع شراء محطة رئيسة من مصنع ما ويستطيع جلب وحدات RTUs من مصنع أخر، وبدورها تمتلك هذه الوحدات مرحلات تحكم متصلة بها هي أجهزة إلكترونية ذكية تستعمل برتوكول DNP3، وكل هذه التجهيزات يمكن أن تأتي من شركات ومصنعين مختلفين من بداية التصميم أو حتى عند القيام بالتحديثات.[16]

تكون أفضل تطبيقات أنظمة سكادا في العمليات الموزعة على مساحات ومناطق جغرافية واسعة، وتكون سهلة المراقبة والتحكم وتتطلب تدخلاً متكرراً أو منتظماً أو عادياً. سوف يتم تطبيق أنظمة السكادا في بحثنا على أنظمة نقل القدرة الكهربائية التي تغطي عادة آلاف الكيلومترات المربعة، ويتم التحكم بها عن طريق فتح قواطع وإغلاقها، ويجب أن تكون سريعة الاستجابة لتغيرات الأحمال على الخطوط الكهربائية .



الشكل (4.1): نظام قدرة[17].

5. النتائج ومناقشتها

❖ **إجراء اختبار لتحديد القيمة العظمى للبيانات المُرسلةMTU**

نستطيع القول أنّ OPNET محاكٍ قوي وشائع الاستخدام في المصانع والأبحاث وذلك بسبب خصائصه والمجموعة الكبيرة من الخيارات المضمنة داخله والتي تساعد في نمذجة ومحاكاة الشبكات الكبيرة. الشكل (5.1) يبين خطوات انشاء أي مشروع باستخدام المحاكي OPNET.

الشكل(5.1): خطوات انشاء شبكة باستخدام المحاكي OPNET

- لدينا العلاقة الرياضية التي تعطي زمن الارسال اللازم $\mathbf{T_{transmission}}$.[18]

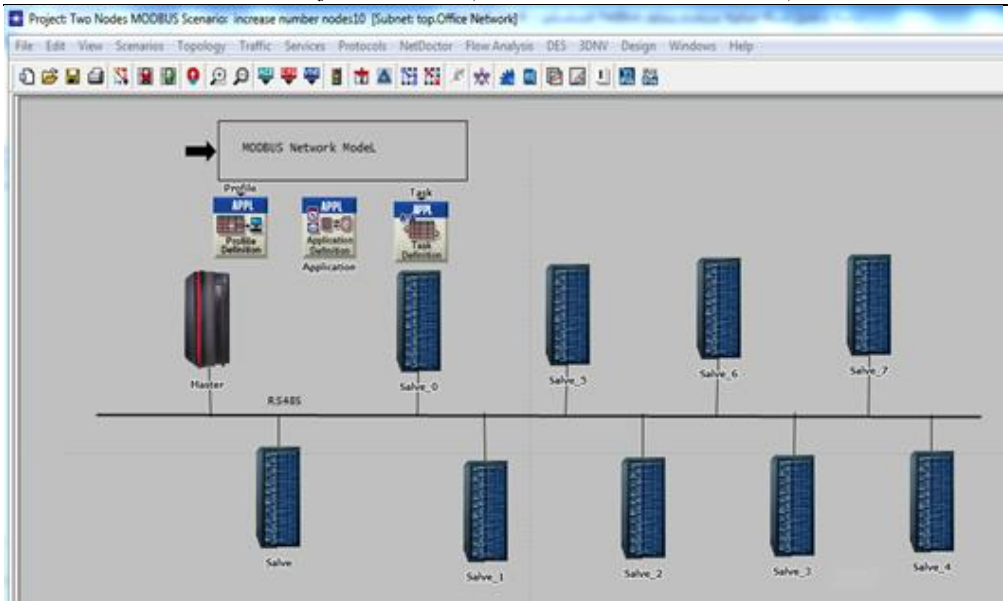
$$\mathbf{T_{transmission}} = \frac{\mathbf{D\ (H+MTU)}}{\mathbf{MTU*R}}$$

حيث أنّ:

- MTU (Maximum Transmission Unit) حجم الأقصى لوحدة البيانات.
- (D): حجم البيانات الكلي (Data).
- (H): حجم الإطار للبرتوكول المستخدم.
- (R): معدّل الارسال.

لا بد من إجراء اختبار لتحديد القيمة العظمى للبيانات المُرسلةMTU لتحقّيق أفضل أداء للشبكة بالاعتمّاد على البارامترات المضبوطة في الشبكة الصناعيّة الأساسية، تمّ رصد تأثير العاملين (عدد العقد وحجم الإطارH وحجم البيانات المُرسلة MTU) على الأداء العام للشبكة الصناعيّة والتي تستخدم أحد أنواع برتوكولات Fieldbus الصناعيّة وهو برتوكول MODBUS ذو الناقل التسلسلي.[19]

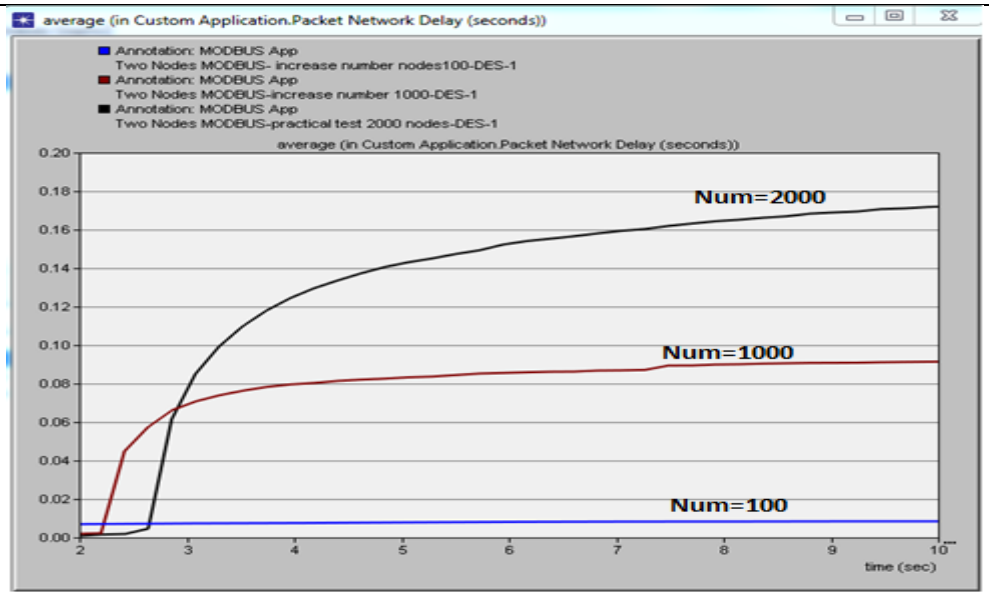
يُظهر الشكل(7.2) نموذج لشبكة صناعيّة Modbusمؤلفة من 10 عقد (9 Master /Slaves،



الشكل(5.2): شبكة صناعيّة مؤلفة من ماستر و9 توابع.

دراسة وتحليل النتائج:

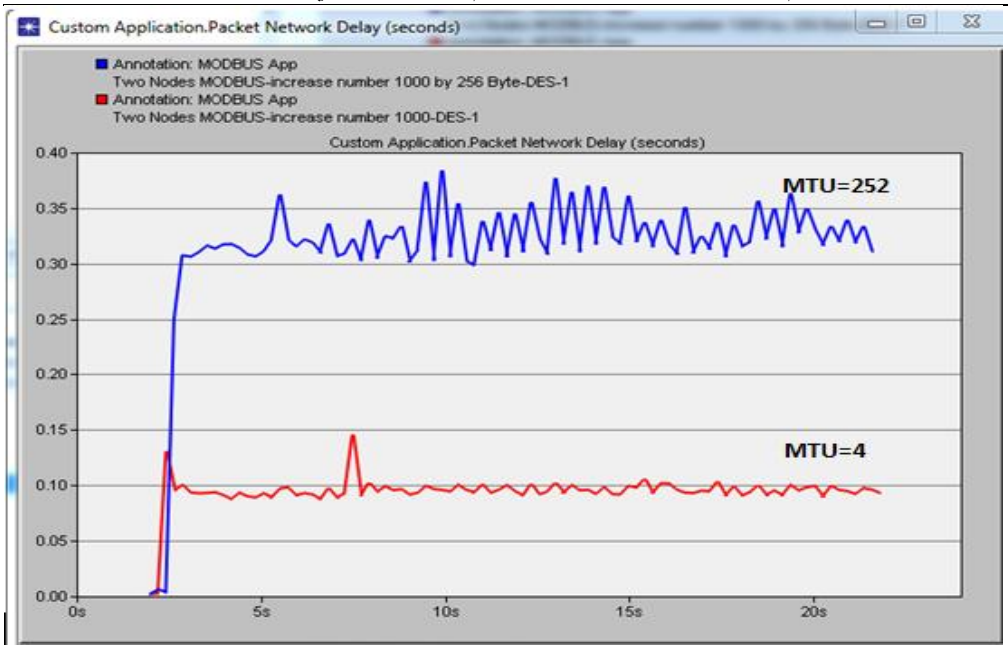
في الحالة الأولى: تمّ زيادة عدد العقد التابعة في الشبكة الصناعيّة بشكل تصاعدي وفق التسلسل الآتي (100–1000–2000) مع تثبيت حجم الإطار على قيمة 8Byte وتمّ رصد تغيّر زمن تأخير إطار الشبكة حيث تمّ تشغيل المحاكاة لمدة 10 ثانية.



الشكل(5.3): تغيّر زمن تأخير الإطار للشبكة الصناعيّة عند زيادة كبيرة لعدد العقد.

يُوضح الشكل(5.3) أن زمن التأخير سجل ارتفاع بشكل كبير من القيمة 0.1s عند عدد العقد (1000) وصولاً للقيمة 0.2s عند العدد (2000).

في الحالة الثانية: تمّ تغيير حجم البيانات المرسلة من القيمة 8Byte إلى القيمة 256Byte لشبكة صناعيّة مؤلفة من (1000) عقدة وتمّ رصد تأثير هذا التغيّر على زمن تأخير الإطار حيث تمّ تشغيل المحاكاة لمدة 20 ثانية.



الشكل(5.4): أثر العامل MTU على زمن تأخير الإطار لشبكة مؤلفة من 1000 عقدة.

نلاحظ من الشكل(5.4) تسجيل قيمة تأخير 0.4s عند الحجم 256Byte على الرغم من تلبية الشبكة لمتطلبات الزمن الحقيقي إلا أنه يجب عدم تجاوز عدد العقد الشبكة ذات الناقل التسلسلي لقيمة (1000) عقدة نتيجة الاقتراب الكبير من القيم الحدية 0.5s التي تخل بمتطلبات الزمن الحقيقي.

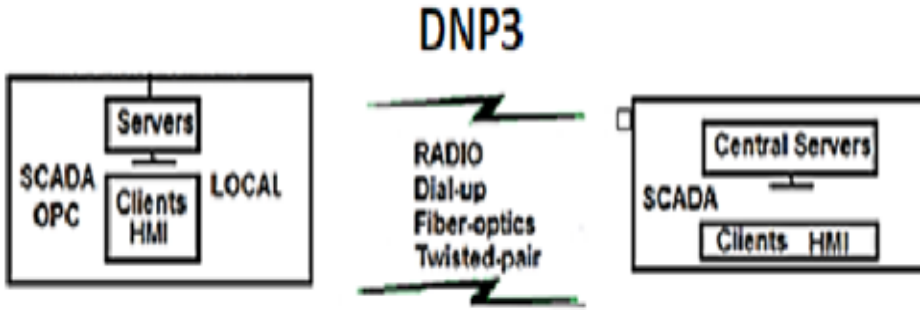
نتائج شبكة صناعيّة تستخدم برتوكول MODBUS ذو الناقل التسلسلي:

1) زيادة استخدامية الناقل بشكل كبير بزيادة عدد العقد في الشبكة.
2) زيادة تأخير الشبكة بزيادة عدد العقد وزيادة حجم الإطار المرسل.
3) يجب عدم تجاوز عدد العقد لقيمة (1000) والإطار عند الحجم الأعظمي256Byte حرصاً على تحقيق متطلبات الزمن الحقيقي والقيمة المعيارية (0.5) ثانية. حيث0.5 ثانية هي القيمة الحدية لزمن استجابة الإطار في بروتوكول Modbus ذو النقل التسلسلي.Page5 [21]

❖ **إجراء اختبار وتحسين امن بروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان**

يتم ربط بروتوكول الاتصالات DNP3 ببرمجة خوارزمية تبادل مفتاح ديفي–هيلمان ضمن حاسوب HMI/Client عند المرسل والمستقبل. تتم عملية تطبيق المصادقة بين الطرفية client والمحطة الرئيسية severو فق الخطوات التالية:

1–تبادل المفاتيح وفق خوارزمية ديفي هيلمان.2–بعدها يصبح لدى الطرفين نفس المفتاح السري ندعوه مفتاح الجلسة. 3–تقوم الطرفية بإنشاء شهادة رقمية وتشفيرها بالمفتاح العام وارسالها للمحطة الرئيسية لفك تشفير الشهادة بالمفتاح الخاص والتأكد منها.4–بعد نجاح التأكد يحصل اتصال بين الطرفين.

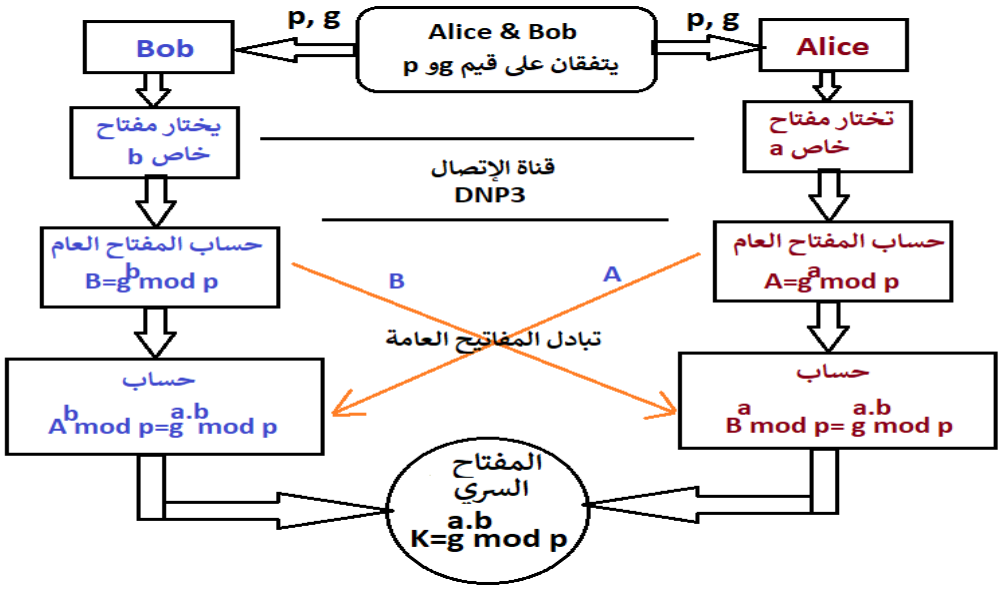


الشكل(5.5): بروتوكول الشبكة الموزعة DNP3 للاتصالات بين المحطة الرئيسة والطرفية

تُعتبر خوارزمية D–H الأول من نوعها في موضوع تبديل المفاتيح، حيث تسمح لشخصين بتبادل بيانات حساسة دون أن يفهمها الطرف الثالث (المتصنت) حتى ولو حصل على نسخة منها. تعتمد الخوارزمية في عملها على إنشاء مفتاح سري مشترك يمكن استخدامه فيما بعد لتشفير المحادثات باستخدام خوارزمية تشفير مفتاح متماثل Symmetric–key.وهو بروتوكول موثوق به للغاية ضد التداخلات الكهرومغناطيسية EMI، لكنه غير آمنًا من هجمات المتسللين.

في وقتنا الحالي، تبادل مفتاح ديفي–هيلمان هو الخوارزمية المعيارية في العديد من بروتوكولات الانترنت للأمان والحماية. مع تطور الشبكات الصناعية عبر روابط الاتصالات الموزعة DNP3، الشكل(5.5) ، جعل مسالة الأمان والحماية من الاختراقات ضرورة قصوى.

إن بروتوكول DNP3 معرض لعدد من الهجمات مثل العبث بالأجهزة أو هجوم الرجل في المنتصف، اقترحنا في بحثنا التحسين الأول في زيادة امن بروتوكول DNP3 باستخدام خوارزمية الشكل الآتي (5.6).



الشكل(5.6): خوارزمية ديفي هيلمان D–H [20]

وتمت المحاكاة لخوارزمية ديفي هيلمان بواسطة لغة Python وفق الآتي:

```
# Generate prime number and generator
    import random
    def generate_prime_number():
    """
    Generate a random prime number between 100 and 1000.
    """
    prime = random.randint(100, 1000)
    while not is_prime(prime):
    prime = random.randint(100, 1000)
    return prime
    def is_prime(n):
    """
    Check if a number is prime.
    """
    if n <= 1:
    return False
    for i in range(2, int(n**0.5) + 1):
    if n % i == 0:
    return False
    return True
    def calculate_public_key(prime, generator, private_key):
    """
    Calculate the public key using the Diffie-Hellman algorithm.
    """
    return (generator ** private_key) % prime

    def calculate_shared_secret(prime, public_key, private_key):
    """
     Calculate the shared secret using the Diffie-Hellman
     algorithm.
    """
    return (public_key ** private_key) % prime



prime = generate_prime_number()
generator = random.randint(2, prime - 1)
```

```
# Generate private keys for Alice and Bob
alice_private_key = random.randint(2, prime - 1)
bob_private_key = random.randint(2, prime - 1)

# Calculate public keys for Alice and Bob
alice_public_key = calculate_public_key(prime, generator, alice_private_key)
bob_public_key = calculate_public_key(prime, generator, bob_private_key)
# Calculate shared secrets for Alice and Bob
alice_shared_secret = calculate_shared_secret(prime, bob_public_key, alice_private_key)
bob_shared_secret = calculate_shared_secret(prime, alice_public_key, bob_private_key)


# Print the results
print("Prime number:", prime)
print("Generator:", generator)
print("Alice's private key:", alice_private_key)
print("Bob's private key:", bob_private_key)
print("Alice's public key:", alice_public_key)
print("Bob's public key:", bob_public_key)
print("Alice's shared secret:", alice_shared_secret)
print("Bob's shared secret:", bob_shared_secret)
```

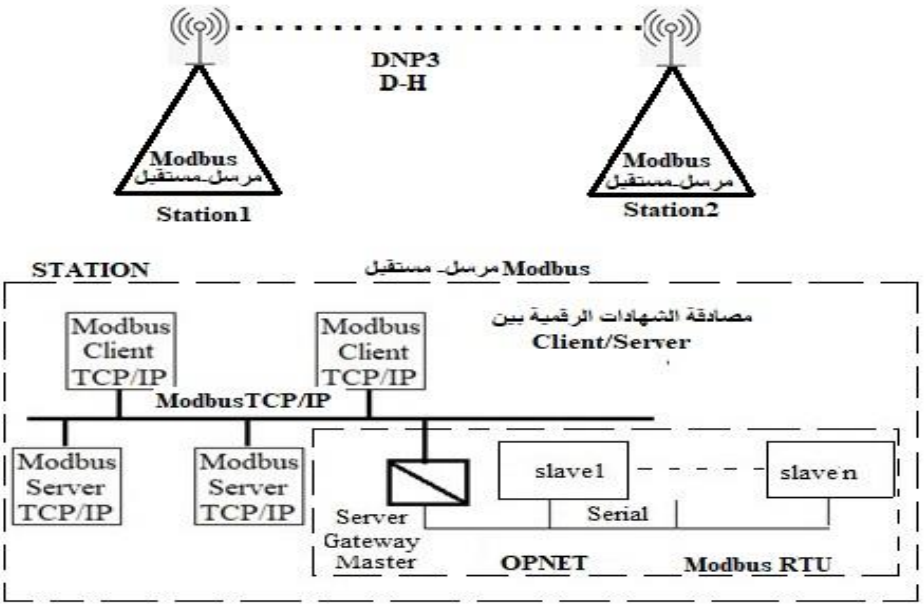
Prime number: 193
Generator: 137
Alice's private key: 160
Bob's private key: 114
Alice's public key: 108
Bob's public key: 27
Alice's shared secret: 1
Bob's shared secret: 1

Prime number: 877
Generator: 545
Alice's private key: 212
Bob's private key: 601
Alice's public key: 553
Bob's public key: 694
Alice's shared secret: 647
Bob's shared secret: 647

نلاحظ من النتائج أن المستخدمين (Master-Clients) حصلوا على نفس قيمة المفتاح **(1, K 647,….)** عند وجود هجمات مثل العبث بالأجهزة أو رجل دخل على الخط، رغم أنه حصل

على القيم **p(139, 877,…), g(137, 575,...), A(108, 553,...), B(27, 694,...)** لكنه لم يستطيع الحصول على المفتاح **K** الصحيح لأنه لا يعرف قيم المختارة السرية **a(160, 212, ….), b(114, 601,…)** من قبل Master(Bob)/Slave(Alice).

❖ **إجراء اختبار والتحسين الثاني في أمن شبكة Modbusعن طريق المصادقة Client/Serverبتوقيع وتشفير شهادات رقمية باستخدام الأداة مفتوحة المصدر OpenSSL**

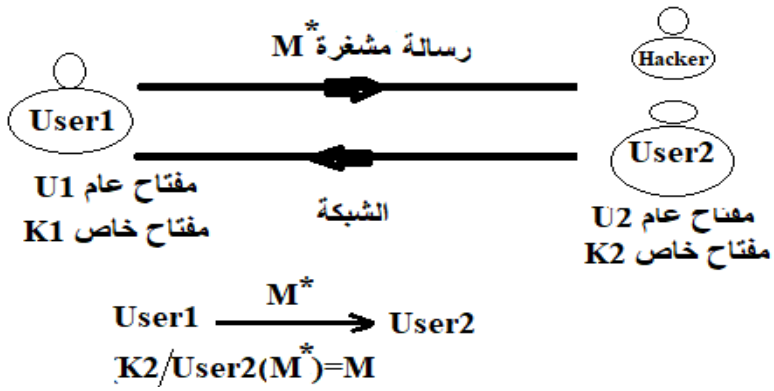


الشكل(5.7): محطة MODBUS

تم الاعتماد على خوارزمية ديفي هيلمان الامنة في نقل البيانات وتبادل المفاتيح بين محطتين عن بعد بواسطة الأنترنت، وسنقوم بتحسين النظام باستخدام OpenSSL للمصادقة باستخدام شهادات رقمية موقعة ومشفرة بشكل امن باستخدام المفاتيح غير المتناظرة وهذا يحل مشكلة القناة الغير آمنة والقرصنة. حيث تقوم الطرفية Clientبإنشاء شهادة رقمية (عبارة عن معرف IDوعنوان الجهاز Addr في الشبكة) وتشفيرها بالمفتاح العام الذي وصلها من خوارزمية D–H وترسل الشهادة للمحطة الرئيسية(Sever/Gateway(Master ، عندئذ تقوم المحطة

الرئيسية بفك تشفير الشهادة بالمفتاح الخاص والتأكد منها وحفظها على انها تابعة للطرفية Client. بعد نجاح المصادقة يحصل اتصال بين المحطة الرئيسية والطرفية.

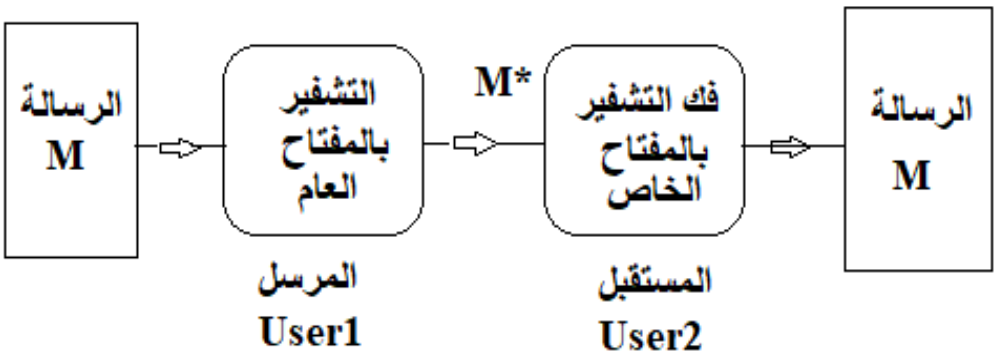
نوع التشفير المستخدم هو التشفير الغير المتماثلAsymmetric encryption ، حيث أن الرسالة المشفرة الرسالة المشفرة بمفتاح عام U لا يمكن قراءتها إلا بواسطة مالك المفتاح الخاصK المقابل .لذا، باستخدام المفتاح الخاص K1 من قبل User1يستطيع أن يوقع معلوماته ويفك رموزها ليعالجها. فمثلاً إذا User1 يرغب في إرسال رسالة M إلى User2، فسوف يستخدم المفتاح العام لـ User2 من أجل تحقيق رسالة مشفرة *M. يستخدم User2 المفتاح الخاص حتى يتمكن من فك الرسالة المشفرة *M ويحصل على الرسالة M. يمكن استئناف العملية وفقًا للشكل الآتي(5.8):



الشكل(5.8): التشفير بالمفتاح العام وفك التشفير بالخاص

إذا اعترض Hacker الرسالة *M، فلن يتمكن من تحديد M من *M بدون المفتاح الخاص K2 لـ User2. لذلك من المستحيل تقريبًا العثور على مفتاح خاص K لعميل User ما من مفتاحه العام U. لكن المشكلة أنه يمكن لخادم "القراصنة" Hacker إ عادة توجيه الموقع للعميل أو الخادم إلى موقع مزيف واسترداد البيانات. والحل هو استخدام الشهادات الرقمية، وهي باختصار وثائق إلكترونية أو شهادات رقمية تستخدم للتحقق من هوية كيان رقمي أو حتى شخصًا يرغب في إنشاء اتصالات آمنة. تُعد الشهادات الرقمية أساسية في التجارة الإلكترونية الحديثة، والشبكات الصناعية، والخدمات المصرفية. إن توقيع وتشفير الشهادات الرقمية يحل مشكلة القناة

الغير آمنة والقرصنة وتتيح هذه الشهادة للموقع إثبات الهوية للعملاء أو للطرفيات Clients كما هو موضح في الشكل الآتي:



الشكل (5.8): توقيع وتشفير الشهادات الإلكترونية

الخطوات الرئيسية في التشفير غير المتناظر باستخدام الأداة OpenSSL

التشفير غير المتناظر (Asymmetric Cryptography) هو نوع من التشفير يستخدم زوجًا من المفاتيح: مفتاح عام (Public Key) ومفتاح خاص (Private Key). يُستخدم المفتاح العام للتشفير، بينما يُستخدم المفتاح الخاص لفك التشفير. هذا النوع من التشفير يوفر ميزة الأمان في تبادل البيانات دون الحاجة إلى مشاركة المفتاح الخاص، مما يجعله مناسبًا للتطبيقات مثل التوقيعات الرقمية وتبادل المفاتيح.

1) يتم أولاً تعزيز أمان شبكة Modbus بإنشاء معلمات نظام (DH) Diffie–Hellman التي تم استقبالها في المحطة

openssl dhparam –out dhparams.pem 2048

```
# إنشاء معلمات DH (عدد أولي كبير وأساس مناسب)
openssl dhparam -out dhparams.pem 2048
```

2) توليد المفاتيح لكل عقدة

- للعميل:

openssl genpkey –paramfile dhparams.pem –out client_dhkey.pem

```
# للعميل:
openssl genpkey -paramfile dhparams.pem -out client_dhkey.pem
```

- للخادم:

openssl genpkey –paramfile dhparams.pem –out server_dhkey.pem

```
# للخادم:
openssl genpkey -paramfile dhparams.pem -out server_dhkey.pem
```

3) عملية تبادل المفاتيح

- العميل يرسل معاملاته العامة للخادم:

openssl pkey –in client_dhkey.pem –pubout –out client_pubkey.pem

- الخادم يرسل معاملاته العامة للعميل:

openssl pkey –in server_dhkey.pem –pubout –out server_pubkey.pem

```
openssl pkey -in server_dhkey.pem -pubout -out server_pubkey.pem
```

```
openssl pkey -in client_dhkey.pem -pubout -out client_pubkey.pem
```

4) توليد المفتاح المشترك:

- على جانب العميل:

openssl pkeyutl –derive –inkey client_dhkey.pem –peerkey server_pubkey.pem –out shared_secret.bin

```
# على جانب العميل:
openssl pkeyutl -derive -inkey client_dhkey.pem -peerkey server_pubkey.pem -out shared_secre
t.bin
```

- على جانب الخادم:

openssl pkeyutl -derive -inkey server_dhkey.pem -peerkey client_pubkey.pem -out shared_secret.bin

```
# على جانب الخادم:
openssl pkeyutl -derive -inkey server_dhkey.pem -peerkey client_pubkey.pem -out shared_secre
t.bin
```

5) استخدام المفتاح المشترك لتشفير الاتصالات

- تحويل المفتاح المشترك إلى صيغة مناسبة للتشفير

openssl enc -aes-256-cbc -kfile shared_secret.bin -in command.txt -out command.enc

```
# تحويل المفتاح المشترك إلى صيغة مناسبة للتشفير
openssl enc -aes-256-cbc -kfile shared_secret.bin -in command.txt -out command.enc
```

- فك التشفير على الطرف الآخر

openssl enc -d -aes-256-cbc -kfile shared_secret.bin -in command.enc -out command_decrypted.txt

```
# فك التشفير على الطرف الآخر
openssl enc -d -aes-256-cbc -kfile shared_secret.bin -in command.enc -out command_decrypted.txt
```

6) تنفيذ التوقيع الرقمي للأوامر:

- العميل: توقيع الأمر قبل الإرسال

openssl dgst -sha256 -sign client.key -out command.sig command.txt

```
# العميل: توقيع الأمر قبل الإرسال
```

- الخادم: التحقق من التوقيع

openssl dgst -sha256 -verify client.pubkey -signature command.sig command.txt

آلية الحماية ضد الهجمات

- حماية ضد التنصت:
  - لا يتم نقل المفتاح السري عبر الشبكة
  - كل جلسة اتصال لها مفتاح مشترك فريد
- حماية ضد هجوم Man-in-the-Middle:
  - دمج آلية المصادقة باستخدام شهادات رقمية

إنشاء شهادة موقعة للخادم (اختياري)

openssl req -x509 -newkey rsa:2048 -keyout server.key -out server.crt -days 365

تحديث المفاتيح الدوري: - تغيير المعلمات الأساسية دورياً - تجديد المفاتيح المشتركة لكل جلسة اتصال

متطلبات التنفيذ

-تعديلات بروتوكول Modbus بإضافة مرحلة مصافحة أولية لتبادل المفاتيح، دعم تشفير AES للبيانات المتبادلة

-إدارة المفاتيح تخزين آمن لمعلمات DH وآلية لتحديث المعلمات الأساسية.

-متطلبات الأجهزة لدعم عمليات حسابية معقدة وذاكرة كافية لتخزين المعلمات

فوائد الحل

-أمان أمامي مثالي: حتى إذا سُرق المفتاح الخاص، لا يمكن فك تشفير الجلسات السابقة.

-مرونة عالية: يمكن تغيير المعلمات الأساسية دون التأثير على النظام.

-تكامل مع أنظمة موجودة: يمكن تطبيقه كطبقة إضافية فوق بروتوكول Modbus الحالي

6. الخاتمة.

- تم في بحثنا التحسين الأول لأمن المعلومات لبروتوكول DNP3 باستخدام خوارزمية ديفي هيلمان أثناء نقل البيانات بين محطتان Modbus، وتمت المحاكاة لهذه الخوارزمية بواسطة لغة Python للحصول على نفس قيمة المفتاح K.
- تم في التحسين الثاني استخدام الأداة OpenSSL في شبكة Modbus للمصادقة باستخدام شهادات رقمية موقعة ومشفرة بشكل امن باستخدام المفاتيح غير المتناظرة بين الوحدات الطرفية clients والمحطات الرئيسية servers وهذا حل مشكلة القناة الغير آمنة والقرصنة.
- تم أيضاً بناء نموذج شبكة صناعية تستخدم بروتوكول Modbus باستخدام محاكي الشبكات OPNET، بإجراء عملية تحليلية للنتائج وبهدف تحديد القيم الأفضل للعوامل المؤثرة في الأداء العام للشبكة الصناعيّة الحقلية عندما يتغير حجم البيانات بالإطار إلى 256 Byte للوصول للإدارة المثلى لبروتوكولModbus .
- توصلنا إلى أن زيادة الاستخدامية بزيادة عدد العقد في الشبكة بحيث لا يتجاوز عددها 1000 عقدة والموافق 0.4 ثانية

أما أهمية البحث فتكمن أولاً في تحقيق أمن معلومات وحماية الشبكة وإزالة مخاطر الهجمات بخوارزميات وأدوات فعالة وسهلة التنفيذ وثانياً في معرفة عدد العقد الأعظمي بشرط عدم تجاوز الزمن 0.5 ثانية وهو زمن استجابة الإطار في بروتوكولModbus .

7. التوصيات والآفاق المستقبلية.

- ✓ نوصي بدراسة تأثير عوامل أخرى تؤثر في بارامترات أداء الشبكة الصناعية مثل هجوم رفض الخدمة الموزع (DDOS) وغيرها من هجمات حرمان الخدمة.
- ✓ نوصي بزيادة موثوقية طريقة D–H باستخدام أعدادًا أولية كبيرة أو منحنيات إهليلجيه (ECDH) واستخدام الذكاء الاصطناعي في الحماية.
- ✓ ننصح باستخدام برنامج التعليمي الإلكتروني Cryptology مفتوحة المصدر والمجاني للتشفير بشكل رسومات بيانيةCryptographic وتشفير تحليليCryptanalytic.
- ✓ نوصي بوضع نماذج لبرتوكولات صناعيّة أخرى مثل (برتوكول PROFINET، برتوكول ASI، برتوكول CAN) وغيرها ودراسة وتحليل أداءها وتأثير الأمان على الأداء.

المراجع العلمية

[1] https://www.opc7.com / **"opc-server-for-Modbus"**. Industrial connectivity solutions and information

[2] https://www.opc7.com/ **"what-technologies-does-opc-use"**/ Industrial connectivity solutions and information.

[3] KUKI. A. 2014 **"Modeling computer networks by the help of OPNET tools** "Proceedings of the 9th International Conference on Applied Informatics, p. 251–258.

[4]. Amoah. R. 2016. **"Securing DNP3 broadcast communications in SCADA systems"**. IEEE Transactions on Industrial Informatics, Camtepe S & Foo, E 12(4), 1474-1485.

[5] AlANAZI. M, ABDUN. M, CHOWDHURY. MJM. 2023 **"SCADA vulnerabilities and attacks"** Computers & security 125: 103028.

[6] PRABHU. A. JENICE. D. RAJESH. H. 2023 **"Authentication of WSN for Secured Medical Data Transmission Using Diffie Hellman Algorithm".** Computer. Syst. Sci. Eng. 45(3): 2363-

[7] SETHI. A .S. HNATISHIN. V .Y. 2013 **"The Practical OPNET User Guide for Computer Network Simulation"**

[8] KRUPANEK.B, BOGACZ.R. 2016. **"OPNET Modeler simulations of performance for multi nodes wireless systems"**, Silesian University of Technology, Poland, 10p.

[9] MITTRA.A. 2017. **" What is the Diffie-Hellman Key Exchange Protocol and how does it work?** "CCNP, CompTIA, Network security.

[10] Larry L. Peterson, Bruce S. Davie. 2012 . **"Network Security"** in Computer Networks (Fifth Edition).

[11] KIM. B, LEE. D, CHOI. T**.** 2015 **"Performance Evaluation for Modbus/TCP Using Network Simulator NS3"**, IEEE, Kyungpook National University, Korea,10p.

[12] ALI. Q, 2007 **" Measurements and Performance Analysis of Industrial Ethernet"**. IEEE, University of Mosul, Iraq, 16p.

[13] DARWISH. I, IGOBE. O & SAADAWI. T 2016. **"Vulnerability Assessment and Experimentation of Smart Grid DNP3"**. Journal of Cyber Security and Mobility, 23-54.

[14] IGBE. O, DARWISH. I, SAADAWI. T. 2017**. "Deterministic dendritic cell algorithm application to smart grid cyber-attack**

detection". In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (pp. 199-204). IEEE.

[15] BERGE. 2004 ."**Fieldbuses for Process Control: Engineering, Operation and Maintenance"** ISA, p. 20, USA.

[16] AXELSON. J 2004. **"Practical modern SCADA protocols dnp3,608705 and Relate Systems"** Serial Port Complete. Lakeview Research communication systems.

[17] ATASSI. M, WAFAI. H 2024 **"Industrial Communication &Networks, Automation"** research seminars and lectures in College of Mechanical and Electrical Engineering at Al-Baath University and Damascus University.

[18] GUO. Y PAN. Y and CAI. L. 2016 **"OPNET-based Analysis of MTU Impact on Application Performance"**IEEE. Communication University. China.pp.197-207.

[19] SETHI.A.S, HnatyshynV.Y. 2013. **"The Practical OPNET User Guide for Computer Network Simulation"**

[20] FAHMY. S 2021 **"Secure voice cryptography based on Diffie-Hellman algorithm"**
IOP Conference Series Materials Science and
Engineering 1076(1):012057

[21] Mahmood,M and Al-Naima,F, **"OPNET Similation of data Transmission Network: A Case Study for Control System in Petroleum Refinery Complex in Iraq"**, IEEE. Nahrain University, Baghdad, Iraq,p12, 2015.

[22] Darwish, I., Igbe, O., & Saadawi, T. (2016). V**ulnerability Assessment and Experimentation of Smart Grid DNP3**. Journal of Cyber Security and Mobility, 5(1), 23.54.

[23] Igbe, O., Darwish, I., & Saadawi, T. (2017, June). **Deterministic dendritic cell algorithm application to smart grid cyber-attack detection**. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 199-204). IEEE.

[24] ANSSI, 2013. **"Digital Signature"** The private key, Wikiwix.

[25] Emsisoft, 2014, "**What is a digital certificate?**". Security Blog.

[26] Roche. D **"Securing communications"** Asymmetric encryptions. NSI terminal

[27] Solution ID: INFO141, 2024 "**OpenSSL-Quick-Reference- Guide** knowledge. digicert.com/general-information/
[28] L. Gyongyosi and S. Imre, **"A survey on quantum computing technology"**, Computer Science Review, vol. 31, pp. 51–71, 2019

تأثير المعالجة الحرارية المسبقة T4 على خصائص الوصلة الملحومة بطريقة لحام المزج الاحتكاكي لسبيكة الألمنيوم-AA 6082-

طالبة الماجستير: ريم قاص بولات[1]

إشراف: الدكتور محمود الأسعد[2]

الملخص: تم اعتماد منهجية معينة قائمة على تطبيق معالجة حرارية مسبقة على سبيكة الألمنيوم 6082 ومن ثم اللحام بطريقة المزج الاحتكاكي لصفيحتين بالأبعاد (100mm×60mm×8mm) ومقارنة النتائج.تم تطبيق المعالجة الحرارية T_4 والمؤلفة من محلولية بدرجتي حرارة (500°C−550°C) وزمني ابقاء (30min−1h) ومن ثم بُردت العينات بالماء البارد ومن ثم عُتِقَت طبيعياً بالإبقاء لفترتين زمنيتين (أسبوع−15 يوم).تم اختبار العينات قبل اللحام وتسجيل النتائج وبعد ذلك نُفِذَ اللحام على العينات المعالجة باستخدام أداة من الفولاذ وخطوتي لحام.أُجريت الاختبارات على العينات وتم تسجيل النتائج وتحليلها احصائياً باستخدام طريقة تاغوتشي ولوحظت كفاءة المعالجة المسبقة بتحسين خواص الوصلة اللحامية حيث كانت أفضل قيمة لمقاومة الشد 236,4Mpa عند درجة حرارة 550°C وزمن 1h وتعتيق لمدة 15يوم.

الكلمات المفتاحية: المعالجات الحرارية المسبقة− سبيكة الألمنيوم 6082− لحام المزج الاحتكاكي− معالجة المحلولية− تعتيق طبيعي

[1] طالبة ماجستير في كلية الهندسة الميكانيكية والكهربائية -قسم التصميم والإنتاج- جامعة حمص

[2] أستاذ مساعد في قسم هندسة التصميم والإنتاج في كلية الهندسة الميكانيكية والكهربائية -جامعة حمص

Effect of Pre-Heat Treatment T_4 on Properties of Weld Joint by Friction Stir Welding for Aluminum Alloy -AA 6082-

Master's student: Reem Qas Bwlat[3]

Supervised by: Dr.Mahmoud Al-Asaad[4]

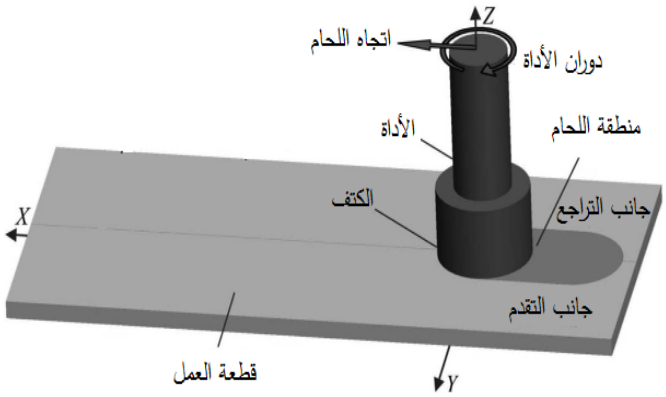
Abstract: A specific methodology was adopted based on applying a pre-heat treatment to aluminum alloy 6082 and then weld the two plates with dimensions (100×60×8)mm by friction stir welding then comparison between the results.Heat treatment was applied consisting of a solution at two temperatures of (500-550)°C and a holding time (30min-1hour) then the samples were cooled with cold water and then naturally aged by keeping for two periods of time (a week-15 days).The samples were tested before welding and the results were recorded after that welding was carried out on the treated samples using a steel tool and two welding steps.Tests were conducted on the samples and the results were recorded and statistically analyzed using the Taguchi method .The efficiency of the pre-treatment was noted by improving the properties, as the best value for tensile strength was 236 Mpa. At a temperature of 550°C, a time of 1 hour, and aging for 15 days.

[3] Master's student in the faculty of mechanical and electrical engineering-Design and production department-Homs university

[4] Assistant professor in the Design and production department at the faculty of mechanical and electrical engineering- Homs university

Keywrds: pre Heat Treatment– Aluminum Alloy 6082– Friction Stir Welding– Solution Treatment– Natural Aging.

مقدمة: يعتبر اللحام من أهم طرائق وصل الأجزاء والهياكل المعدنية للحصول على المنتج النهائي المطلوب إلا أن العديد من طرائق اللحام بحاجة لضبط بعض البارامترات من أجل الحصول على وصلة ذات صفات مرغوبة وخالية من العيوب قدر الإمكان حيث ظهرت في عام 1991 طريقة اللحام بالمزج الاحتكاكي والتي تم اكتشافها على يد Wayne Thomas في بريطانيا حيث ظهرت هذه الطريقة بدايةً كتطبيق مخبري لكن سرعان ما تم اكتشاف أهميتها في وصل العديد من المعادن وخاصة الألمنيوم[1].



الشكل(1): مراحل عملية لحام المزج الاحتكاكي[2]

على الرغم من فعالية طريقة اللحام بالمزج الاحتكاكي في وصل المعادن إلا أنه لابد للوصلة من أن تتعرض لتدهور في بعض الخواص الميكانيكية بفعل الحرارة والاحتكاك الناتجة عن العملية بالكامل لذا كان لابد من اجراء معين يمنع أو يخفف قدر الإمكان من هذا التدهور ألا وهو المعالجات الحرارية حيث تؤثر الحرارة بشكل كبير على بنية المعادن و تعمل على تحويل المادة من حالة فيزيائية إلى أخرى تؤدي لتغيير الترتيب الذري هذا بالإضافة لتغيير كمية التشوهات ضمن البنية البلورية، وللاستفادة من هذا التأثير بشكل يخدم زيادة الطلب على المواد المعدنية وللحصول على

مواد أكثر حداثة تلبي متطلبات العصر كان لابد من توظيف هذا التأثير بآلية معينة وبترتيب معين للبارامترات يخدم تحسين خواص الوصلات الملحومة بطريقة لحام المزج الاحتكاكي.

تشمل المعالجات الحرارية كافة عمليات التسخين والإبقاء عند درجات حرارة ثابتة ومن ثم التبريد بمعدلات مناسبة في أوساط تبريد مختلفة للمنتجات المعدنية بهدف تغيير كل من الخواص الميكانيكية، البنية الداخلية بالإضافة للتحكم قدر الإمكان بحالة الإجهادات المتبقية ضمن هذه المنتجات لتؤدي الغرض المصنوعة لأجله حيث تنوعت المعالجات الحرارية لابل طُبقت بآلية تسمح بالجمع ما بين أكثر من معالجة واحدة فقط وأطلق عليها رموز ودلالات حسب أنظمة التوصيف الحراري.

الجدول(1): رموز ودلالات أنظمة التوصيف الحراري[3]

F	السبيكة كما تم تلقيها من عمليات التشكيل المختلفة وذلك دون ذكر معلومات عن أي نسب تشكيل أو حرارة معينة
O	التخمير وهي المعالجة التي تطبق على السبيكة من أجل الحصول على أفضل مطيلية وثبات في الأبعاد
H	التصلد الانفعالي وهي العمليات التي تطبق على السبيكة وذلك من أجل تقويتها من خلال عمليات التشكيل المختلفة ومن الممكن أن تلحق عمليات التشكيل بعض المعالجات الحرارية وعادةً ما يلحق بالحرف H رقمين أو أكثر
W	المحلولية وهي خاصة بالسبائك التي تعتق عند درجة حرارة الغرفة
T	المعالجة الحرارية وهي مجموعة معالجات تختلف عن ظروف الدلالات السابقة وتطبق عادةً على السبائك التي يمكن أن تخضع لبعض عمليات التشكيل عادةً ما تلحق الحرف Tرقمان أو أكثر

للحصول على الحاجة المرجوة من المعالجات الحرارية لابد من معرفة كل من درجة الحرارة، زمن الإبقاء ومعدلات التبريد المناسبة لكل معدن لأنه في حال عدم ملائمة أي عامل من العوامل السابقة مع المعدن المعالج يؤدي بدوره لتأثير ضار وغير مرغوب به فيما يخص خواص المعدن.

بدأ العديد من الباحثين باجراء دراسات وابحاث تجمع مابين اللحام والمعالجة الحرارية وذلك للاستفادة من إمكانية الآليتين للحصول على الخواص المرجوة والمطلوبة كما لجأ البعض منهم لتنظيم سير عملية التجارب بشكل أكثر تنظيماً وبوقت أقصر باعتمادهم على طرق تصميم التجارب وكان أكثرها شهرةً واعتماداً في الأبحاث طريقة تاغوتشي والتي تم اقتراحها من قبل Dr.Genichi Taguchi في أواخر الـ 1950 وبداية الـ 1960حيث اعتمدت هذه الطريقة على نظام معين قائم على تشكيل مصفوفة الهدف منها دراسة بارامترات العملية لكن بعدد أقل من التجارب العملية كما أنها تتيح للباحث تحديد أي بارامتر يملك التأثير الأكبر في العملية المدروسة[4].

قام الباحثونA.ALDwairi وآخرون بإجراء عدد من التجارب لمعرفة كفاءة المعالجة الحرارية المسبقة للحام وذلك بمعالجة قطعة من سبائك الألمنيوم–النحاس بسماكة 8mm حيث كانت المعالجة عبارة عن تخمير بدرجة حرارة 415°C لمدة 1,5h ومن ثم تقسية بالماء البارد كما اتجه الباحث أيضاً إلى منهجية أخرى في المعالجة فكانت سلسلة المعالجة الأخرى للقطعة هي عبارة عن محلولية عند درجة حرارة 490°C لمدة 1h ومن ثم تسقية بالماء ومن ثم تعتيق طبيعي عند درجة حرارة الغرفة ثم أُجريت عملية اللحام بالمزج الاحتكاكي و توصل الباحث إلى أن الوصلة المعرضة لتعتيق مسبق تمتلك أكبر قيمة للقساوة وأقل معدل للاهتراء مقارنة بالوصلة المعرضة للتخمير المسبق [5].

قام الباحثون H.Aydin وآخرون عام 2009 بإجراء مجموعة من التجارب على سبيكة الألمنيوم 2024 من خلال تطبيق عدد من المعالجات الحرارية على صفيحتين بسماكة 3mm حيث قسمت المعالجات الحرارية إلى خمس مجموعات وهي:

الجدول(2): مجموعات المعالجات الحرارية الخمسة

تعتيق طبيعي	تعتيق اصطناعي		سقاية	محلولية		رمز	رقم
زمن الإبقاء	زمن الإبقاء	درجة الحرارة	معدل التبريد	زمن الإبقاء	درجة الحرارة		
عدة سنوات			ماء بارد	2,5 h	510°C	T_4	1
			ماء بارد	2,5 h	510°C	W	2
	10h	100°C	ماء بارد	2,5 h	510°C	T_{6d}	3
	10h	190°C	ماء بارد	2,5 h	510°C	T_{6b}	4
			هواء	2,5 h	510°C	O	5

بعد تطبيق هذه المعالجات أجرى الباحث لحام مزج احتكاكي لوصل الصفيحتين و توصل بأن للمحلولية والتعتيق دور كبير في تحسين كفاءة الوصلة حيث أن أفضل قيمة للمتانة يتم الحصول عليها من عينات المجموعة الرابعة وللقساوة والمتانة معاً هي عينات المجموعة الأولى أما بالنسبة للاستطالة فيتم الحصول عليها من عينات المجموعة الخامسة[6] .

قام الباحثون S.Verma وآخرون بعام 2019 بدراسة تأثير ثلاثة ظروف حرارية مختلفة على السبيكة 6082 حيث اعتمد الباحث في خطته البحثية على دراسة وصلة ملحومة بدرجة حرارة الغرفة بالإضافة لثلاث وصلات مسخنة مسبقاً لثلاث درجات حرارة مختلفة °C(150−125−100) بالإضافة لثلاث وصلات مبردة مع اللحام بثلاث طرق بالماء الفاتر والماء البارد والحار بدرجات حرارة على الترتيب 2°C،22°C،65°C وبعد الدراسة والبحث تبين للباحثين بأن أقل معدل اهتراء كان عند تسخين الوصلة للدرجة 100°C [7].

لجأ الباحثون R.poongkundran وآخرون في عام 2016 إلى تسخين صفيحة من سبيكة الألمنيوم AA7075 بسماكة6,35mm لدرجات حرارة مختلفة °C(250−200−150−100) حيث تم تنفيذ لحام المزج الاحتكاكي بعد التسخن للعينات وفي النهاية توصل الباحث بأنه يتم الحصول على

أفضل قيم للخواص الميكانيكية عند التسخين لدرجة حرارة 100°C وتبدأ الخواص بالانحدار بالارتفاع بدرجة الحرارة[8] .

قام الباحثون (A.Alnajjar) عام 2021 بدراسة لمعرفة كفاءة المعالجة الحرارية المسبقة للحام قطعتين من سبيكة الألمنيوم 6061 بسماكة 5mm حيث اعتمد في معالجته الحرارية المسبقة على عدة ترتيبات.

الجدول(3): منهجية ترتيب المعالجات الحرارية

1	مجموعة عينات المعالجة محلولياً عند درجة حرارة 530°C وزمن إبقاء لمدة ساعة ومن ثم التبريد بالماء البارد
2	مجموعة عينات المعتقة طبيعياً وذلك لمدة اسبوع
3	مجموعة العينات المعتقة اصطناعياً عند درجتي حرارة °C(220–180) وأزمنة إبقاء –2–1) 6–10) h

توصل الباحث بأن الحالة الأولية للمعدن تؤثر بشكل كبير على كفاءة الوصلة الملحومة حيث كانت وسطياً بحدود 60% ووصلت بشكل أعظم إلى 99%. [9].

من خلال الدراسات السابقة نلاحظ اهتمام معظم الأبحاث بدراسة تأثير المعالجة الحرارية التي تسبق لحام المزج الاحتكاكي لذا في هذا البحث سوف يتم دراسة تأثير المعالجة الحرارية المسبقة على وصلة لحام مزج احتكاكي لسبيكة ألمنيوم 6082 من خلال اجراء عدد من التجارب ومن ثم اجراء عدد من الاختبارات الميكانيكية على العينات لابل سوف يتم الاستعانة بطريقة تاغوتشي لتصميم تجارب البحث والمساعدة في معرفة البارامتر الذي يملك التأثير الأكبر على الخواص الميكانيكية.

هدف البحث: يهدف البحث إلى زيادة كفاءة المنتجات المصنوعة من سبائك الألمنيوم ويركز بالأخص على الوصلات اللحامية المنجزة بطريقة لحام المزج الاحتكاكي للسبيكة 6082 بسماكة

8mm وذلك لما لهذه السبيكة أهمية في كثير من التطبيقات الصناعية ولصعوبة لحام هذه القيمة من السماكة دون ظهور مشاكل وعيوب في الوصلة اللحامية وذلك من خلال الاعتماد على قدرة المعالجات الحرارية المسبقة وخاصةً T4 المكونة من محلولية و تعتيق طبيعي.في التأثير على توزع العناصر الأساسية للسبيكة بمنظومة معينة وذلك وفقاً للخاصية المطلوب تحسينها وفي الحد والتخفيف من الآثار اللاحقة لبارامترات عملية اللحام على السبيكة المدروسة وبالتالي توظيف المعالجة الحرارية المسبقة للحصول على وصلة لحامية بمواصفات جيدة.

مواد وطرق البحث:

أولاً: فرن المعالجة الحرارية:

تم استعمال فرن المعالجة الحرارية نوع CARBOLITE بحيث تصل أعلى درجة حرارة للدرجة 1200°C ويبين الجدول التالي مواصفات الفرن المستخدم

الجدول (4): المواصفات الفنية لفرن المعالجة الحرارية المستخدم

درجة الحرارة العظمى	1200°C
درجة حرارة التشغيل	1100°C
الزمن اللازم للتسخين الكامل	45min
أبعاد الحجرة	400×245×235mm
الأبعاد الخارجية	705×505×675mm
الأبعاد الخارجية مع الباب	905×505×675mm
الحجم	13Lit
الاستطاعة العظمى	7000W
الوزن الكلي	63Kg

ويتم استخدام الفرن من أجل معالجة العينات قبل اللحام بالإضافة لمعالجة أداة اللحام قبل تشكيلها.

الشكل(2):الفرن الكهربائي المستخدم في المعالجة الحرارية

يتم اعتماد معالجة حرارية تطبق على القطع قبل اجراء عملية الوصل بعملية المزج الاحتكاكي وهي عبارة عن المعالجة T_4 والتي تتألف من المحلولية والتعتيق الطبيعي.

الجدول(5): المعالجة الحرارية المسبقة المطبقة قبل تنفيذ اللحام

T_4						
التعتيق الطبيعي		**السقاية**	**المحلولية**			
زمن الابقاء		تبريد	زمن الإبقاء		الحرارة	
time2	time1	بالماء	time2	time1	T2	T1
15days	7days	البارد	1h	30min	550	500

ثانياً: المواد الخام والعينات:

المادة المستخدمة في هذا البحث هي عبارة عن سبيكة ألمنيوم 6082 وتم التحقق من التركيب الكيميائي لهذه السبيكة باستخدام جهاز التحليل الطيفي (Spectro Analytical Instrument) حيث تم الحصول على النتائج وهي مطابقة لمعايير (B209M–ASTM).

الجدول(6): التركيب الكيميائي للسبيكة المستخدمة في البحث

العنصر	Al%	Si%	Fe%	Cu%	Mn%
6082 المعيارية	rest	0,7−1,3	0,50	0,10	0,4−1
نتائج التحليل المقاسة	97,4	0,948	0,269	0,061	0,399
العنصر	Mg%	Cr%	Zn%	Ti%	−
6082 المعيارية	0,6−1,2	0,25	0,20	0,10	−
نتائج التحليل المقاسة	0,739	0,018	0,028	0,021	−

الشكل(3): العينة كما تم تلقيها

تم شحذ وجه العينة قبل قصها وتنظيفها وذلك منعاً لأي خطأ أو عرقلة في عملية القياس والاختبار فيما بعد ومن ثم تم الاعتماد على الفارزة نوع (Liang Wai Milling Machine) من أجل تقسيم العينة للأبعاد الأولية وفيما بعد تم تقطيع العينات يدوياً بالمنشار اليدوي وتنظيف الأسطح الجانبية بالجلخ الأرضي للحصول على القطع النهائية بالأبعادmm(8×100×60).

الشكل(4): مراحل تجهيز العينات

ثالثاً: آلة اللحام والأداة:

بناءً على القراءة المكثفة للأبحاث السابقة ومعرفة مزايا ومساوئ كل أداة على حدة وبناءً على السماكة المختارة تم الاعتماد على شكل أداة ذات رأس مخروطي وكتف مسطح من فولاذ H13 و هو نوع من أنواع الفولاذ السبائكي حيث يملك خواص ميكانيكية مميزة لأداة اللحام كتحمل التعب الحراري ودورات التسخين والتبريد ومقاومته للتآكل والتكسير كما يتمتع بالاستقرار عند المعالجة الحرارية وهو ذو صلابة عالية ويستخدم على نطاق واسع لأدوات اللحام [10].

الجدول (7): أبعاد أداة اللحام المستخدمة

قطر الكتف	طول الكتف	القطر الأول للرأس	القطر الثاني للرأس	طول الرأس
20mm	25mm	6mm	7,5mm	7,9mm

تم تنفيذ المعالجات الحرارية المطلوبة بحيث يتم التخمير للأداة بشكل تدريجي لتقل قساوتها ومن ثم يتم تشكيلها وصولاً للشكل المطلوب.

بعد الحصول على الشكل النهائي المطلوب للأداة يتم اجراء معالجة التقسية وذلك لزيادة قساوة مادة الأداة وكذلك زيادة مقاومتها للتعب الحراري وللتآكل، حيث تتم المعالجة على مرحلتين ومن بعدها يتم تطبيق المراجعة النهائية على الأداة ويتم تكرارها مرتين متتاليتين بنفس البارامترات الحرارية وذلك لضمان التحول الكامل للأوستنيت المتبقي إلى مارتنسيت حيث تم قياس قساوة الأداة وكانت 657HV وهي مقاربة للقيم المرجعية.

الجدول (8): المعالجات الحرارية المطبقة لتجهيز الأداة

تخمير Annealing		تشغيل	تقسيةHardening				إرجاع Tempering	
			تسخين preheat		Austenitizing			
T	Time		T	Time	T	Time	T	Time
220	15min		220	1h	1190	4min	540	1h
420	15min		500	1h	تبريد بالزيت		تكرر معالجة الارجاع مرتين عند نفس الشروط والتبريد بالهواء	
640	15min		730	1h				
870	15min							
تبريد بالفرن لـ540								
تبريد نهائي بالهواء								

الشكل (5): أداة اللحام النهائية

يتم تنفيذ اللحام على الفارزة العامودية نوع ARHYM وذلك بوضع القطع المراد لحامها على طاولة الآلة والتثبيت الجيد والمعايرة بشكل دقيق ويتم اعتماد خطوتين للحام بشكل ثابت وزاوية إمالة بمقدار 2°.

الشكل (6): آلة اللحام(الفارزة)

الجدول(9): بارامترات اللحام المستخدمة

الخطوةmm/rot	سرعة التقدمmm/min	سرعة الدوران rpm
0,04	45	1110
0,19	218	

رابعاً: أساسيات التصميم وترتيب العينات:

يتم بدايةً وبالاعتماد على كل من بارامترات المعالجة واللحام ترتيب العينات باستخدام برنامج minitab والاعتماد على طريقة تاغوتشي في تصميم التجارب.

في البدء يتم تشكيل مصفوفة عامودية بأربعة عوامل لكل عامل(بارامتر) مستويين أي قيمتين وبالتالي يتم الحصول على مصفوفة L8 بثمان سطور وأربعة أعمدة وعليه يتم الحصول على ثمان عينات للاختبار.

الجدول (10): المصفوفة العمودية لترتيب عينات التجارب في البحث

	C1	C2	C3	C4
	Tw	soaktime	timeaging	pitch
1	500	30	7	0.04
2	500	30	15	0.19
3	500	60	7	0.19
4	500	60	15	0.04
5	550	30	7	0.19
6	550	30	15	0.04
7	550	60	7	0.04
8	550	60	15	0.19

فيما بعد يتم تصنيف العوامل بالترتيب من الأكثر تأثير إلى الأقل تأثير بعد الحصول على نتائج الاختبار ويعتمد ذلك على مفهوم الرتبة في تصنيف البارامترات (العوامل) حسب أهميتها تنازلياً، أي أن العامل ذو الرتبة الأولى يكون العامل الأكثر تأثيراً وتتحدد رتبة كل عامل بناءً عل قيمة Delta والتي تمثل الفرق بين متوسطات الاستجابة عند أعلى وأدنى مستوى لكل عامل.

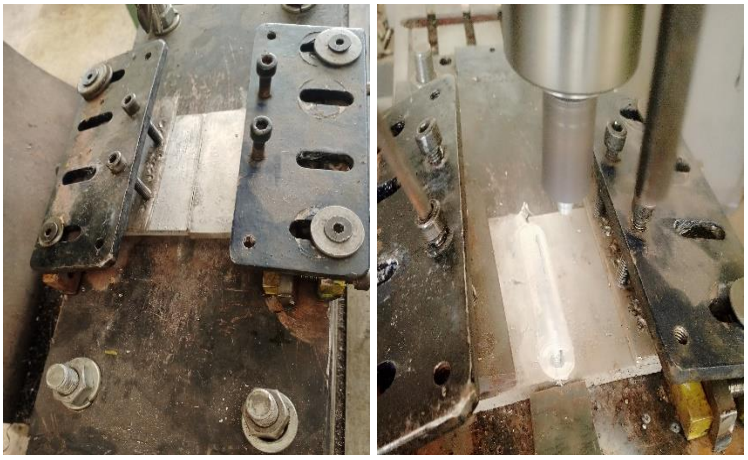
خامساً: تنفيذ اللحام :

يتم اجراء اختبارات للعينة قبل اجراء أية معالجة حرارية ولحام وذلك للمقارنة فيما بعد بين النتائج.

كما يتم لحام عينتين دون أية معالجة حرارية وتسجيل النتائج أيضاً للمقارنة فيما بعد.

يتم اعتماد ثمان عينات تتم معالجتها بناءً على الترتيب السابق ضمن فرن المعالجة الحرارية ويتم تنفيذ اختبار الشد عليها لمعرفة النتائج.

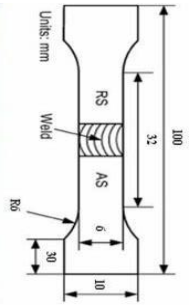
فيما بعد يتم تنفيذ المعالجة الحرارية على ثمان عينات أخرى ومن ثم اللحام على الفارزة العمودية بحيث يتم البدء بمرحلة الغرز لأداة اللحام ومن ثم شوط التقدم ومن ثم مرحلة التراجع للأداة.



الشكل(7): تنفيذ اللحام على العينات المعالجة حرارياً

سادساً: الاختبارات التجريبية والاحصائية والنتائج:

يتم اجراء اختبار الشد على جهاز الشد نوع (TINIUS OLSEN HK50S) أما عينة اختبار الشد للحام فيتم اقتطاعها بشكل عمودي على خط اللحام وبالأبعاد الموضحة بالشكل(8) حسب المواصفة ASTM E8M [11].



الشكل(8): جهاز اختبار الشد وشكل عينة الاختبار

تقسم مجموعات الاختبار لأربعة مجموعات وهي :

- العينة الأساس كما تم تلقيها
- مجموعة العينات الملحومة فقط دون معالجة مسبقة
- مجموعة العينات المعالجة فقط
- مجموعة العينات المعالجة مسبقاً والملحومة فيما بعد

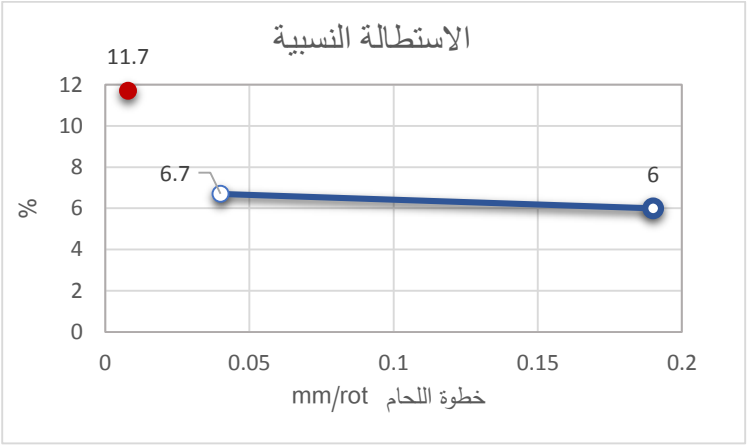
وفيما يلي جداول بأهم النتائج للمجموعات الأربعة:

الجدول(11): نتائج اختبار العينة الأساس

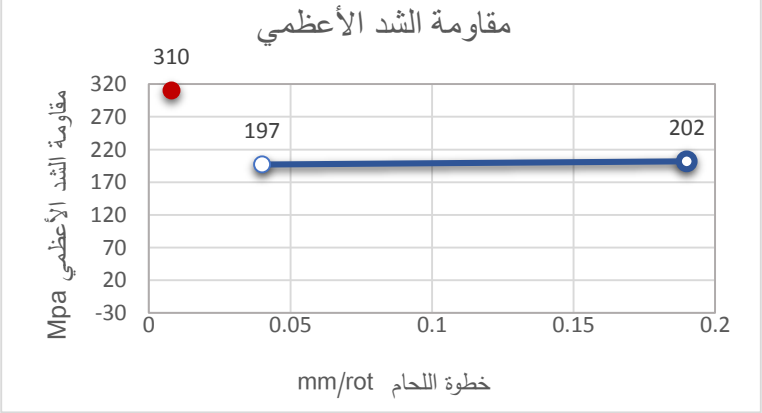
مقاومة الشد الأعظمي	الإستطالة
310 Mpa	11,7 %

الجدول(12):نتائج اختبار العينات الملحومة فقط

رقم العينة	W1	W2
بارامترات اللحام	1100 rpm	1100 rpm
	$mm/min45$	$mm/min218$
	0,04 mm/rot	0,19 mm/rot
مقاومة الشد الأعظمي Mpa	197,836	202,783
الإستطالة%	6,7	6



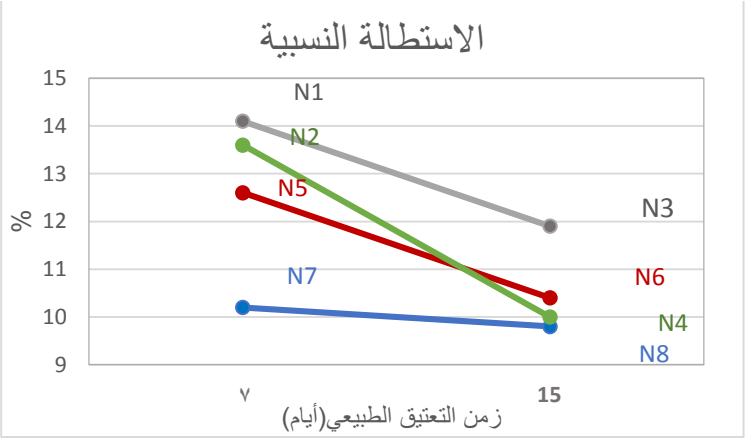
الشكل (9):مقارنة الاستطالة النسبية للعينات الملحومة كما تم تلقيها مع المعدن الأساس



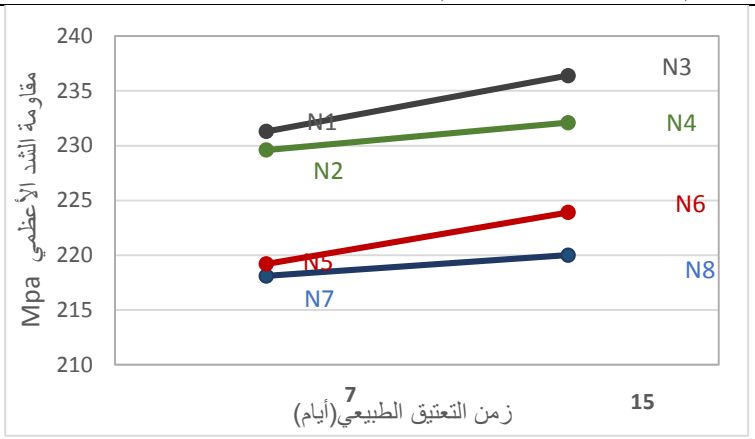
الشكل (10):مقارنة مقاومة الشد العظمى للعينات الملحومة للسبيكة كما تم تلقيها مع المعدن الأساس

الجدول(13): نتائج اختبار مجموعة العينات المعالجة فقط

الاستطالة %	مقاومة الشد الأعظمي Mpa	التعتيق الطبيعي Days	بارامترات المحلولية		N
			min	C°	
10,2	218,1	7	30	500	**N1T4**
9,8	220	15	30	500	**N2T4**
12,6	229,6	7	60	500	**N3T4**
10,4	232,1	15	60	500	**N4T4**
13,6	219,2	7	30	550	**N5T4**
10	223,9	15	30	550	**N6T4**
14,1	231,3	7	60	550	**N7T4**
11,9	236,4	15	60	550	**N8T4**



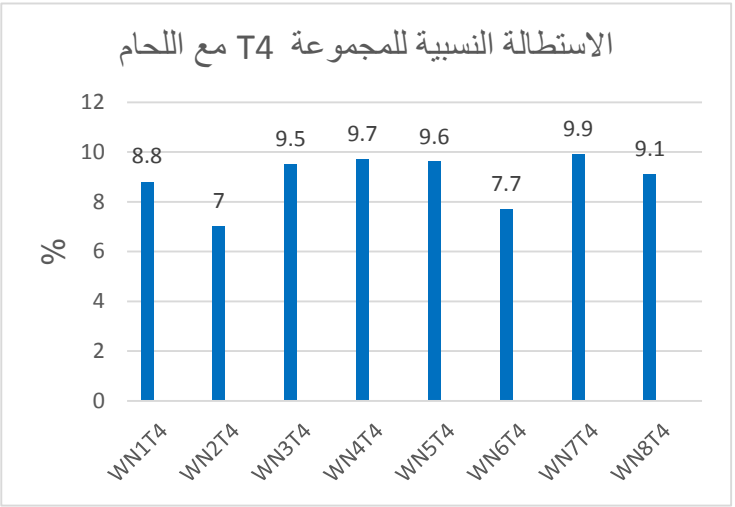
الشكل (11): مخطط مقارنة نتائج الاستطالة النسبية لعينات المجموعة T4 قبل تنفيذ اللحام



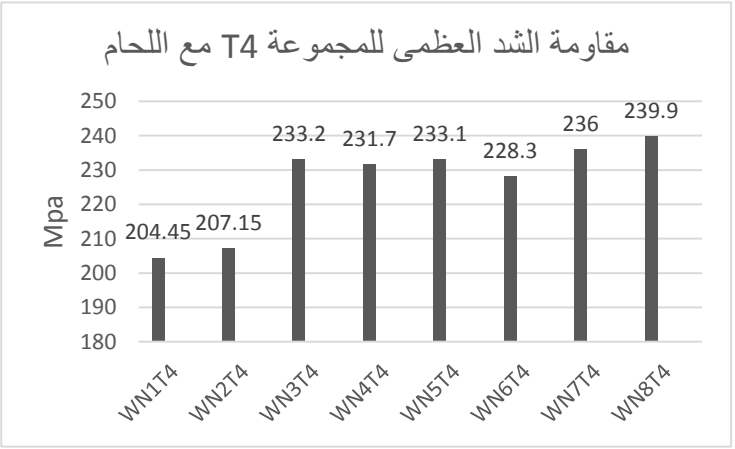
الشكل (12): مخطط مقارنة نتائج مقاومة الشد العظمى لعينات المجموعة T4 قبل تنفيذ اللحام

الجدول(14): نتائج اختبار مجموعة العينات المعالجة مسبقاً و الملحومة

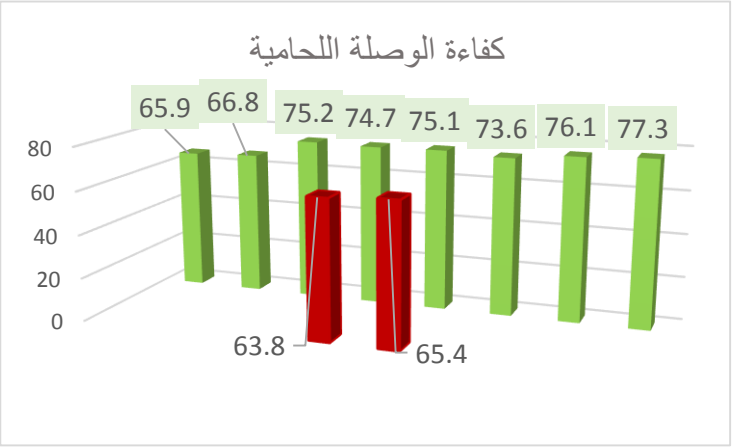
رقم العينة	بارامترات المحلولية		بارامترات التعتيق الطبيعي Days	بارامترات اللحام	مقاومة الشد الأعظمي Mpa	الاستطالة النسبية %
	الحرارة C°	زمن الإبقاء min				
WN1T4	500	30	7	0,04	204,45	8,8
WN2T4	500	30	15	0,19	207,15	7
WN3T4	500	60	7	0,19	233,2	9,5
WN4T4	500	60	15	0,04	231,7	9,7
WN5T4	550	30	7	0,19	233,1	9,6
WN6T4	550	30	15	0,04	228,3	7,7
WN7T4	550	60	7	0,04	236	9,9
WN8T4	550	60	15	0,19	239,9	9,1



الشكل (13): مخطط الاستطالة النسبية لعينات T4 بعد تنفيذ اللحام



الشكل (14): مخطط مقاومة الشد العظمى لعينات T4 بعد تنفيذ اللحام



الشكل (15): مخطط مقارنة كفاءة الوصلات اللحامية قبل المعالجة المسبقة وبعد تطبيقها

بعد الانتهاء من الاختبارات ومعرفة النتائج على أرض الواقع تبدأ هنا عملية التحليل لهذه النتائج بالاعتماد على طريقة تاغوتشي بحيث يتم ادخال النتائج إلى البرنامج لمعرفة ترتيب تأثير النتائج حسب الأهمية تنازلياً.

يتم تحليل النتائج فقط للعينات المعالجة والملحومة فبعد ترتيب العينات يتم ادخال عمود بنتائج مقاومة الشد ومن ثم الاستطالة فيما بعد.

الجدول(15): ترتيب تأثير العوامل تنازلياً حسب الأهمية بالنسبة لمقاومة الشد

Larger is better

Level	Tw	soaktime	timeaging	pitch
1	46.80	46.76	47.09	47.03
2	47.39	47.43	47.10	47.16
Delta	0.60	0.66	0.00	0.12
Rank	2	1	4	3

الجدول(16): ترتيب تأثير العوامل تنازلياً حسب الأهمية بالنسبة للاستطالة

Larger is better

Level	Tw	soaktime	timeaging	pitch
1	18.77	18.29	19.50	19.07
2	19.12	19.60	18.39	18.82
Delta	0.35	1.30	1.11	0.25
Rank	3	1	2	4

سابعاً: مناقشة النتائج:

بعد اجراء العديد من الاختبارات تم التوصل للعديد من النتائج وقسمت لثلاثة أقسام وكان أبرزها:

نتائج عينات اللحام فقط:

- أدى اللحام لانخفاض الخواص الميكانيكية مقارنة بخواص السبيكة الأساس حيث يلاحظ بأن الاستطالة انخفضت لمقدار النصف من استطالة السبيكة الأساس.
- مع زيادة الخطوة تزداد مقاومة الشد للوصلة اللحامية على عكس الاستطالة فإنها تتناقص مع زيادة الخطوة لكن بشكل غير ملحوظ.
- كانت أعلى كفاءة للوصلة بمقدار 65,41%.

نتائج عينات المعالجة الحرارية فقط:

- مع زيادة درجة حرارة وزمن إبقاء المحلولية تزداد كل من مقاومة الشد والاستطالة النسبية
- مع ازدياد زمن التعتيق الطبيعي تنخفض الاستطالة
- تكون أعلى قيمة للاستطالة عند درجة حرارة محلولية 550°C وزمن إبقاء 1h وزمن تعتيق طبيعي 7d بقيمة 14,1%.
- تكون أدنى قيمة للاستطالة عند درجة حرارة محلولية 500°C وزمن إبقاء 30 min وزمن تعتيق 15d بقيمة 9,8%.

- تكون أعلى قيمة لمقاومة الشد عند درجة حرارة محلولية 550°C وزمن إبقاء 1h وزمن تعتيق طبيعي15d بقيمة 236,4 Mpa.
- تكون أدنى قيمة لمقاومة الشد عند درجة حرارة محلولية 500°C وزمن إبقاء 30 min وزمن تعتيق 7d بقيمة 218,1 Mpa.

نتائج عينات المعالجة المسبقة واللحام معاً:

- تكون أعلى كفاءة للوصلة المعالجة مسبقاً 77,3% وأقل كفاءة 65,9% بحيث تبقى أكبر من كفاءة الوصلات اللحامية دون أي معالجة حرارية.
- يؤثر ازدياد الخطوة سلباً على الاستطالة
- تكون أعلى قيمة للاستطالة عند درجة حرارة 550°C وزمن 1h وزمن تعتيق 7d وخطوة 0,04 mm/rot بقيمة 9,9.
- تكون أدنى قيمة للاستطالة عند درجة حرارة 500°C وزمن إبقاء 15d وخطوة 0,19 mm/rot بقيمة 7% لكن مع ذلك تبقى أكبر من أعلى استطالة في عينات اللحام فقط.
- تكون أعلى قيمة لمقاومة الشد عند درجة حرارة 550°C وزمن1h وزمن تعتيق 15d وخطوة 0,19 mm/rot بقيمة 239,9 Mpa.
- تكون أدنى قيمة لمقاومة الشد عند درجة حرارة 500°C وزمن 30 min وزمن تعتيق 7d وخطوة 0,04 mm/rot بقيمة 204,45 Mpa.

ثامناً: الاستنتاجات والتوصيات:

تم في هذا البحث تطبيق المعالجة الحرارية T_4 المؤلفة من (معالجة محلولية + تبريد بالماء البارد + تعتيق طبيعي) ثم اللحام على سبيكة ألمنيوم 6082 بسماكة 8mm ولوحظ بعد المقارنة ما بين نتائج اللحام فقط والمعالجة واللحام معاً بأن هذه المعالجة المسبقة تحسن بشكل كبير من الخواص المتدهورة نتيجة اللحام ويبدو ذلك واضحاً من قيم مقاومة الشد حيث تكون أقل كفاءة للوصلة اللحامية في حال تطبيق هذه المعالجة أعلى من أدنى كفاءة في حال اللحام فقط.

من الممكن اعتبار هذا البحث كمرجع للأبحاث المشابهة مع الانتباه لطبيعة كل مادة وبارامترات اللحام أيضاً ومن الممكن أيضاً التوسع بتطبيق معالجات حرارية مسبقة أخرى.

تاسعاً: المراجع: References

[1] Krasnowski, K. (2014). Experimental study of FSW t-joints of EN-AW 6082-T6 and their behaviour under static loads. Arabian Journal for Science and Engineering, 39(12), 9083-9092

[2] Šibalic, N., & Vukčevič, M. (2019). RESEARCH ON THE QUALITY OF THE WELDED JOINT OF ALUMINIUM ALLOY SHEET AA6082-T6 USING FSW, MIG AND TIG METHODS. Materials & Technologies/Materiali in Tehnologije, 53(5).

[3] ASME Internationa.(1991). Heat Treating of Aluminum Alloys.*ASME Handbook*(vol.4, p. 841-879).

[4] Atil, H., & Unver, Y. (2000). A different approach of experimental design: Taguchi method. Pakistan journal of biological sciences, 3(9), 1538-1540

[5] Al-Dwairi, A. F., Abdelall, E., & Rivero, I. (2020). Effect of Pre-welding Heat Treatment on the Mechanical Properties of Friction Stir Welded Al–4 wt.% Cu Alloys. Metallography, Microstructure, and Analysis, 9, 169-179.

[6] Aydın, H., Bayram, A., Uğuz, A., & Akay, K. S. (2009). Tensile properties of friction stir welded joints of 2024 aluminum alloys in different heat-treated-state. Materials & Design, 30(6), 2211-2221.

[7] Verma, S., Misra, J. P., & Gupta, M. (2019, July). Effect of preheating and water-cooling on the wear properties of FS welded AA6082 joint. In Journal of Physics: Conference Series (Vol. 1240, No. 1, p. 012116). IOP Publishing.

[8] Poongkundran, R., & Senthilkumar, K. (2017). Effect of preheating on microstructure and tensile properties of friction stir welded AA7075 aluminium alloy joints. Brazilian Archives of Biology and Technology, 59Poongkundran, R., & Senthilkumar, K. (2017). Effect of preheating on microstructure and tensile properties of friction stir welded AA7075 aluminium alloy joints. Brazilian Archives of Biology and Technology, 59

[9] Al Najjar,N.A.(2021).The influence of microstructure variables of aluminium alloys on the strength of joint welded by the friction stir welding.[Dissertation].Homs university,approved(in Arabic).

[10] Al Assad, M., Al Massoud, T., & Al Najjar, A. (2021). Effect of the post-heat treatment on the welded joint properties by friction stir welding method for similar aluminum alloys-AA6082-.Journal of Homs university, 43(9), 37-64,approved(in Arabic).

[11] ASTM, Standard test methods for Tension Testing of metallic materials, E8-15a annual book of ASTM standards, American Society for Testing and Materials,Philadelphia.

تقييم استهلاك الموارد لخوارزميات التعلم الآلي في كشف الشذوذ في شبكات سلاسل الكتل

علي عطية[1] أ.د.ماهر عباس[2] د.وسيم رمضان[3]

(1) طالب دكتوراه في قسم هندسة الشبكات والنظم الحاسوبية، كلية الهندسة المعلوماتية، جامعة حمص.

(2) أستاذ دكتور في قسم هندسة الشبكات والنظم الحاسوبية، كلية الهندسة المعلوماتية، جامعة حمص.

(3) دكتور في كلية الهندسة الزراعية، جامعة حمص.

الملخص

يعد اكتشاف الشذوذ في سلاسل الكتل إجراءً أمنياً بالغ الأهمية، يركز على تحديد الأنماط غير العادية أو غير المتوقعة في شبكات سلاسل الكتل والمعاملات. من خلال الكشف بشكل استباقي عن هذه الانحرافات، يهدف إلى حماية أنظمة سلاسل الكتل من الهجمات الضارة والاحتيال ومشاكل الأداء، وضمان سلامة وموثوقية التكنولوجيا.

يستعرض هذا البحث تحليلاً شاملاً لاستهلاك الموارد اللازمة لتشغيل خمسة من خوارزميات التعلم الآلي: شجرة القرار، الغابة العشوائية، أقرب جار، الانحدار اللوجستي، ومصنف الانتخاب بين أفضل ثلاثة خوارزميات. تم تقييم أداء هذه الخوارزميات من حيث استهلاك الذاكرة، نسبة استخدام المعالج، ومتطلبات التخزين، إضافةً إلى دقتها في كشف الشذوذ باستخدام معايير مثل الدقة و .F1-score كما تم تصنيف استهلاك الموارد لهذه الخوارزميات لثلاثة تصنيفات بحيث يتم تصنيف الخوارزمية

الى تصنيف مرتفع لاستهلاك الموارد او تصنيف متوسط لاستهلاك الموارد أو تصنيف منخفض لاستهلاك الموارد.

أظهرت النتائج أن الغابة العشوائية كانت الأفضل بين الخوارزميات ذات المتطلبات العالية، محققة دقة 99% و F1-score قدره 0.99. بينما تفوقت شجرة القرار بين الخوارزميات ذات المتطلبات المتوسطة بدقة 94.6% و F1-score بلغ 0.95. أما في فئة الخوارزميات ذات الموارد المنخفضة، فقد كانت خوارزمية الانحدار اللوجستي الأكثر كفاءة بدقة 50.22 و f1score 0.5.

الكلمات المفتاحية: سلاسل الكتل، كشف الشذوذ، التعلم الالي، تحليل الموارد، التصنيف.

Evaluation of Resource Consumption of Machine Learning Algorithms in Anomaly Detection in Blockchain Networks

Ali Atia [(1)], Prof. Maher Abbas [(2)], Dr. Wassim Ramadan [(3)]

(1) PhD student in the Department of Networks and Computer Systems Engineering, Faculty of Information Engineering, University of Homs.

(2) Professor in the Department of Networks and Computer Systems Engineering, Faculty of Information Engineering, University of Homs.

(3) PhD in the Faculty of Agricultural Engineering, University of Homs.

Abstract

Blockchain anomaly detection is a critical security measure that focuses on identifying unusual or unexpected patterns in blockchain networks and

transactions. By proactively detecting these anomalies, it aims to protect blockchain systems from malicious attacks, fraud, and performance issues, and ensure the safety and reliability of the technology.

This paper presents a comprehensive analysis of the resource consumption required to run five machine learning algorithms: decision tree, random forest, nearest neighbor, logistic regression, and selection classifier among the top three algorithms. The performance of these algorithms was evaluated in terms of memory consumption, processor utilization, and storage requirements, in addition to their accuracy in anomaly detection using criteria such as accuracy and F1-score.

The resource consumption of these algorithms was also classified into three categories, so that the algorithm is classified into a high resource consumption category, a medium resource consumption category, or a low resource consumption category. The results showed that random forest was the best among the algorithms with high requirements, achieving an accuracy of 99% and an F1-score of 0.99. While decision tree outperformed among the algorithms with medium requirements with an accuracy of 94.6% and an F1-score of 0.95. As for the category of algorithms with low resources, the logistic regression algorithm was the most efficient with an accuracy of 50.22 and an F1-score of 0.5.

Keywords: Blockchain, Anomaly Detection, Machine Learning, Resource Analysis, Classification.

1. مقدمة

يعد دمج اكتشاف الشذوذ في أنظمة سلاسل الكتل وسيلة واعدة لتعزيز الأمان والثقة. من خلال تحديد الأنماط والسلوكيات غير العادية، يمكن لهذه الخوارزميات المساعدة في اكتشاف الأنشطة الضارة ومنع الاحتيال والحفاظ على سلامة شبكة سلاسل الكتل .ومع ذلك، تأتي هذه الفوائد مع تحذير بالغ الأهمية في استهلاك الموارد. تتوزع بيئات سلاسل الكتل بطبيعتها وغالباً ما تكون مقيدة بالموارد. على عكس الأنظمة المركزية حيث قد تكون الطاقة الحسابية الوفيرة متاحة بسهولة، تعتمد سلاسل الكتل غالباً على عقد لامركزية بمستويات متفاوتة من قدرات المعالجة مما يفرض ضرورة لمعرفة متطلبات الموارد اللازمة لكل خوارزمية لمعرفة قدرة العقد في سلاسل الكتل على استخدامها، على الرغم من تعدد الدراسات التي تناولت كشف الشذوذ في سلاسل الكتل باستخدام خوارزميات التعلم الآلي، إلا أن معظمها ركز على تحسين دقة الكشف دون تحليل تأثير هذه الخوارزميات على استهلاك الموارد. يهدف هذا البحث إلى سد هذه الفجوة من خلال تقديم تحليل شامل لمتطلبات الموارد، مما يساعد في اختيار الخوارزمية الأكثر كفاءة وفقاً لقدرات العقد داخل شبكات سلاسل الكتل.

2. مشكلة البحث

مع اكتساب تقنية سلاسل الكتل اعتماداً واسع، أصبحت الحاجة إلى تدابير أمنية قوية أمراً بالغ الأهمية. يعالج اكتشاف الشذوذ باستخدام التعلم الالي في سلاسل الكتل هذه الحاجة من خلال تحديد الانحرافات عن السلوك الطبيعي الذي قد يشير إلى هجمات ضارة أو ثغرات أو أنشطة احتيالية.

تعتمد العديد من الدراسات على خوارزميات التعلم الآلي لكشف الشذوذ، لكنها غالباً ما تهمل تحليل متطلبات الموارد اللازمة لتشغيل هذه الخوارزميات في بيئات سلاسل الكتل، التي تتميز بكونها لامركزية ومحدودة الموارد. هذه الفجوة البحثية تثير تساؤلاً حول مدى قدرة العقد المختلفة في الشبكة على تشغيل خوارزميات كشف الشذوذ بكفاءة دون التأثير على الأداء العام.

3. هدف البحث

يهدف البحث بشكل رئيسي الى دراسة وتحليل متطلبات الموارد المطلوبة لاستخدام مصنفات التعلم الالي لكشف الشذوذ في سلاسل الكتل عن طريق تقسيم الخوارزميات الى ثلاثة أنواع: مصنفات ذو متطلبات عالية ومصنفات ذو متطلبات متوسطة ومصنفات ذو متطلبات ضعيفة مع مراعاة دقة كشف الشذوذ المترافقة مع استخدام الموارد.

4. سلاسل الكتل

سلاسل الكتل هي دفتر رقمي لامركزي يخزن السجلات بشكل آمن عبر شبكة الاجهزة بطريقة شفافة وغير قابلة للتغيير ومقاومة للتلاعب. تتكون من كتل من البيانات مرتبطة ببعضها البعض في سلسلة زمنية [3]، ويمكن لجميع عقد الشبكة الوصول الى سلسلة الكتل وتتبع جميع المعاملات التي يتم اجراؤها [30].

1.4 نواع سلاسل الكتل

لقد تطورت تقنية سلاسل الكتل بشكل كبير في السنوات القليلة الماضية وبناءً على سماتها المختلفة، يمكن تقسيمها إلى أنواع متعددة [3].

- **سلاسل الكتل العامة**

سلاسل الكتل العامة مفتوحة للعامة ويمكن لأي فرد أن يشارك في عملية صنع القرار من خلال أن يصبح عقدة، ولكن قد يستفيد المستخدمون أو لا يستفيدون من مشاركتهم في عملية صنع القرار.

- **سلاسل الكتل الخاصة**

هذه الأنواع من سلاسل الكتل ليست مفتوحة للعامة ومفتوحة فقط لمجموعة من الأشخاص أو المنظمات ويتم مشاركة السجل مع الأعضاء المشاركين فقط.

- **سلاسل الكتل شبه الخاصة**

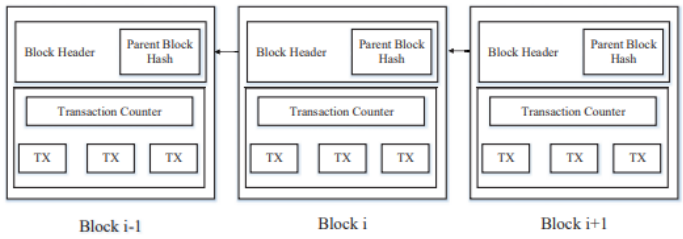
في سلسلة الكتل شبه الخاصة، يكون جزء من سلسلة الكتل خاصاً ويخضع لسيطرة مجموعة أو منظمات، والباقي مفتوح للجمهور ليتمكن أي شخص من المشاركة فيه.

- **دفتر الأستاذ المرخص**

في هذا النوع من سلسلة الكتل، يكون المشاركون معروفين وموثوقين بالفعل. في دفتر الأستاذ المرخص، يتم استخدام بروتوكول اتفاق للحفاظ على نسخة مشتركة من الحقيقة بدلاً من آلية الإجماع.

2.4 بنية سلاسل الكتل

نشأت فكرة سلسلة الكتل من ورقة بيضاء كتبها ناكاموتو ساتوشي في عام 2008 [17]. تمتلك سلسلة الكتل، والتي تسمى أيضاً دفتر الأستاذ الموزع، كتلاً متتالية، ترتبط ببعضها البعض من خلال قيمة التجزئة لرأس الكتلة السابقة. وبصرف النظر عن التجزئة، يتم أيضاً تضمين الطابع الزمني والرقم العشوائي وبيانات المعاملات في كتلة[1] كما هو موضح في الشكل 1.



شكل 1 بنية سلاسل الكتل المصدر [2]

تتكون سلاسل الكتل مما يلي [2]:

- **الكتلة:**

تتكون الكتلة من رأس الكتلة وجسم الكتلة. وعلى وجه الخصوص، يتضمن رأس الكتلة: (أ) إصدار الكتلة: يشير إلى مجموعة قواعد التحقق من صحة الكتلة التي يجب اتباعها. (ب) تجزئة جذر شجرة ميركل: قيمة تجزئة جميع المعاملات في الكتلة. (ج) الطابع الزمني. (د) nBits: عتبة الهدف لتجزئة الكتلة الصالحة. (هـ) Nonce: حقل مكون من 4 بايت، يبدأ عادةً بالرقم 0 ويزداد مع كل حساب تجزئة (و) تجزئة الكتلة الأصلية: قيمة تجزئة 256 بت تشير إلى الكتلة السابقة، يتكون جسم الكتلة من عداد المعاملات. يعتمد الحد الأقصى لعدد المعاملات التي يمكن أن تحتويها الكتلة على حجم الكتلة وحجم كل معاملة. تستخدم سلاسل الكتل آلية تشفير غير متماثلة للتحقق من صحة مصادقة المعاملات [13].

- **المناقلات:** تمثل المعاملة تفاعلًا بين الأطراف. في العملات المشفرة cryptocurrency، على سبيل المثال، تمثل المعاملة نقل العملة المشفرة بين مستخدمي شبكة سلاسل الكتل.

3.4 مزايا تقنية البلوك تشين

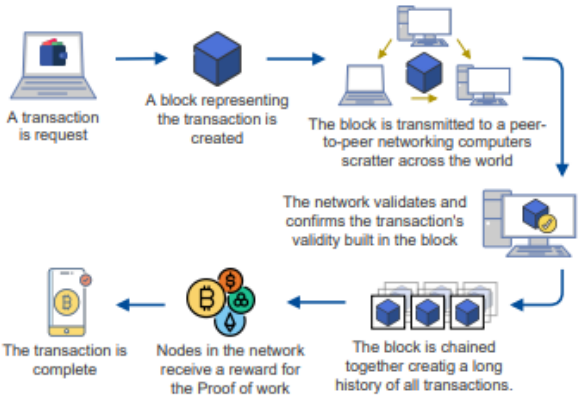
أبرز مزايا تقنية سلاسل الكتل وفق :[3]

- واحدة من أكبر مزايا تقنية البلوك تشين هي التوزيع الذي يسمح بمشاركة قاعدة البيانات دون وجود هيئة أو كيان مركزي. نظراً للطبيعة اللامركزية لتقنية البلوك تشين، يكاد يكون من المستحيل تعديل البيانات مقارنة بقاعدة البيانات التقليدية.
- يتم تمكين المستخدمين من التحكم في معلوماتهم ومعاملاتهم.
- توفر تقنية البلوك تشين الشفافية والثبات للمعاملات حيث لا يمكن تغيير أو حذف جميع المعاملات.

4.4 الية عمل سلاسل الكتل

تبدأ العملية بطلب المعاملة ومن ثم يتم إنشاء كتلة تمثل المعاملة ثم يتم نقل الكتلة إلى العقد nodes المتصلة بشبكة نظير إلى نظير وبعدا تتحقق الشبكة من صحة المعاملة المضمنة في الكتلة وتؤكدها

لتكتمل المعاملة ثم تتلقى العقد في الشبكة مكافأة لإثبات العمل يتم ربط الكتلة معًا لإنشاء تاريخ طويل لجميع المعاملات. يوضح الشكل 2 معاملة تتم معالجتها بواسطة تقنية سلاسل الكتل.



شكل 2 الية عمل سلاسل الكتل المصدر [1]

5. التعلم الالي

هو فرع من فروع الذكاء الاصطناعي (AI) وعلوم الكمبيوتر الذي يركز على استخدام البيانات والخوارزميات لتقليد الطريقة التي يتعلم بها البشر، وتحسين دقتها تدريجياً. يعد التعلم الآلي مكوناً مهماً في المجال المتنامي لعلوم البيانات. من خلال استخدام الأساليب الإحصائية، يتم تدريب الخوارزميات على إجراء تصنيفات أو تنبؤات في مشاريع التنقيب عن البيانات. تؤدي هذه الأفكار بعد ذلك إلى اتخاذ القرار داخل التطبيقات والشركات، مما يؤثر بشكل مثالي على مقاييس النمو الرئيسية [12].

تمر عملية التعلم الآلي في عدد من الخطوات وهي: استخراج البيانات – تحليل البيانات – إعداد البيانات – تدريب النموذج – تقييم النموذج [14].

15. أنواع التعلم الآلي

بناءً على أساليب وطريقة التعلم، ينقسم التعلم الآلي إلى أربعة أنواع أساسية، وهي[13]:

- **التعلم الآلي الخاضع للإشراف**

كما يوحي اسمه، يعتمد التعلم الآلي الخاضع للإشراف على الإشراف. هذا يعني أنه في أسلوب التعلم الخاضع للإشراف، يتم تدريب الآلات باستخدام مجموعة البيانات "المعنونة" (labels) ، ومن ثم بناءً على التدريب، تتنبأ الآلة بالخرج الذي يكون إما تنبؤ أو تصنيف (classification, regression)، تم في هذا البحث الاعتماد على التعلم الخاضع للإشراف وتحديداً التصنيف وهو ماسيتم التركيز عليه.

- **التعلم بدون إشراف**

يختلف التعلم غير الخاضع للإشراف عن أسلوب التعلم الخاضع للإشراف؛ كما يوحي اسمها، ليس هناك حاجة للإشراف. وهذا يعني في التعلم الآلي غير الخاضع للإشراف، أن الآلة يتم تدريبها باستخدام مجموعة البيانات غير المعنونة.

- **التعلم شبه الخاضع للإشراف**

التعلم شبه الخاضع للإشراف هو نوع من خوارزمية التعلم الآلي التي تقع بين التعلم الآلي الخاضع للإشراف والتعلم غير الخاضع للإشراف. فهو يمثل الأرضية الوسيطة بين خوارزميات التعلم الخاضع للإشراف (مع بيانات التدريب المعنونة) والتعلم غير الخاضع للإشراف (بدون بيانات تدريب معنونة) ويستخدم مزيجاً من مجموعات البيانات المصنفة وغير المصنفة خلال فترة التدريب.

6. الشذوذ

يعرف الشذوذ بالشكل العام بأنه أنماط في البيانات لا تتوافق مع مفهوم محدد جيداً للسلوك الطبيعي، ويمكن تعريف أنظمة كشف الشذوذ على أنها أجهزة أو برامج تقوم بمراقبة البيانات المتعلقة بمجال معين لتحديد الحالات الشاذة والمختلفة عن السلوك الطبيعي [31].

1.6 تحديات كشف الشذوذ

على مستوى مجرد، يتم تعريف الشذوذ على أنه نمط لا يتوافق مع السلوك الطبيعي المتوقع. وبالتالي، فإن أسلوب اكتشاف الشذوذ المباشر هو تحديد منطقة تمثل السلوك الطبيعي وإعلان أي ملاحظة في البيانات لا تنتمي إلى هذه المنطقة الطبيعية على أنها شذوذ. لكن هناك عدة عوامل تجعل هذا النهج البسيط ظاهرياً صعباً للغاية [16]:

- من الصعب للغاية تحديد منطقة طبيعية تشمل كل سلوك طبيعي محتمل. بالإضافة إلى ذلك، غالباً ما تكون الحدود بين السلوك الطبيعي والشاذ غير دقيقة.
- عندما تكون الحالات الشاذة نتيجة لأفعال خبيثة، غالباً ما يتكيف الأعداء الخبثاء لجعل الملاحظات الشاذة تبدو طبيعية، مما يجعل مهمة تعريف السلوك الطبيعي أكثر صعوبة.
- عادة ما يكون توافر البيانات المصنفة للتدريب / التحقق من صحة النماذج المستخدمة بواسطة تقنيات اكتشاف العيوب مشكلة رئيسية.

نظراً للتحديات المذكورة أعلاه، فإن مشكلة اكتشاف الشذوذ، في شكلها الأكثر عمومية، ليس من السهل حلها.

2.6 الشذوذ في سلاسل الكتل

يشير الشذوذ إلى أي انحراف أو مخالفة أو قيمة شاذة عن نمط أو سلوك متوقع أو طبيعي. في سياق سلاسل الكتل، يمكن أن يشير الشذوذ إلى أنشطة غير عادية أو سلوك مريب أو تهديدات أمنية محتملة داخل شبكة سلاسل الكتل. يتضمن اكتشاف الشذوذ في سلاسل الكتل عملية تحديد مثل هذه الشذوذ. قد يكون اكتشاف الشذوذ في بيئة سلاسل الكتل أمراً صعباً بسبب عدة أسباب [17]: 1. الطبيعة الموزعة وغير القابلة للتغيير: سلاسل الكتل عبارة عن دفتر حسابات لامركزي وموزع، حيث يحتفظ كل مشارك بنسخة من سلاسل الكتل بالكامل. بمجرد تسجيل معاملة وإضافتها إلى كتلة، تصبح غير قابلة للتغيير عملياً. وهذا يعني أنه لا يمكن إزالة أي معاملة شاذة أو احتيالية

بمجرد إضافتها إلى سلاسل الكتل بسهولة. يجب أن تأخذ تقنيات اكتشاف الشذوذ في الاعتبار هذه الخاصية الفريدة لسلسلة الكتل أثناء تحديد الشذوذ والتخفيف منه. 2. كمية هائلة من البيانات: تولد شبكات سلسلة الكتل كمية هائلة من البيانات بسبب التسجيل المستمر للمعاملات. يمكن أن يكون تحليل ومعالجة هذا الحجم الكبير من البيانات في الوقت الفعلي مكثفاً من الناحية الحسابية. يجب أن تكون طرق اكتشاف الشذوذ قابلة للتطوير وفعالة بما يكفي للتعامل مع الإنتاجية العالية لمعاملات سلسلة الكتل. 3. أنماط المعاملات المعقدة: يمكن أن تظهر معاملات سلسلة الكتل أنماطاً وتبعيات معقدة. يمكن أن تظهر الشذوذ في أشكال مختلفة، مثل أحجام المعاملات غير الطبيعية، وأنواع المعاملات غير العادية، والتغيرات المفاجئة في سلوك الشبكة، أو الأنشطة الضارة. يجب أن تكون خوارزميات اكتشاف الشذوذ قادرة على التقاط وفهم أنماط المعاملات المعقدة هذه للكشف عن الشذوذ بشكل فعال.

1.2.6 أنواع الشذوذ في سلاسل الكتل

يمكن أن تحدث عدة أنواع من الشذوذ في سلاسل الكتل، والتي يمكن أن تكون مؤشراً على نشاط احتيالي أو ضار. فيما يلي بعض الأنواع الشائعة من الشذوذ في سلاسل الكتل [17] : 1. هجمات الإنفاق المزدوج: يحدث هجوم الإنفاق المزدوج عندما يحاول الفرد إنفاق نفس العملة المشفرة مرتين. يمكن القيام بذلك عن طريق إنشاء معاملة وهمية، والتي يتم بثها بعد ذلك إلى الشبكة. إذا تم قبول المعاملة المزيفة وإضافتها إلى سلاسل الكتل قبل المعاملة المشروعة، يمكن للفرد أن ينفق نفس العملة المشفرة مرتين فعلياً. 2. ازدحام الشبكة: يحدث ازدحام الشبكة عندما يتجاوز عدد المعاملات التي يتم بثها إلى الشبكة قدرتها على المعالجة. يمكن أن يؤدي هذا إلى تأخيرات في معالجة المعاملات وزيادة رسوم المعاملات وربما رفض المعاملات الصالحة. 3. المعاملات الاحتيالية: تحدث المعاملات الاحتيالية عندما يحاول الفرد التلاعب بالبلوك تشين عن طريق إنشاء معاملات وهمية أو تعديل المعاملات الموجودة. يمكن القيام بذلك في محاولة لسرقة العملة المشفرة أو الحصول على وصول غير مصرح به إلى الشبكة. 4. الأخطاء في العقود الذكية: العقود الذكية هي عقود

ذاتية التنفيذ تعمل على سلاسل الكتل .إذا كانت هناك أخطاء في كود العقد الذكي، فقد يؤدي هذا إلى سلوك غير متوقع، والذي يمكن استغلاله من قبل الجهات الخبيثة. 5. هجمات :Sybil تحدث هجمات Sybil عندما ينشئ فرد هويات مزيفة متعددة، أو "Sybils"، على الشبكة. يمكن القيام بذلك في محاولة للتلاعب بآلية الإجماع والسيطرة على الشبكة.

7. الدراسة المرجعية

تتضمن ادبيات الدراسة مجموعة من الخوارزميات لمعالجة الشذوذ في مجموعات البيانات ولكون مجموعات بيانات سلاسل الكتل لها وضع خاص فقد تنوعت هذه الاساليب فمنها التعلم الآلي والتعلم العميق. سيتم الاعتماد في هذا البحث على ذكر الدراسات السابقة على طريقة تصنيفها حسب نوع خوارزمية الكشف عن الشذوذ في سلاسل الكتل حيث يفيد هذا التصنيف في النقاط التالية:

1. التعرف على التقنيات المستخدمة حالياً لكشف الشذوذ في سلاسل الكتل.
2. التعرف على الطرائق الأفضل من خلال عمليات المقارنة بين طرائق كشف الشذوذ.
3. تحديد أسباب اختيار خوارزمية عن أخرى في اكتشاف الشذوذ الشبكي.

حيث ركزت الدراسات على استخدام طرائق التعلم الآلي بإشراف أكثر من التعلم الآلي دون اشراف نظراً لاعتبار مشكلة الشذوذ مشكلة تصنيف حيث تصنف البيانات في سلاسل الكتل على أنها إما بيانات طبيعية أو بيانات غير طبيعية. بالمقابل تناولت العديد من الدراسات استخدام التعلم العميق نظراً لفعالية التعلم العميق والقدرة على اكتشاف أنماط شذوذ جديدة وقلة تأثرها بمشكلة عدم توازن البيانات.

فكانت خوارزمية الغابة العشوائية وشجرة القرار وخوارزمية أقرب جار وLogistic regressionn هي الأكثر استخداماً مقارنة بغيرها.

1.7 طرائق التعلم بإشراف

تبحث [22] الدراسة في تطبيق نماذج التعلم الآلي للكشف عن الشذوذ وتحليل الاحتيال في معاملات سلاسل الكتل داخل Open Metaverse، وسط التعقيد المتزايد للمعاملات الرقمية. باستخدام مجموعة بيانات مكونة من 78600 معاملة تعكس مجموعة واسعة من سلوكيات المستخدم وأنواع المعاملات، تم تقييم فعالية العديد من النماذج التنبؤية، بما في ذلك RandomForest و LinearRegression و SVR و DecisionTree و KNeighbors و GradientBoosting و AdaBoost و Bagging و XGB و LightGBM، بناءً على متوسط خطأ التربيع المتبادل للتحقق MSE كشف التحليل أن أساليب المجموعة، وخاصة RandomForest و Bagging، أظهرت أداءً متفوقًا مع متوسط خطأ تربيعي للتحقق المتبادل −0.00445 و−0.00415 على التوالي، مما يسلط الضوء على قوتها في مجموعة بيانات المعاملات المعقدة. وعلى النقيض من ذلك، كان LinearRegression و SVR من بين الأقل فعالية، حيث بلغ متوسط أخطاء التباين المتوسط − 224.67 و−468.57، مما يشير إلى عدم التوافق المحتمل مع خصائص مجموعة البيانات. ويؤكد هذا البحث على أهمية اختيار استراتيجيات التعلم الآلي المناسبة في سياق معاملات سلاسل الكتل داخل Open Metaverse، مما يبرز الحاجة إلى مناهج متقدمة وقابلة للتكيف.

يقدم البحث [23] نهجاً هندسياً آلياً للميزات لمعاملات سلاسل الكتل .يتضمن ذلك عملية استخراج الميزات، حيث تعرف بأنها عملية إنشاء مجموعة ميزات باستخدام خصائص البيانات التي تعزز أداء خوارزميات تعلم الآلة [32]. حصلت هذه الميزات على دقة اختبار عالية بشكل ملحوظ لتصنيف معاملات البيتكوين الشاذة (88.0٪) ومعاملات Ethereum EOA (97.86٪ . تم تقييم الميزات المصممة باستخدام نماذج التعلم الآلي المختلفة LR, RF, k-NN, DT , NB , XG ، والتي أظهرت أداء تصنيف عالياً في التجارب حيث كانت RF الأفضل . تم تحليل أهمية الميزة باستخدام تقنية .ShAP عكست درجة أهمية الميزة أن الميزات المصممة هي في الواقع الأكثر أهمية لتصنيف معاملات سلاسل الكتل.

تم اقتراح نموذجاً في [24] للكشف عن الاحتيال يعتمد على التعلم الآلي في سلاسل الكتل. تم استخدام خوارزميتان للتعلم الآلي – XGboost والغابة العشوائية تستخدمان لتصنيف المعاملات. تدرب تقنيات التعلم الآلي مجموعة البيانات بناءً على أنماط المعاملات الاحتيالية والمتكاملة وتتنبأ بالمعاملات الواردة الجديدة حيث وصلت دقة النماذج الى 90%.

تستخدم الدراسة [25] تقنيات طريقة التصفية مثل المعلومات المتبادلة وتحليل التباين وإزالة الميزة المتكررة لتحديد المجموعة المثالية من الميزات تقوم الدراسة بفحص وتصنيف أفضل 10 مجموعات من الميزات باستخدام مصنف الغابة العشوائية لأهمية الميزةRF، بناءً على مجموعة البيانات التي تم إنتاجها بواسطة أفضل نهج للتصفية (مما يعطي دقة أعلى). بعد ذلك، يتم استخدام منهجية المجموعة لإنشاء النموذج النهائي، باستخدام مجموعة البيانات النهائية المكونة من 10 ميزات. الغرض من هذا النهج هو تعزيز مستوى اكتشاف الشذوذ في شبكة سلاسل الكتل .لتحديد فعالية النموذج المقترح، يتم إجراء التجارب ومقارنته بالمصنفات الفردية XGBوشجرة القرار والانحدار اللوجستي والغابة العشوائية وأقرب جار تكشف نتائج الدراسة أن نهج التصويت الجماعي يحقق معدل دقة 96.78٪، متجاوزاً دقة نماذج التصنيف الفردية التي تستخدم الميزات المثلى. بالإضافة إلى ذلك، تشير نتائج الدراسة إلى أن اختيار الميزات وكميتها يؤثران بشكل كبير على ناتج النموذج.

تم في الدراسة [26] استخدام تقنيات التعلم الآلي لتقديم نهج يمكنه اكتشاف الحسابات الاحتيالية على .Ethereum تم استخدام خوارزميات K-Nearest Neighbor وRandom Forest وXGBoost على مجموعة بيانات مجمعة من 4681 حالة إلى جانب 2179 حسابًا احتياليًا مرتبطًا و2502 حسابًا عاديًا. حققت تقنيات XGBoost وRF وKNN متوسط دقة 96.80٪ و94.8٪ و8٪ و87.85٪ ومتوسط 0.995 AUC و0.99 و0.93 على التوالي.

يركز الحل المقترح في [27]على استخدام نهج ديناميكي حيث يتم استخدام السلوك التشغيلي الطبيعي لسلاسل كتل Ethereum لتدريب خوارزميات ML وسيتم وضع علامة على أي انحراف على أنه

شذوذ وسيتم اكتشافه بواسطة النظام. تم استخدام أربع خوارزميات ML بما في ذلك K-Nearest Neighbors (KNN)و Gaussian Naive Bayes (GaussianNB) و Random Forestو Stochastic Gradient Descent (SDG) لتدريب والتحقق من دقة الحل المقترح. أظهرت النتائج التجريبية أن خوارزمية الغابة العشوائية قدمت أفضل دقة بنسبة 99.84٪ مقارنة بخوارزميات التعلم الآلي الأخرى.

2.7 طرائق التعلم دون اشراف

قام الباحثون في [19] باستخدام خوارزمية Isolation Forest للكشف عن الشذوذ داخل مجموعة بيانات معاملات سلاسل الكتل التي تضمنت ميزات مختلفة مثل مبالغ المعاملات ودرجات المخاطرة ومدة الجلسة. من إجمالي 78600 معاملة تم تحليلها، حددت الخوارزمية 3930 معاملة على أنها شذوذ، تمثل حوالي 5٪ من مجموعة البيانات. كشف التحليل أن أكثر أنواع المعاملات شيوعاً المرتبطة بالشذوذ كانت "البيع" و "الاحتيال"، مما يشير إلى ميل أعلى لهذه الفئات لإظهار سلوك غير منتظم وتشير الأنماط الجغرافية والسلوكية التي أبرزتها هذه الدراسة إلى أن التركيز على المخاطر وأنواع المعاملات الخاصة بالمنطقة يمكن أن يعزز الأمن العام لشبكات سلاسل الكتل . ومن خلال تحديد المناطق وأنواع المعاملات الأكثر عرضة للشذوذ، يمكن لأصحاب المصلحة تنفيذ استراتيجيات مراقبة وتدخل أكثر فعالية

الغرض الرئيسي من هذه الدراسة في [20] هو تقديم طريقة جديدة لاكتشاف الشذوذ في Bitcoin بكفاءة أكثر ملاءمة. في هذه الدراسة، تم استخدام نهج الشذوذ الجماعي. بدلاً من اكتشاف شذوذ العناوين والمحافظ الفردية، تم فحص شذوذ المستخدمين. بالإضافة إلى استخدام طريقة اكتشاف الشذوذ الجماعي، تم استخدام خوارزمية Trimmed_Kmeans للتجميع. تظهر نتائج هذه الدراسة أن الشذوذ أكثر وضوحًا بين المستخدمين الذين لديهم محافظ متعددة. كشفت الطريقة المقترحة عن 14 مستخدمًا ارتكبوا عمليات احتيال، بما في ذلك 26 عنوانًا في 9 حالات، في حين كشفت

الأعمال السابقة عن 7 عناوين كحد أقصى في 5 حالات احتيال. بالإضافة إلى تقليل تكلفة المعالجة لاستخراج الميزات، فإن النهج المقترح يكشف عن المزيد من المستخدمين غير الطبيعيين والسلوكيات الشاذة.

يناقش البحث [21] تحديد الشذوذ مع الإشارة بشكل خاص إلى شبكة معاملات البيتكوين .في هذه الحالة، يعد سلوك الشذوذ وكيلًا للنشاط المقلق، وبالتالي فإن الهدف هو العثور على الشذوذ في مجموعة البيانات من حيث نسبتها المئوية. لتحقيق ذلك، تم استخدام طريقة اختيار الميزة وهي اختيار الميزة الأمامية المتسلسلة جنباً إلى جنب مع ثلاث تقنيات ML، وتجميع kmeans، وغابة العزل، وآلة الدعم المتجه (SVM) وتم الحصول على أعلى دقة بنسبة 98.2٪ في SVM مقارنة بجميع الطرق الأخرى

بعدما تم عرض التوجهات المستخدمة لكشف الشذوذ في سلاسل الكتل باستخدام التعلم الآلي بنوعيه التعلم بإشراف وتعلم بدون إشراف. نلاحظ تفوق خوارزميات التعلم الآلي لاكتشاف الشذوذ في سلاسل الكتل وهي الغابة العشوائية وشجرة القرار وخوارزمية أقرب جار والانحدار اللوجستي على باقي خوارزميات التعلم الآلي وكثرة استخدامهم في هذا المجال ولذلك سيتم اختيارهم في هذا البحث كمايتم استخدام خوارزمية الانتخاب (الجميع بين أفضل ثلاثة مصنفات بينهم).

يوضح الجدول 1 مقارنة الدراسات المرجعية التي استخدمت التعلم بإشراف لكشف الشذوذ في سلاسل الكتل، حيث لم تتم دراسة متطلبات موارد خوارزميات التعلم الآلي لاكتشاف الشذوذ في سلاسل الكتل من قبل الأبحاث السابقة لذلك سيتم الاكتفاء بعرض معايير أداء الخوارزميات في كشف الشذوذ دون معايير قياس موارد أداء الخوارزميات

جدول 1 مقارنة الدراسات المرجعية

الدراسة	الخوارزميات المستخدمة	أبرز النتائج
[22]	RandomForest و LinearRegression و SVR و DecisionTree و KNeighbors و GradientBoosting و AdaBoost و Bagging و XGB و LightGBM	RandomForest و Bagging، أظهرت أداءً متفوقًا مع متوسط خطأ تربيعي للتحقق المتبادل – 0.00445 و−0.00415 على التوالي، مما يسلط الضوء على قوتها في مجموعة بيانات المعاملات المعقدة
[23]	LR, RF, k-NN, DT , NB , XG	RF الأفضل لتصنيف معاملات البيتكوين الشاذة (88.0٪) ومعاملات Ethereum EOA (97.86٪) .
[24]	XGboost والغابة العشوائية	وصلت دقة النماذج الى 90%.
[25]	XGB شجرة القرار والانحدار اللوجستي والغابة العشوائية وأقرب جار	تكشف نتائج الدراسة أن نهج التصويت الجماعي يحقق معدل دقة 96.78٪
[26]	K-Nearest Neighbor و Random Forest و XGBoost	حققت تقنيات XGBoost و RF و KNN متوسط دقة 96.80٪ و 94.8٪ و 8٪ و 87.85٪
[27]	K-Nearest Neighbors (KNN) و Gaussian Naive Bayes (GaussianNB)و Random Forest و Stochastic Gradient Descent (SDG)	أظهرت النتائج التجريبية أن خوارزمية الغابة العشوائية قدمت أفضل دقة بنسبة 99.84٪
الدراسة الحالية	شجرة القرار، الغابة العشوائية، أقرب جار، الانحدار اللوجستي، ومصنف الانتخاب	تقييم أداء الخوارزميات من حيث استهلاك الذاكرة، نسبة استخدام المعالج، ومتطلبات التخزين، إضافةً إلى دقتها في كشف الشذوذ، وتصنيف استهلاك الموارد لهذه الخوارزميات لثلاثة تصنيفات. الغابة العشوائية كانت الأفضل بين الخوارزميات ذات المتطلبات العالية، محققة دقة 99% و F1-score قدره 0.99. بينما تفوقت شجرة القرار بين الخوارزميات ذات المتطلبات المتوسطة بدقة 94.6% و F1-score بلغ 0.95. أما في فئة الخوارزميات

		ذات الموارد المنخفضة، فقد كانت خوارزمية الانحدار اللوجستي الأكثر كفاءة بدقة 50.22 و f1score 0.5

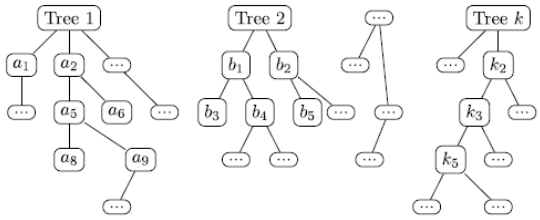
8. الخوارزميات المستخدمة

1.8 شجرة القرار

تعد خوارزمية شجرة القرار خوارزمية مستخدمة على نطاق واسع للتصنيف، والتي تستخدم قيم السمات لتقسيم مساحة القرار إلى مساحات فرعية أصغر بطريقة تكرارية، يمكن تمثيل عمليات اتخاذ القرار مثل كشف الشذوذ بيانياً كشجرة [5].

2.8 الغابة العشوائية

هي مجموعة من أشجار القرار التي تم إنشاؤها من مجموعة البيانات يتم تجميع كل شجرة على حدة لإنتاج تنبؤ فريد بالإجماع على كشف الشذوذ. يتم تمثيل الفكرة الأساسية للغابات العشوائية بشكل تخطيطي في الشكل (3):



شكل3 الفكرة الأساسية للغابة العشوائية

3.8 خوارزمية اقرب جار

تجد الخوارزمية أكثر الملاحظات تشابهاً مع تلك التي يجب أن تتنبأ بها والتي تستمد منها حدساً جيداً للإجابة المحتملة عن طريق حساب متوسط القيم المجاورة، أو عن طريق اختيار فئة الإجابة الأكثر شيوعاً فيما بينها. يمكن لـ KNN التعامل بسهولة مع مئات التسميات [9]. عادة، يعمل

KNN على معرفة جيران الملاحظة بعد استخدام مقياس المسافة مثل الإقليدية (الخيار الأكثر شيوعاً)[8] . على سبيل المثال في حال كانت نقطة بيانات معينة يجب التنبؤ بها بأنها شاذة او طبيعية فيتم النظر الى أقرب جيرانها لتصنيف هذه النقطة.

4.8 الانحدار اللوجستي

تقدر الانحدارات اللوجستية احتمالية وقوع حدث ما، مثل التصويت أو عدم التصويت، استنادًا إلى مجموعة بيانات معينة من المتغيرات المستقلة. غالباً ما يستخدم هذا النوع من النماذج الإحصائية (المعروف أيضاً باسم نموذج اللوغاريتم) للتصنيف والتحليلات التنبؤية. نظراً لأن النتيجة هي احتمالية، فإن المتغير التابع محصور بين 0 و1. في الانحدار اللوجستي [29].

5.8 مصنف الانتخاب voting

تم دمج المصنفات الثلاثة الأفضل وهي KNN,RF,DT للحصول على مصنف انتخابي بين هذه الخوارزميات بحيث يتم تصنيف البيانات الشاذة والطبيعة بناء على غالبية الأصوات بدلاً من الاعتماد على خوارزمية واحدة.

9. معايير الأداء

تم تقسيم معايير الأداء الى معايير أداء الخوارزميات ومعايير قياس موارد أداء الخوارزميات وذلك في مرحلة اختبار الخوارزميات.

1.9 معايير قياس الموارد

تم اعتماد على الذاكرة العشوائية RAM و نسبة استخدام المعالج CPU ومساحة التخزين اللازم لتشغيل مصنف التعلم الآلي وذلك بالاعتماد على الأدوات المستخدمة في البحث.

2.9 معايير أداء الخوارزميات

تم الاعتماد على المعايير التالية نظراً لكون المشكلة هي مشكلة تصنيف البيانات على انها طبيعية او شاذة.

- **دقة التصنيف accuracy**

دقة التصنيف هي ما نعنيه عادةً عندما نستخدم مصطلح الدقة. إنها نسبة عدد التنبؤات الصحيحة إلى العدد الإجمالي لعينات الإدخال [10]. وتعطى الدقة بالمعادلة 1:

$$\text{Accuracy}= \frac{\text{number of correct predictions}}{\text{total number of predictions}} \ldots(1)$$

- **Confusion Matrix**

مصفوفة الارتباك كما يوحي الاسم تعطي مصفوفة كإخراج وتصف الأداء الكامل للنموذج. يوضح الشكل 4 مصفوفة الارتباك:

		Predicted	
		Negative	**Positive**
Actual	**Negative**	True Negative	False Positive
	Positive	False Negative	True Positive

شكل 4 مصفوفة الارتباك المصدر [11]

يمكن حساب دقة المصفوفة بأخذ متوسط القيم الموجودة عبر "القطر الرئيسي" كما هو موضح بالمعادلة 2:

$$\text{Accuracy} = \frac{\text{TruePositive+TrueNegative}}{\text{TotalSample}} \ldots(2)$$

- **الدقة Precision**

هي عدد النتائج الإيجابية الصحيحة مقسوماً على عدد النتائج الإيجابية التي تنبأ بها المصنف كما هو موضح في المعادلة 3، بعبارات أبسط، الدقة هي النسبة بين الإيجابيات الحقيقية وجميع الإيجابيات.

$$\text{Precision} = \frac{\text{TruePositive}}{\text{TotalPredicted Positive}} \quad \ldots(3)$$

- **Recall الاسترجاع**

هو عدد النتائج الإيجابية الصحيحة مقسوماً على عدد جميع العينات ذات الصلة (جميع العينات التي كان ينبغي تحديدها على أنها إيجابية) [60]. الاسترجاع هو مقياس النموذج الذي يحدد الإيجابيات الحقيقية بشكل صحيح. رياضياً موضح بالمعادلة 4:

$$\text{Recall}=\frac{\text{TruePositive}}{\text{TruePositive+FasleNegative}} \quad \ldots(4)$$

- **F1 Score**

F1 Score هو المتوسط التوافقي بين الدقة والاسترجاع. نطاق نقاط F1 هو [0، 1]. يخبر بمدى دقة المصنف(عدد الحالات التي يصنفها بشكل صحيح). رياضياً f1score موضح بالمعادلة 5.

$$\text{F1score}= \frac{2*\text{Precision}*\text{Recall}}{\text{Precision+Recall}} \quad \ldots(5)$$

10. الاعداد التجريبي

يجدر الذكر بأنه تم استخدام جهاز حاسوب محمول ذو المواصفات التالية كما يوضح الجدول 2.

جدول 2 مواصفات الحاسوب المستخدم

المواصفة	القيمة
تردد المعالج	2.5
الذاكرة العشوائية RAM	8
عدد الأنوية	3
جيل الحاسوب	7

11. التطبيق العملي

تم استخدام لغة البرمجة بايثون و Juypter كمحرر للتعليمات البرمجية وذلك من اجل تحليل بيانات سلاسل الكتل وتقييم استهلاك الموارد لخوارزميات التعلم الآلي في كشف الشذوذ في شبكات سلاسل الكتل واقتراح تصنيف استهلاك الموارد لكل خوارزمية بحيث يتم تصنيف الخوارزمية الى تصنيف مرتفع لاستهلاك الموارد او تصنيف متوسط لاستهلاك الموارد أو تصنيف منخفض لاستهلاك الموارد بناء على اجمالي النقاط التي حصلت عليها في استهلاك المعالج والذاكرة والتخزين لكشف الشذوذ.

1.11 مجموعة البيانات المستخدمة

تم استخدام مجموعة بيانات Metaverse Financial Transactions Dataset توفر مجموعة البيانات هذه المعاملات القائمة على تقنية سلاسل الكتل، بهدف توفير مجموعة غنية ومتنوعة وواقعية من البيانات لتطوير واختبار نماذج الكشف عن الشذوذ، وتحليل الاحتيال [18].

تم تصميم مجموعة البيانات هذه لمجموعة واسعة من الاستخدامات، بما في ذلك على سبيل المثال لا الحصر:

- الكشف عن الشذوذ وتحليل الاحتيال في معاملات سلاسل الكتل.
- البحث في إدارة الأصول الرقمية الآمنة والشفافة.
- تطوير واختبار الخوارزميات لتقييم المخاطر والتحقق من المستخدم.

تتضمن مجموعة البيانات 78600 سجل، يمثل كل منها معاملة بالميزات التالية الموضحة بالجدول3.

جدول 3 ميزات مجموعة البيانات

الميزة	الشرح
Timestamp	تاريخ ووقت المعاملة.
Hour of Day	جزء الساعة من الطابع الزمني للمعاملة.
Sending Address	عنوان المرسل.
Receiving Address	عنوان المستقبل.
Amount	مبلغ المعاملة.
Transaction Type	تصنيف المعاملة (على سبيل المثال، التحويل، البيع، الشراء، الاحتيال، التصيد الاحتيالي).
Location Region	المنطقة الجغرافية المحاكاة للمعاملة.
PrefixIP	بادئة عنوان IP المحاكاة للمعاملة.
Login Frequency	تردد جلسات تسجيل الدخول للمستخدم، ويختلف حسب الفئة العمرية.
Session Duration	مدة جلسات النشاط بالدقائق.
Purchase Pattern	النمط السلوكي للمشتريات (على سبيل المثال، مركّزة، عشوائية، عالية القيمة).
Age Group	تصنيف المستخدمين إلى جدد، وراسخين، وقدامى بناءً على تاريخ نشاطهم.
Risk Score	درجة المخاطرة المحسوبة بناءً على خصائص المعاملة وسلوك المستخدم.
Anomaly	تقييم مستوى المخاطرة (على سبيل المثال، مخاطرة عالية، مخاطرة معتدلة، مخاطرة منخفضة).

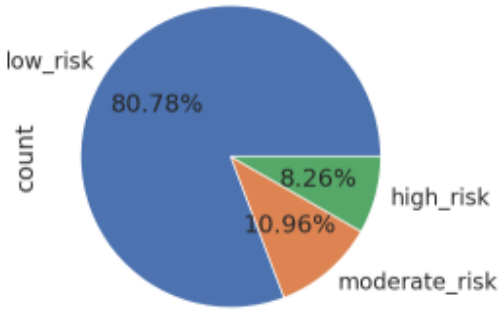
2.11 تحليل البيانات ومعالجتها

في البداية تم قراءة مجموعة البيانات كما هو موضح في الشكل 5.

timestamp	hour_of_day	sending_address	receiving_address	amount
2022-04-11 12:47:27	12	0x9d32d0bf2c00f41ce7ca01b66e174cc4dcb0c1da	0x39f82e1c09bc6d7baccc1e79e5621ff812f50572	796.949206
2022-06-14 19:12:46	19	0xd6e251c23cbf52dbd4721079147873e655d8096f	0x51e8fbe24f124e0e30a614e14401b9bbfed5384c	0.010000
2022-01-18 16:26:59	16	0x2e0925b922fed01f6a85d213aa2718f54b8ca305	0x52c7911879f783d590af45bda0c0ef2b8536706f	778.197390
2022-06-15 09:20:04	9	0x93efefc25fcaf31d7695f28018d7a11ece55457f	0x8ac3b7bd531b3a833032f07d4e47c7af6ea7baca	300.838358
2022-02-18 14:35:30	14	0xad3b8de45d63f5cce28aef9a82cf30c397c6ceb9	0x6fdc047c2391615b3facd79b4588c7e9106e49f2	775.569344

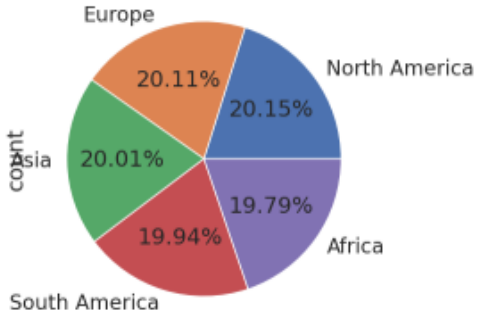
شكل 5 عرض اول خمسة اسطر من مجموعة البيانات

ليتم بعدها التأكد من خلو البيانات من القيم الفارغة او المكررة، يوضح الشكل 6 النسبة المئوية لتوزيع المعاملات ذات الخطورة العالية والمنخفضة، تشكل المعاملات ذات الخطورة المنخفضة low risk نسبة 80% من بين اجمالي المعاملات في مجموعة البيانات.



شكل 6 النسبة المئوية لتوزيع المعاملات ذات الخطورة العالية والمنخفضة

يوضح الشكل 7 مصدر المعاملات بين القارات من الواضح ان التوزيع متقارب جدا (موزع بالتساوي) بالتالي لا يرتبط مصدر المعاملات بنسبة خطورة المعاملة.

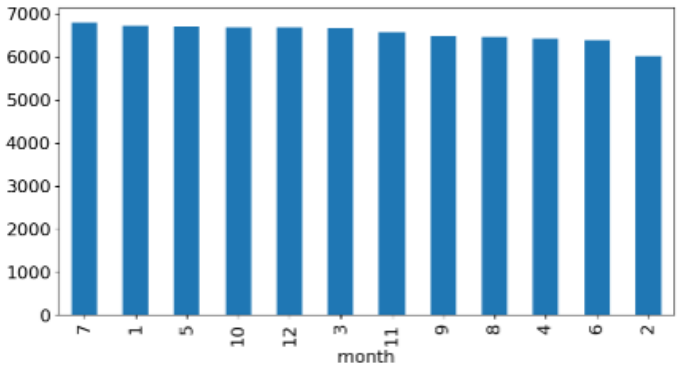


شكل 7 مصدر المعاملات

يوضح الشكل 8 نوع المعاملات في مجموعة البيانات من الواضح ان المعاملات المرتبطة بالبيع او الشراء او نقل الأموال هي الأكثر.

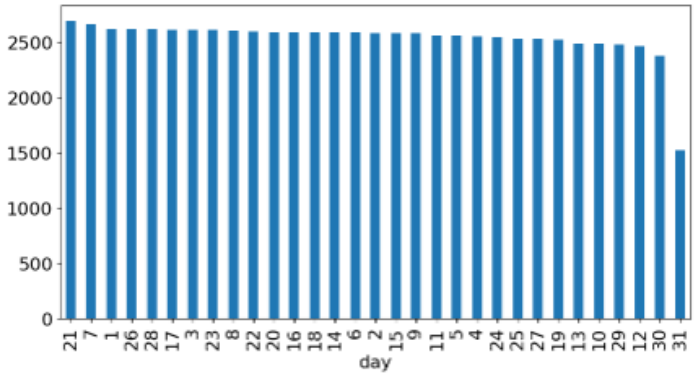
شكل 8 نوع المعاملة

من ثم تم إنشاء مجموعة جديدة من الميزات وهي السنة والشهر واليوم والدقيقة والساعة والثانية من العمود time stamp ليتم اضافتها الى مجموعة البيانات. يوضح الشكل 9 توزع المعاملات وفق الشهر، كافة الأشهر يتم فيها معاملات بنسب متقاربة.



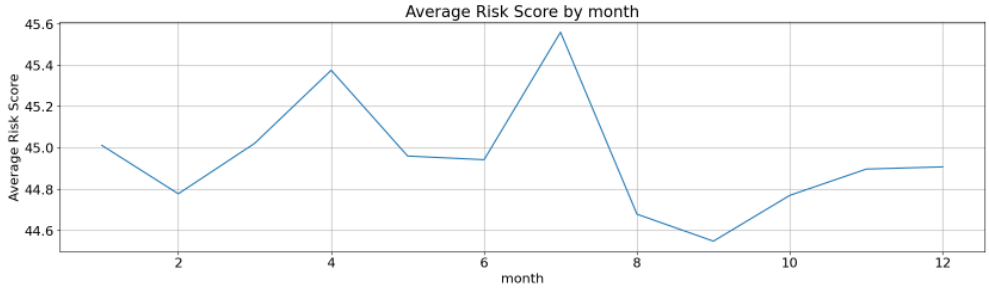
شكل 9 توزع المعاملات وفق الشهر

يوضح الشكل 10 توزع المعاملات وفق اليوم، كافة الايام يتم فيها معاملات بنسب متقاربة.



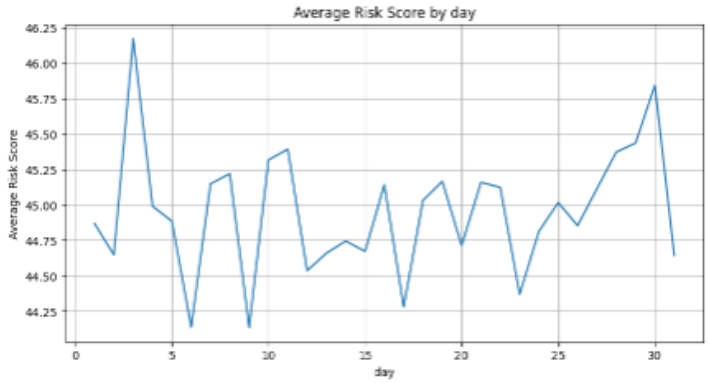
شكل 10 توزع المعاملات وفق اليوم

يوضح الشكل 11 متوسط الخطورة في المعاملات نسبة للشهر، اعلى مستوى خطورة هي في الشهر السابع والرابع.



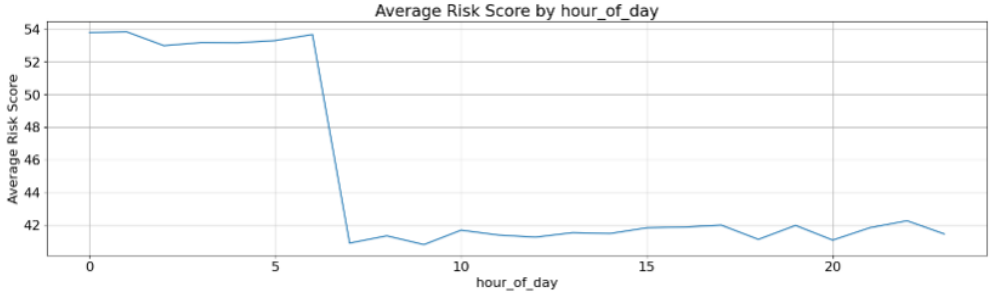
شكل 11 متوسط الخطورة في المعاملات نسبة للشهر

يوضح الشكل 12 متوسط الخطورة في المعاملات نسبة لليوم، اعلى مستوى خطورة هي في بداية أيام الشهر واخرها.



شكل 12 متوسط الخطورة في المعاملات نسبة لليوم

يوضح الشكل 13 متوسط الخطورة في المعاملات نسبة للساعة في المتوسط، هناك مخاطر عالية جدًا في ساعات الصباح الباكر (من الساعة 12 صباحاً إلى الساعة 7 صباحاً) مقارنة بالساعات المتبقية.



شكل 13 متوسط الخطورة في المعاملات نسبة للساعة

تم بعد ذلك معالجة البيانات وفق مايلي:

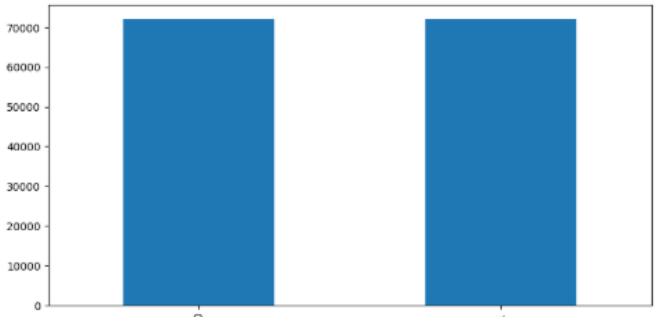
- حذف الميزة time stamp نظراً لانه تم استخلاص الميزات السابقة منه.
- حذف الميزات التالية عن طريق الاعتماد على هندسة الميزات والمعرفة بالمجال transaction_type, location_region, ip_prefix, login_frequency, session_duration, purchase_pattern, age_group, risk_score

فالميزات السابقة هي ميزات تم الحصول عليها من خصائص المستخدمين في شبكة سلاسل الكتل والمعاملات التي تم اجراءها فيها، لكن هذه الميزات لايتم اضافتها الى معلومات الكتلة في الشبكة مما يتعذر استخدامها لكشف الشذوذ في تطبيق سلاسل الكتل.

بعد ذلك تم اعتماد على المعاملات ذات الخطورة العالية high risk كمعاملات شاذة والباقي معاملات طبيعية كون نسبة الخطورة فيها متوسطة فما دون. ليكون عدد المعاملات الطبيعية 72105والمعاملات الشاذة 6495.

ليتم بعد ذلك تعيين العناوين إلى فهارس فريدة ثم ترميز العناوين الفريدة باستخدام LabelEncoder حيث يعدّ LabelEncoder أسلوب ترميز شائع للتعامل مع المتغيرات الفئوية. في هذه التقنية، يتم تعيين عدد صحيح فريد لكل عنوان عقدة. بعدها تم تقييس الميزة amount ,ويعد تقييس الميزة طريقة مستخدمة لتطبيع نطاق المتغيرات المستقلة أو ميزات البيانات. في معالجة البيانات، يُعرف أيضاً باسم تطبيع البيانات ويتم إجراؤه عموماً أثناء خطوة المعالجة المسبقة للبيانات. حيث تساعد عملية التطبيع، على سبيل المثال – في تمحور الميزات حول 0 أو في النطاق (0،1) حسب تقنية القياس وقد تم استخدام standard scaler.

ونظراً لكون البيانات غير متوازنة تم تطبيق تقنية موازنة البيانات RandomOverSampler وهي تقنية تستخدم لإجراء أخذ عينات عشوائية زائدة من الفئات الأقلية في مجموعات البيانات غير المتوازنة. وتعمل عن طريق تحديد عينات عشوائية من الفئة الأقلية مع الاستبدال لموازنة الفئات. يوضح الشكل 14 توزع البيانات بعد عملية الموازنة حيث أصبح كل فئة تحتوي على 72105 عينة.

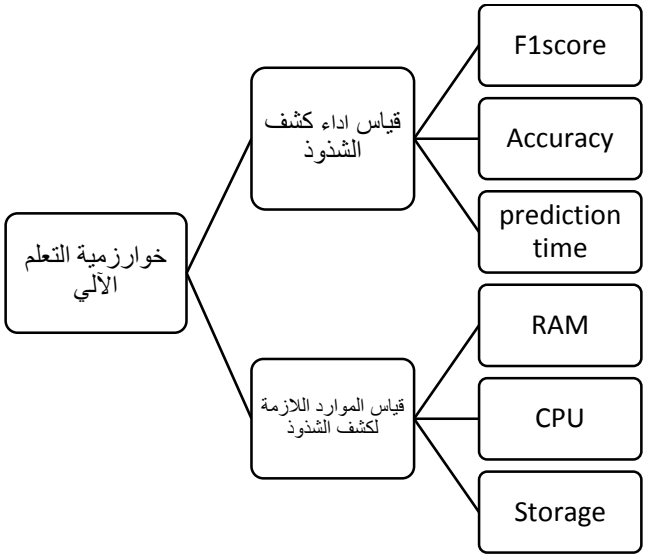


شكل 14 توزع البيانات بعد عملية الموازنة

ليتم بعدها الانتقال الي مرحلة تقسيم البيانات حيث تم تقسيم البيانات الى 80% للتدريب و 20% للاختبار.

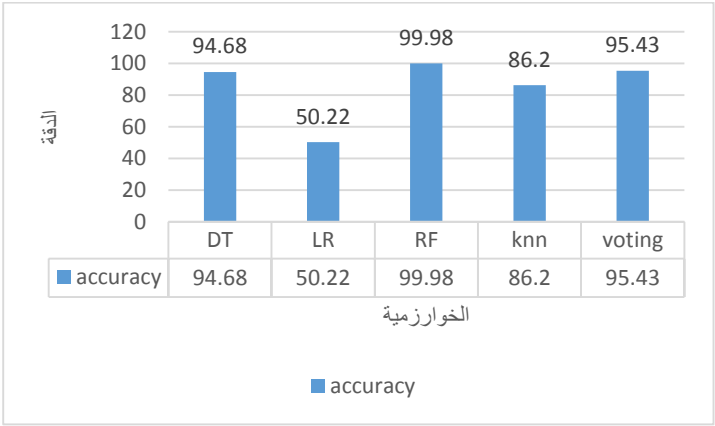
3.11 التجارب

تم استخدام نماذج التعلم الالي وهي DT,RF,KNN,LR لاكتشاف الشذوذ في سلاسل الكتل وتم قياس استهلاك الموارد لكل خوارزمية. يوضح الشكل 15 مخطط العمل في التجارب.



شكل 15 مخطط العمل في التجارب

يوضح الشكل 16 تجميع تائج الدقة لكافة المصنفات، من الواضح تفوق خوارزمية الغابة العشوائية وذلك يوافق الدراسات السابقة:

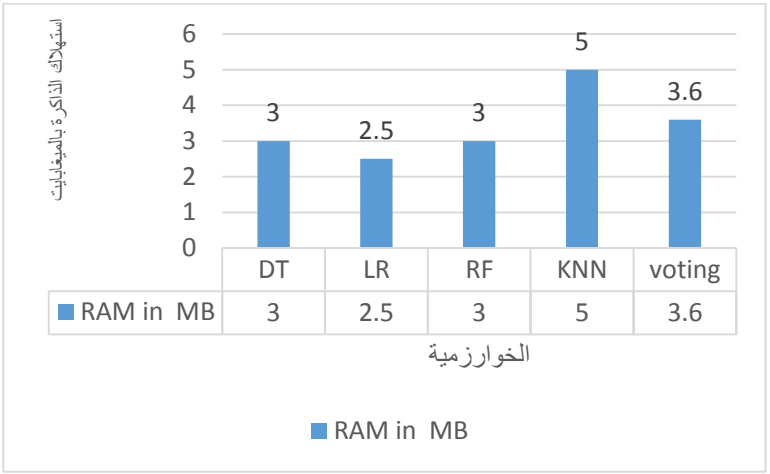


شكل 16 تجميع نتائج الدقة لكافة المصنفات

يوضح الشكل 17 تجميع f1score الدقة لكافة المصنفات، من الواضح تفوق خوارزمية الغابة العشوائية وذلك يوافق الدراسات السابقة:

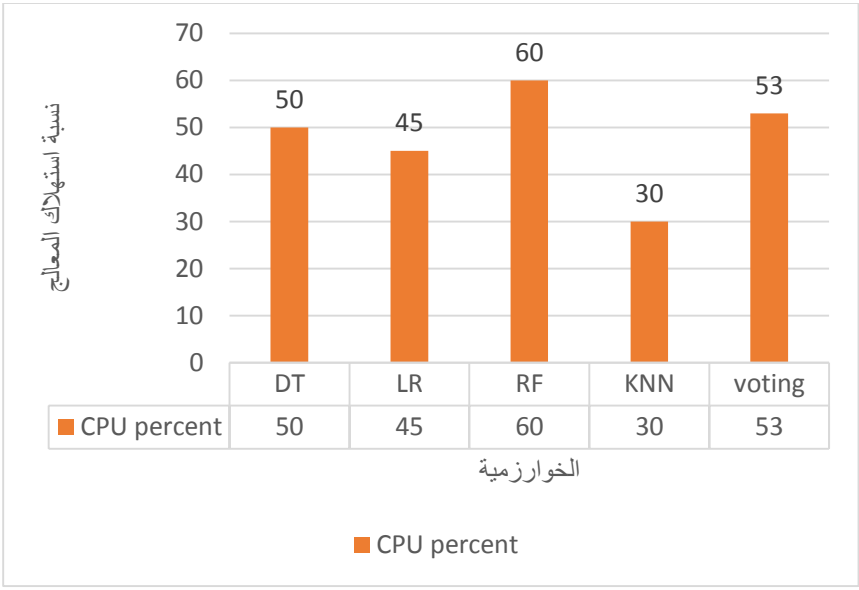
شكل 17 تجميع f1score الدقة لكافة المصنفات

يوضح الشكل 18 استهلاك الذاكرة للخوارزميات اثناء التجارب، من الواضح تقارب استهلاك الذاكرة للخوارزميات.



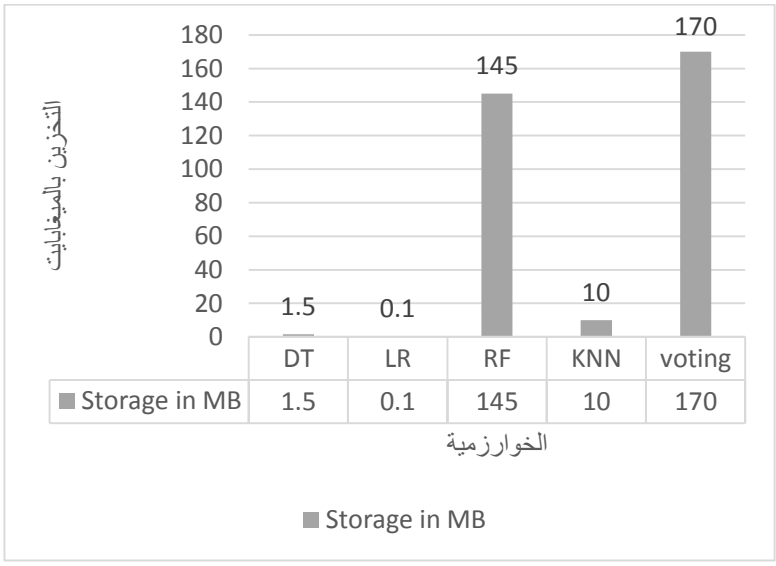
شكل 18استهلاك الذاكرة للخوارزميات اثناء التجارب

يوضح الشكل 19 نسبة استهلاك المعالج اثناء التجارب، من الواضح ان خوارزمية الغابة العشوائية والانتخاب هي من أكثر الخوارزميات استهلاكاً للمعالج.



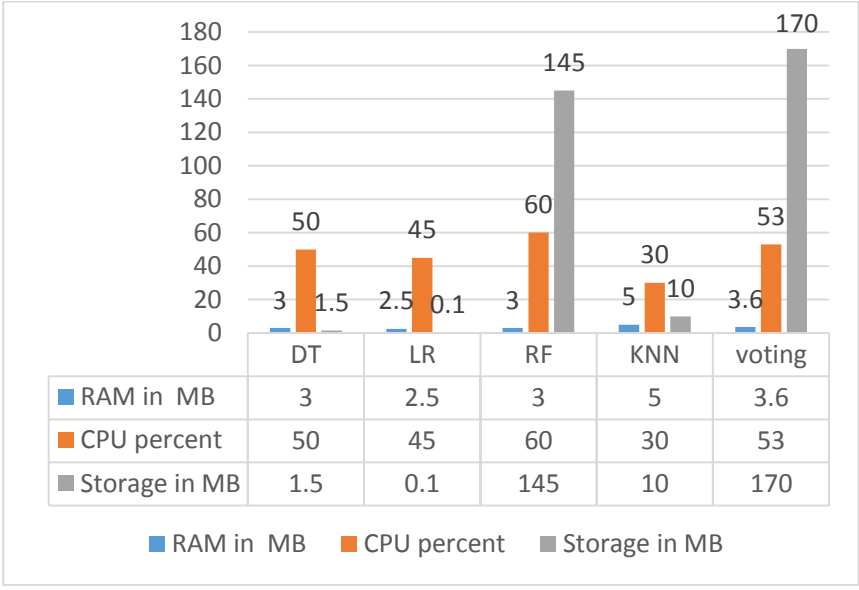
شكل 19 نسبة استهلاك المعالج اثناء التجارب

يوضح الشكل 20 مساحة التخزين اللازمة للخوارزميات، من الواضح ان خوارزمية الغابة العشوائية والانتخاب هي من أكثر الخوارزميات استهلاكا لمساحة التخزين.



شكل 20 مساحة التخزين اللازمة للخوارزميات

يوضح الشكل 21 افة الموارد التي تم استهلاكها اثناء التجارب، من الواضح ان خوارزمية الغابة العشوائية والانتخاب هي من أكثر الخوارزميات تطلباً للموارد.



	DT	LR	RF	KNN	voting
RAM in MB	3	2.5	3	5	3.6
CPU percent	50	45	60	30	53
Storage in MB	1.5	0.1	145	10	170

شكل 21 كافة الموارد التي تم استهلاكها اثناء التجارب

من النتائج السابقة يمكن التوصل الى التالي:

- **تصنيف استهلاك الموارد لكل خوارزمية**

يوضح الجدول 4 تصنيف استهلاك الموارد لكل خوارزمية بحيث يتم تصنيف الخوارزمية الى تصنيف مرتفع لاستهلاك الموارد او تصنيف متوسط لاستهلاك الموارد أو تصنيف منخفض لاستهلاك الموارد بناء على اجمالي النقاط التي حصلت عليها.

جدول 4 تصنيف استهلاك الموارد لكل خوارزمية

الخوارزمية	استهلاك المعالج (CPU %)	استهلاك الذاكرة (RAM MB)	حجم التخزين (MB)	إجمالي النقاط	التصنيف النهائي
الغابة العشوائية(RF)	60%	3 MB	145 MB	8	مرتفع (High Resource)
مصنف الانتخاب (Voting Classifier)	53%	3.6 MB	170 MB	8	مرتفع (High Resource)
شجرة القرار(DT)	50%	3 MB	1.5 MB	5	متوسط (Mid Resource)
أقرب جار(KNN)	30%	5 MB	10 MB	5	متوسط (Mid Resource)
الانحدار اللوجستي (LR)	45%	2.5 MB	0.1 MB	3	منخفض (Low Resource)

- **طريقة حساب التصنيف:**

1. **استهلاك المعالج:(CPU %)**
   - أكثر من 50% → 3 نقاط (مرتفع)
   - بين 40% و 50% → 2 نقاط (متوسط)
   - أقل من 40% → 1 نقطة (منخفض)
2. **استهلاك الذاكرة:(RAM MB)**

- **تم ملاحظة أن جميع النماذج لا تستهلك كم كبير من الذاكرة وللحفاظ على تناسق التصنيف يمكن اقتراح**
- أكثر من 4MB → 3 نقاط (مرتفع)
- بين 3MB و 4MB → 2 نقاط (متوسط)
- أقل من 3MB → 1 نقطة (منخفض)

3. **حجم التخزين المطلوب:(MB)**

- أكثر من 100MB → 3 نقاط (مرتفع)
- بين 50MB و100MB → 2 نقاط (متوسط)
- أقل من 50MB → 1 نقطة (منخفض)

التصنيف النهائي:

- **High Resource (مرتفع)** : مجموع النقاط ≤ 7
- **Mid Resource (متوسط):** مجموع النقاط بين 4 و6
- **Low Resource (منخفض):** مجموع النقاط ≥ 3

وبناء على كافة التجارب والنتائج وتصنيف النماذج تبين مايلي:

- من بين الخوارزميات ذات المتطلبات العالية كانت الغابة العشوائية افضل بدقة وصلت الى 99 % و f1score 0.99.
- من بين الخوارزميات ذات المتطلبات المتوسطة كانت شجرة القرار افضل بدقة وصلت الى 94.6% و f1score 0.95.

- من بين الخوارزميات ذات المتطلبات المنخفضة وصلت دقة LR الى 50.22 و f1score 0.5
- بغض النظر عن استهلاك الموارد كانت خوارزمية الغابة العشوائية هي اعلى نتائج من بين الخوارزميات افضل بدقة وصلت الى 99 % و f1score 0.99 في حين كانت خوارزمية LR هي الأسوء بدقة 50.22 و f1score 0.5.

12. الخلاصة والعمل المستقبلي

تم في هذا البحث دراسة وتحليل الموارد المطلوبة لتشغيل خوارزميات التعلم الالي لاكتشاف الشذوذ في سلاسل الكتل من اجل ذلك تم استخدام 5 خوارزميات تعلم الي وقياس أداء الخوارزميات لاكتشاف الشذوذ وفق معيار الدقة و f1score وتم قياس استهلاك هذه الخوارزميات للموارد وفق استهلاك الذاكرة ونسبة استهلاك المعالج والتخزين وتم بعدها تقسيم الخوارزميات بالنسبة لاستهلاك الموارد لثلاثة تصنيفات وهي تصنيف موارد منخفض وتصنيف موارد متوسط وتصنيف موارد عالي وتم تصنيف خوارزمية شجرة القرار وخوارزمية الانتخاب كموارد عالية وخوارزمية DT كموارد متوسطة وخوارزميتي LR و KNN كموارد منخفضة، فمن بين الخوارزميات ذات المتطلبات العالية كانت الغابة العشوائية افضل بدقة وصلت الى 99 % و f1score 0.99 ومن بين الخوارزميات ذات المتطلبات المتوسطة كانت شجرة القرار افضل بدقة وصلت الى 94.6 % و f1score 0.95 ومن بين الخوارزميات ذات المتطلبات الضعيفة كانت LR افضل بدقة 50.22 و f1score 0.5

للعمل المستقبلي من الممكن استخدام التعلم العميق للتحقق من القدرة على اكتشاف الشذوذ في سلاسل الكتل وقياس نسبة استهلاك الموارد لمعرفة إمكانية تضمينها ضمن عقد سلاسل الكتل.

13. جدول الاختصارات

AI	**Artificial Intelligence**
DT	**Decision Tree**
KNN	**K-Nearest Neighbor**
LR	**Logistic Regression**
MI	**Machine learning**
NN	**Neural network**
RF	**Random forest**
SGD	**Stochastic Gradient Descent**

المراجع

[1] Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2022). Blockchain for the metaverse: A review. arXiv preprint arXiv:2203.09738.

[2] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). Ieee, 2017.

[3] Sarmah, Simanta Shekhar. "Understanding blockchain technology." Computer Science and Engineering 8.2 (2018): 23-29.

[4] Bashir, Imran. Mastering blockchain. Packt Publishing Ltd, 2017.

[5] L. Rokach, O. Maimon, Decision trees, in: O. Maimon, L. Rokach (Eds.), "Data Mining and Knowledge Discovery Handbook" , Springer, Boston, MA, pp. 165-192, 2005.

[6] Song, Y. Y., & Lu, Y, "Decision tree methods: applications for classification and prediction". Shanghai archives of psychiatry, 27(2), 130–135. 2015.

[7] Hastie T, Tibshirani R, Friedman J. "The Elements of Statistical Learning", Springer, . pp: 269-272, 2001

[8]Introduction to Algorithms for Data Mining and Machine Learning Xin-She Yang Middlesex University School of Science and Technology London, United Kingdom.

[9] John Wiley & Sons, "Machine Learning For Dummies" Published by: New Jersey Media and software compilation 2016

[10] https://towardsdatascience.com/metrics-to-evaluate-your-machine-learning-algorithm-f10ba6e38234

[11] https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9

[12] https://www.ibm.com/cloud/learn/machine-learning

[13] Mehra, Sidharth & Hasanuzzaman, Mohammed, "Detection of Offensive Language in Social Media Posts", 2020.

[14]https://towardsdatascience.com/steps-of-a-machine-learning-process-7acc43973385

[15]Monowar H. Bhuyan,Dhruba K. Bhattacharyya,Jugal K. Kalita "Network Traffic Anomaly Detection and Prevention Concepts ،Techniques ،and Tools", 2017.

[16]Jose, Shijoe & Malathi, D. & Reddy, Bharath & Jayaseeli J D, Dorathi. "A Survey on Anomaly Based Host Intrusion Detection System". Journal of Physics, 2018.

[17] Siddamsetti, S., Tejaswi, C., & Maddula, P. (2024). Anomaly detection in blockchain using machine learning. Journal of Electrical Systems, 20(3), 619-634.

[18] https://www.kaggle.com/datasets/faizaniftikharjanjua/metaverse-financial-transactions-dataset

[19] Siddique, Quba. "Anomaly Detection in Blockchain Transactions within the Metaverse Using Anomaly Detection Techniques." Journal of Current Research in Blockchain 1.2 (2024): 155-165.

[20] Shayegan, Mohammad Javad, et al. "A collective anomaly detection technique to detect crypto wallet frauds on bitcoin network." Symmetry 14.2 (2022): 328.

[21] Singh, P., Agrawal, D., & Pandey, S. (2023). Anomaly detection and analysis in blockchain systems.

[22] Airlangga, G. (2024). Anomaly Detection in Blockchain Transactions: A Machine Learning Approach within the Open Metaverse. Jurnal Informatika Ekonomi Bisnis, 308-312.

[23] Samantha Jeyakumar , Eugene Yugarajah , Andrew Charles , Punit Rathore , et al. Feature Engineering for Anomaly Detection and Classification of Blockchain Transactions. TechRxiv. March 27, 2023.

[24] 9.Ashfaq T, Khalid R, Yahaya AS, Aslam S, Azar AT, Alsafari S, Hameed IA. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors. 2022; 22(19):7162. https://doi.org/10.3390/s22197162

[25] 12. Hisham, S., Makhtar, M., & Aziz, A. A. (2023). An interpretable ensemble model framework for real-time anomaly detection

and prediction of Ethereum blockchain transactions. International Journal of Advanced Technology and Engineering Exploration, 10(103), 676.

[26] Sallam, Amer, et al. "Fraudulent account detection in the Ethereum's network using various machine learning techniques." International Journal of Software Engineering and Computer Systems 8.2 (2022): 43-50.

[27] Anthony, Njoku ThankGod, et al. "Anomaly detection system for Ethereum blockchain using machine learning." Proceedings of the 19th International Conference on Manufacturing Research. Vol. 25. IOS Press, 2022.

[28] Airlangga, Gregorius. "Deep Learning for Anomaly Detection and Fraud Analysis in Blockchain Transactions of the Open Metaverse." Jurnal Informatika Ekonomi Bisnis (2024): 324-329.

[29] https://www.ibm.com/think/topics/logistic-regression

[30] Eng. Mohammad khalil, Dr. Mohammed Alchaita, Dr. Mohammad Assoura, Study of the blockchain and its potential use in verifying ownership of the public key in sending encrypted messages,Homs University Journal, Volume 43, Issue 10, 2021

[31] Eng. Ali Yassin, Dr. Kamal Al-Salloum, Dr. Wassim Ramadan, Selecting the Optimal Classification Threshold Dynamically in Early Anomaly Detection Systems Based on Deep Learning, Homs University Journal, Volume 44, Issue 8, 2022.

[32] Ali Yassin, Dr. Kamal Al-Salloum, Dr. Wassim Ramadan Selecting the Optimal Combination of Hyperparameter Tuning and Feature Selection to Improve the Performance of Anomaly Detection Systems Eng. Mechanical, Homs University Journal. Volume 44, Issue 5, 2022

تحديد العتبة المثلى للمعاملات الشاذة باستخدام التعلم الآلي لتحسين أمن سلاسل الكتل

علي عطية[1] أ.د.ماهر عباس[2] د.وسيم رمضان[3]

(1) طالب دكتوراه في قسم هندسة الشبكات والنظم الحاسوبية، كلية الهندسة المعلوماتية، جامعة حمص.

(2) أستاذ دكتور في قسم هندسة الشبكات والنظم الحاسوبية، كلية الهندسة المعلوماتية، جامعة حمص.

(3) دكتور في كلية الهندسة الزراعية، جامعة حمص.

الملخص

إن التقارب بين اكتشاف الشذوذ وتحديد العتبة في تقنية البلوك تشين يخلق إطاراً أمنياً متطوراً يستفيد من التعلم الآلي لحماية الشبكات اللامركزية. يبدأ هذا النهج المتكامل بجمع ومعالجة بيانات معاملات البلوك تشين مسبقاً، حيث تحدد الخوارزميات المتخصصة الأنماط التي تنحرف عن السلوك المتوقع. تتطلب معاملات البلوك تشين مراقبة متقدمة لضمان الأمن والسلامة مع ظهور التعلم الآلي كأداة قوية لتحديد الأنشطة المشبوهة. من خلال تحليل الأنماط في بيانات المعاملات، يتم تحديد عتبات دقيقة للكشف عن الشذوذ. حيث يكمن مفتاح النجاح في ضبط هذه العتبات بناءً على المعاملات الطبيعية والشاذة، مما يسمح للنظام بالتمييز بين المعاملات الطبيعية والمعاملات الاحتيالية. يهدف هذا البحث إلى تحديد العتبة المثلى للمعاملات الشاذة في سلاسل الكتل باستخدام تقنيات التعلم الآلي، مما يسهم في تعزيز أمان الشبكات اللامركزية. تم تدريب خمس خوارزميات تصنيف، هي: شجرة القرار، الغابة العشوائية، الانحدار اللوجستي، أقرب جار، ومصنف الانتخاب، وذلك

باستخدام بيانات معاملات من مجموعة Metaverse Financial Transactions Dataset التي تحتوي على 78,600 سجل .أُجريت ثلاث تجارب باستخدام تقنيات مختلفة لموازنة البيانات، وقيّم الأداء بناءً على دقة التصنيف (Accuracy) ومعامل .F1-score أظهرت النتائج أن عتبة الخطورة المثلى هي فوق 85(High Risk) ، حيث تفوقت تجربةRandomOverSampler ، محققة دقة 99.99% و F1-score = 0.9 ، مع تحسين أداء خوارزميات الانحدار اللوجستي وأقرب جار بالنسبة لمقياس f1score بمقدار 13% و 39 %على التوالي .تدعم هذه النتائج استخدام تقنيات موازنة البيانات في تعزيز دقة اكتشاف الشذوذ، مما يمهد الطريق لتطوير أنظمة أكثر كفاءة لمكافحة الاحتيال في شبكات سلاسل الكتل.

الكلمات المفتاحية: سلاسل الكتل، كشف الشذوذ، التعلم الالي، عتبة المعاملات الشاذة، التصنيف.

Determining The Optimal Threshold for Anomalous Transactions Using Machine Learning to Improve Blockchain Security

Abstract

The convergence of anomaly detection and thresholding in blockchain technology creates a sophisticated security framework that leverages machine learning to protect decentralized networks. This integrated approach begins with the pre-collection and processing of blockchain transaction data, where specialized algorithms identify patterns that deviate from expected behavior. Blockchain transactions require advanced monitoring to ensure security and integrity, with machine learning emerging as a powerful tool to identify suspicious activities. By analyzing patterns in transaction data, precise thresholds for anomaly detection are determined. The key to success lies in adjusting these thresholds based on normal

and abnormal transactions, allowing the system to distinguish between normal and fraudulent transactions.

This research aims to identify the optimal threshold for anomalous transactions in blockchains using machine learning techniques, which contributes to enhancing the security of decentralized networks. Five classification algorithms, namely decision tree, random forest, logistic regression, nearest neighbor, and election classifier, were trained using transaction data from the Metaverse Financial Transactions Dataset containing 78,600 records.

Three experiments were conducted using different data-balancing techniques, and performance was evaluated based on classification accuracy (Accuracy) and F1-score. The results showed that the optimal risk threshold is above 85 (High Risk), where the RandomOverSampler experiment outperformed, achieving 99.99% accuracy and an F1-score of 0.9, while improving the performance of the logistic regression and nearest neighbor algorithms with respect to the F1-score metric by 13% and 39%, respectively. These results support the use of data balancing techniques to enhance the accuracy of anomaly detection, paving the way for the development of more efficient anti-fraud systems in blockchain networks

Keywords: Blockchains, Anomaly Detection, Machine Learning, Anomaly Transaction Threshold, Classification.

1. مقدمة

لقد أحدث ظهور تقنية البلوك تشين ثورة في المجال التقني، حيث وعدت بشفافية وأمان غير مسبوقين من خلال بنيتها اللامركزية. ومع ذلك، فإن هذه التكنولوجيا تقدم تحديات فريدة من نوعها لمنع الاحتيال. في حين تقدم تقنية البلوك تشين العديد من المزايا، فإن طبيعتها اللامركزية والمجهولة،

إلى جانب ثبات المعاملات، تخلق أرضاً خصبة للجهات الخبيثة. وتزداد هذه المشكلة خطورة مع ارتفاع خسائر الاحتيال في الأنظمة المالية الرقمية، والتي تُقدر بالمليارات سنوي[19] . إن طرق الكشف عن الاحتيال التقليدية، المصممة للأنظمة المركزية، غير مجهزة للتعامل مع التعقيدات المحددة لتقنية البلوك تشين. يكمن أحد التحديات الأساسية في تحديد العتبة المثلى التي تفصل بين المعاملات الطبيعية والمشبوهة بدقة.. وهذا أكثر تعقيداً مما يبدو، حيث تُظهِر معاملات blockchain اختلافات طبيعية يجب تمييزها عن السلوك الشاذ.

الطبيعة الديناميكية لكل من الاستخدام المشروع لـ blockchain والنشاط الاحتيالي تزيد من تعقيد هذه المهمة، حيث تظهر حالات استخدام مشروعة جديدة باستمرار، بينما يكيف الجهات الخبيثة استراتيجياتها باستمرار للتهرب من الكشف. وهذا يتطلب حلولاً تكيفية قادرة على التعلم والتطور جنباً إلى جنب مع التكنولوجيا.

إن التوفيق بين تقليل الإيجابيات الكاذبة (المعاملات المشروعة التي يتم وضع علامة عليها على أنها مشبوهة) والسلبيات الكاذبة (النشاط الاحتيالي المفقود) يتطلب دراسة متأنية، وندرة البيانات اللازمة لتدريب نماذج التعلم الآلي وعدم توازن البيانات يزيدان من تفاقم المشكلة.

جلبت التطورات الأخيرة في التعلم الآلي حلولاً واعدة لهذه المشكلة المعقدة. يمكن لهذه الأنظمة المتطورة تحليل الأنماط المعقدة عبر أبعاد متعددة من بيانات المعاملات، من القيم النقدية إلى الأنماط الزمنية والعلاقات الشبكية. مما يوفر مساراً محتملاً نحو اكتشاف الاحتيال بشكل أكثر قوة وتكيفاً في مشهد blockchain المتطور باستمرار. على الرغم من الجهود السابقة في استخدام التعلم الآلي للكشف عن الشذوذ، لا تزال هناك تحديات في تحديد العتبة المثلى للمعاملات الشاذة، حيث تختلف العتبات وفقاً لأنماط المعاملات والسياقات المختلفة. يهدف هذا البحث إلى معالجة هذه الفجوة من خلال تحديد العتبة المثلى للمعاملات الشاذة في سلاسل الكتل باستخدام تقنيات التعلم الآلي، مما يسهم في تعزيز أمان الشبكات اللامركزية. لتحقيق ذلك تم تدريب خمس خوارزميات

تصنيف، هي: شجرة القرار، الغابة العشوائية، الانحدار اللوجستي، أقرب جار، ومصنف الانتخاب وتم أُجراء ثلاث تجارب باستخدام تقنيات مختلفة لموازنة البيانات، وتقييّم الأداء بناءً على دقة التصنيف Accuracy ومعامل .F1-score

2. مشكلة البحث

تتمثل مشكلة البحث في تحديد عتبة المعاملات الشاذة في سلاسل الكتل باستخدام التعلم الآلي حول إنشاء حد معين يميز بدقة بين المعاملات الطبيعية والشاذة نظراً لكون اختيار العتبة الخاطئة قد يؤدي إلى تصنيف خاطئ للمعاملات، مما يعرقل عمليات كشف الاحتيال أو يزيد من حجب المعاملات السليمة عن طريق الخطأ. يشمل هذا التحدي على عدة عوامل، بداية بالصعوبة المتمثلة في تطوير نماذج التعلم الآلي التي يمكنها تحديد الشذوذ الحقيقي بشكل فعال مقابل الاختلافات الطبيعية في أنماط المعاملات، والتعقيد المنهجي لموازنة الحساسية والخصوصية في الكشف.

3. هدف البحث

يهدف هذا البحث إلى تحديد العتبة المثلى للمعاملات الشاذة في سلاسل الكتل باستخدام تقنيات التعلم الآلي، مما يسهم في تحسين كشف المعاملات الاحتيالية وتعزيز أمن الشبكات اللامركزية. لتحقيق ذلك، يتم تدريب نماذج تصنيف مختلفة على مجموعة بيانات سلاسل الكتل، مع دراسة تأثير تقنيات موازنة البيانات على دقة التصنيف. سيتم تحليل أداء النماذج وتحديد العتبة المثلى التي تضمن تحقيق أعلى كفاءة في كشف الشذوذ مع تقليل الأخطاء في التصنيف.

4. سلاسل الكتل

سلاسل الكتل هي دفتر رقمي لامركزي يخزن السجلات بشكل آمن عبر شبكة الاجهزة بطريقة شفافة وغير قابلة للتغيير ومقاومة للتلاعب. تتكون من كتل من البيانات مرتبطة ببعضها البعض في سلسلة زمنية. (مرجع)

5. التعلم الالي

هو فرع من فروع الذكاء الاصطناعي (AI) وعلوم الكمبيوتر الذي يركز على استخدام البيانات والخوارزميات لتقليد الطريقة التي يتعلم بها البشر، وتحسين دقتها تدريجياً. يعد التعلم الآلي مكوناً مهماً في المجال المتنامي لعلوم البيانات. من خلال استخدام الأساليب الإحصائية، يتم تدريب الخوارزميات على إجراء تصنيفات أو تنبؤات في مشاريع التنقيب عن البيانات. تؤدي هذه الأفكار بعد ذلك إلى اتخاذ القرار داخل التطبيقات والشركات، مما يؤثر بشكل مثالي على مقاييس النمو الرئيسية [12].

6. الشذوذ

يعرف الشذوذ بالشكل العام بأنه أنماط في البيانات لا تتوافق مع مفهوم محدد جيداً للسلوك الطبيعي.ويمكن تعريف أنظمة كشف الشذوذ على أنها أجهزة أو برامج تقوم بمراقبة البيانات المتعلقة بمجال معين لتحديد الحالات الشاذة والمختلفة عن السلوك الطبيعي [21]

6.1 الشذوذ في سلاسل الكتل

يشير الشذوذ إلى أي انحراف أو مخالفة أو قيمة شاذة عن نمط أو سلوك متوقع أو طبيعي. في سياق سلاسل الكتل، يمكن أن يشير الشذوذ إلى أنشطة غير عادية أو سلوك مريب أو تهديدات أمنية محتملة داخل شبكة سلاسل الكتل. يتضمن اكتشاف الشذوذ في سلاسل الكتل عملية تحديد مثل هذه الشذوذ. قد يكون اكتشاف الشذوذ في بيئة سلاسل الكتل أمراً صعباً بسبب عدة أسباب [6]: 1. الطبيعة الموزعة وغير القابلة للتغيير: سلاسل الكتل عبارة عن دفتر حسابات لامركزي وموزع، حيث يحتفظ كل مشارك بنسخة من سلاسل الكتل بالكامل. بمجرد تسجيل معاملة وإضافتها إلى كتلة، تصبح غير قابلة للتغيير عملياً. وهذا يعني أنه لا يمكن إزالة أي معاملة شاذة أو احتيالية بمجرد إضافتها إلى سلاسل الكتل بسهولة. يجب أن تأخذ تقنيات اكتشاف الشذوذ في الاعتبار هذه الخاصية الفريدة لسلسلة الكتل أثناء تحديد الشذوذ والتخفيف منه. 2. كمية هائلة من البيانات: تولد

شبكات سلسلة الكتل كمية هائلة من البيانات بسبب التسجيل المستمر للمعاملات. يمكن أن يكون تحليل ومعالجة هذا الحجم الكبير من البيانات في الوقت الفعلي مكثفاً من الناحية الحسابية. يجب أن تكون طرق اكتشاف الشذوذ قابلة للتطوير وفعالة بما يكفي للتعامل مع الإنتاجية العالية لمعاملات سلسلة الكتل. 3. أنماط المعاملات المعقدة: يمكن أن تظهر معاملات سلسلة الكتل أنماطاً وتبعيات معقدة. يمكن أن تظهر الشذوذ في أشكال مختلفة، مثل أحجام المعاملات غير الطبيعية، وأنواع المعاملات غير العادية، والتغيرات المفاجئة في سلوك الشبكة، أو الأنشطة الضارة. يجب أن تكون خوارزميات اكتشاف الشذوذ قادرة على التقاط وفهم أنماط المعاملات المعقدة هذه للكشف عن الشذوذ بشكل فعال.

6.1.1 أنواع الشذوذ في سلاسل الكتل

يمكن أن تحدث عدة أنواع من الشذوذ في سلاسل الكتل، والتي يمكن أن تكون مؤشراً على نشاط احتيالي أو ضار. فيما يلي بعض الأنواع الشائعة من الشذوذ في سلاسل الكتل [6] : 1. هجمات الإنفاق المزدوج: يحدث هجوم الإنفاق المزدوج عندما يحاول الفرد إنفاق نفس العملة المشفرة مرتين. يمكن القيام بذلك عن طريق إنشاء معاملة وهمية، والتي يتم بثها بعد ذلك إلى الشبكة. إذا تم قبول المعاملة المزيفة وإضافتها إلى سلاسل الكتل قبل المعاملة المشروعة، يمكن للفرد أن ينفق نفس العملة المشفرة مرتين فعلياً. 2. ازدحام الشبكة: يحدث ازدحام الشبكة عندما يتجاوز عدد المعاملات التي يتم بثها إلى الشبكة قدرتها على المعالجة. يمكن أن يؤدي هذا إلى تأخيرات في معالجة المعاملات وزيادة رسوم المعاملات وربما رفض المعاملات الصالحة. 3. المعاملات الاحتيالية: تحدث المعاملات الاحتيالية عندما يحاول الفرد التلاعب بالبلوك تشين عن طريق إنشاء معاملات وهمية أو تعديل المعاملات الموجودة. يمكن القيام بذلك في محاولة لسرقة العملة المشفرة أو الحصول على وصول غير مصرح به إلى الشبكة. 4. الأخطاء في العقود الذكية: العقود الذكية هي عقود ذاتية التنفيذ تعمل على سلاسل الكتل .إذا كانت هناك أخطاء في كود العقد الذكي، فقد يؤدي هذا

إلى سلوك غير متوقع، والذي يمكن استغلاله من قبل الجهات الخبيثة. 5. هجماتSybil: حدث هجمات Sybil عندما ينشئ فرد هويات مزيفة متعددة، أو Sybils على الشبكة. يمكن القيام بذلك في محاولة للتلاعب بآلية الإجماع والسيطرة على الشبكة.

7. الدراسة المرجعية

تتضمن أدبيات الدراسة مجموعة من الطرق لتحديد عتبة المعاملات الشاذة والطبيعية بدءاً من التحليل الاحصائي وهندسة الميزات حيث تعرف هندسة الميزات بأنها عملية إنشاء مجموعة ميزات باستخدام خصائص البيانات التي تعزز أداء خوارزميات تعلم الآلة [20] ووصولاً الى طرق التعلم الآلي والتعلم العميق وذلك من اجل تحديد العتبة الأمثل لفصل القيم الشاذة عن القيم الطبيعية في سلاسل الكتل.

تسعى الدراسة [14] إلى دمج تقنيات الذكاء الاصطناعي القابلة للتفسير وقواعد الشذوذ في مصنفات المجموعة القائمة على الشجرة للكشف عن معاملات البيتكوين الشاذة. يتم استخدام طريقة التفسير الإضافي لـ Shapley (SHAP) لقياس مساهمة كل ميزة. علاوة على ذلك، يتم تقديم قواعد لتفسير ما إذا كانت معاملة البيتكوين شاذة أم لا. ذلك باستخدام التمثيلات الشجرية لفهم سبب تصنيف حالات معينة على أنها شذوذ. لتوفير تفصيلاً خطوة بخطوة لعملية اتخاذ القرار وتسليط الضوء على الميزات والعتبات التي لعبت دوراً حاسماً في اتخاذ القرار، كما تم تقديم خوارزمية أخذ عينات ناقصة تسمى XGBCLUS، مصممة لموازنة بيانات المعاملات الشاذة وغير الشاذة. ومقارنة هذه الخوارزمية بتقنيات أخرى شائعة الاستخدام لتقليل أخذ العينات وزيادة أخذ العينات.

تم في البحث [15] تنفيذ وتقييم خوارزمية اكتشاف الشذوذ القائمة على K–means وهي خوارزمية تجميع شائعة يمكن تطبيقها على اكتشاف الشذوذ. يكتشف K–means الشذوذ من خلال عتبتين بعد إجراء التجميع. المسافة بين عقدة الهدف ومركز ثقل المجموعة التي تنتمي إليها العقدة.

يتم حساب الإحداثيات من كل كمية ميزة. وحجم المجموعة التي تنتمي إليها العقدة. إذا تجاوزت الحد الأقصى أو كانت أصغر من الحد الأقصى، تعتبر العقدة شاذة.

قدمت ورقة البحث [16] نظاماً موثوقاً به للكشف عن الشذوذ، تم استخدام Deep Autoencoder في تنفيذ نظام الكشف عن الشذوذ، على وجه التحديد، يتم البحث عن ضبط المعلمات المحددة جيداً، حتى عندما يؤدي هذا إلى زيادة تعقيد المصنف بشكل كبير، شريطة أن يكون المصنف قادراً على تصنيف البيانات المستهدفة بشكل صحيح. كلما كان النموذج أكثر تعقيداً، كلما كان نطاق التصنيف في مساحة البيانات المستهدفة أصغر، وانخفض احتمال تصنيف القيم المتطرفة بشكل صحيح. بشكل أساسي ومن أجل التنبؤ بما إذا كانت المعاملة الجديدة طبيعية أم احتيالية، يتم حساب خطأ إعادة بناء Deep Autoencoder من تفاصيل المعاملة نفسها. إذا كان الخطأ أكبر من عتبة محددة مسبقاً، فسوف يتم تصنيفه على أنه غير طبيعي، عن طريق استخدام عتبة مجموعة البيانات المثلى وهي طريقة لرفض عينات الفئة الإيجابية (العادية) القريبة من حافة فصل الفئة. قد تؤدي هذه العينات إلى تصنيف مضلل بحيث لا يتم أخذها في الاعتبار.

تقترح الدراسة [17] خوارزمية اكتشاف التطفل التعاوني القائمة على سمة التجميع لـ Blockchain والتي يمكنها التعرف بسرعة على سمات التجميع في معاملات بيانات .Blockchain يتم أيضاً إنشاء نموذج رياضي، بناءً عليه تم تصميم بروتوكول اكتشاف التطفل القائم على سمة التجميع للكشف بدقة عن عدد سمات التجميع. تتمتع الخوارزمية المقترحة بدقة التعرف الممتازة وتكلفة الوقت، يتم النظر في معامل الترجيح لخصائص البيانات وعلاقة مطابقة التشابه في النمط الطبيعي في هذا النهج. تتم مطابقة مواضع المجموعة لتقليل تكلفة اكتشاف بيانات التجميع، ويتم التعرف على خصائص التجميع بدقة.

في [2] تم تطوير مخطط للكشف عن الشذوذ الذي يميز معلمات blockchain على أنها طبيعية أو شاذة باستخدام التحليل الإحصائي وطرق التجميع الهرمي. تم استخدام الهيستوغرام وتوزيعات

الاحتمالات والرسوم البيانية الصندوقية للبيانات لتقدير العتبات للقيم المتطرفة التي قد تشير إلى الهجمات. تم استخدام العتبات التي تم الحصول عليها من المخططات الشجرية لتشكيل مجموعات ومجموعات فرعية بناءً على بنية البيانات الهرمية؛ تعتبر مؤشرات نقاط البيانات التي لا تقع ضمن العتبة شاذة وغير مدرجة في المجموعات.

يركز البحث [3] على اكتشاف الشذوذ داخل مجموعة بيانات معاملات البيتكوين. وتهدف إلى تحسين فهم سلوكيات الشذوذ داخل شبكات البلوك تشين واستكشاف كيفية تحديد هذه الشذوذ بشكل فعال. علاوة على ذلك، تحاول تعزيز الأساليب الحالية للكشف عن الشذوذ الثابت وتوفير تحليل نظري شامل لتقنيات الكشف عن الشذوذ الديناميكي. يتم تدريب النموذج باستخدام إما دالة الخسارة متوسط الخطأ التربيعي أو متوسط الخطأ المطلق بعد التدريب، يقوم النموذج بإجراء تنبؤات على مجموعة الاختبار. ثم يتم حساب خطأ كل معاملة من خلال مقارنة القيم المتوقعة والفعلية. يتم تصنيف المعاملات التي تتجاوز أخطاءها عتبة النسبة المئوية 95 على أنها شذوذ. تضمن هذه العتبة أن يركز النموذج على تحديد أكثر التناقضات تطرفًا، والتي تمثل المعاملات التي تنحرف بشكل كبير عن الأنماط المتوقعة التي يلتقطها النموذج. تم اختيار هذه العتبة لأنها توازن بين الحاجة إلى اكتشاف الشذوذ، والتي تعد نادرة بحكم التعريف، مع الحاجة إلى الحد من الإيجابيات الكاذبة.

تهدف الدراسة [12] إلى اكتشاف الجهات الخبيثة العاملة على شبكة Ethereum وتصنيف الهجمات بناءً على أفعالها. لتحقيق هدف البحث هذا، تم إنشاء مجموعة بيانات جديدة من خلال دمج البيانات حول الجهات الخبيثة المشاركة في أنشطة Ethereum غير المشروعة. تم استخراج الميزات الرئيسية من مجموعة البيانات هذه باستخدام تقنيات اختيار الميزات المتقدمة، بما في ذلك تحليل المكونات الأساسية ((PCA، وكسب المعلومات. تم تطبيق مصنفات التعلم الآلي مثل LGBM وXGBoost وRandom Forest وExtra Tree وBagging و K-Nearest Neighbors لتحديد وتصنيف الجهات الخبيثة بشكل فعال. تؤكد النتائج، التي حققت معدل دقة 98٪، فعاليةInformation Gain عند دمجها مع LGBM و .XGBoostوالجدير بالذكر أن

XGBoost يثبت كفاءته من خلال إكمال التحليل في 13.72 ثانية فقط. بالإضافة إلى تحديد الأنشطة الاحتيالية. يركز الحل المقترح في [7] على استخدام نهج ديناميكي حيث يتم استخدام سلوك التشغيل الطبيعي لسلسلة كتل Ethereum لتدريب خوارزميات التعلم الآلي وسيتم وضع علامة على أي انحراف على أنه شذوذ واكتشافه بواسطة النظام. تم استخدام أربع خوارزميات للتعلم الآلي بما في ذلك K-Nearest Neighbors (KNN) و Gaussian Naive Bayes (GaussianNB) و Random Forest و Stochastic Gradient Descent (SDG) لتدريب والتحقق من دقة الحل المقترح. أظهرت النتائج التجريبية أن خوارزمية الغابة العشوائية قدمت أفضل دقة بنسبة 99.84٪ مقارنة بخوارزميات التعلم الآلي الأخرى.

يوضح الجدول 1 مقارنة الدراسات المرجعية، من الواضح ان الدراسة الحالية تعالج مشكلة البيانات الغير المتوازنة وتعتمد على تحديد عتبة الشذوذ بناء على خصائص المعاملة وسلوك المستخدم ووصلت دقة كشف الشذوذ الى 99.99 %:

جدول 1 مقارنة الدراسات المرجعية

الدراسة	استخدام تقنيات موازنة	دراسة عتبة شذوذ	تحديد عتبة الشذوذ بناءعلى خصائص المعاملة وسلوك المستخدم	طريقة تحديد عتبة الشذوذ	النتائج
[14]	✓	✓	✖	أهمية الميزة باستخدام شجرة القرار	دقة كشف شذوذ تصل الى 0.97
[15]	✖	✓	✖	K-means	معدل fp يصل الى 0.03
[16]	✖	✓	✖	ODT	دقة كشف شذوذ تصل الى 0.99
[17]	✖	✓	✖	التجميع	FPR=0.92
[2]	✖	✓	✖	التجميع والطرق الإحصائية	------

[3]	✖	✓	✖	LSTML Model Traning	(MSE) مساوية ل 85255
الدراسة الحالية	✓	✓	✓	اعتماد عتبة رقمية للشذوذ بناء على خصائص المعاملة وسلوك المستخدم	دقة كشف شذوذ تصل الى 99.99

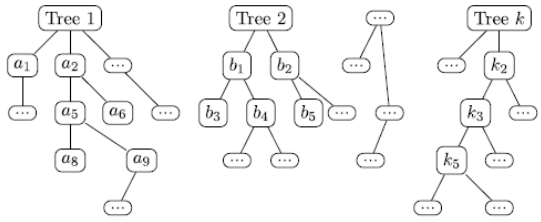
8. الخوارزميات المستخدمة

8.1 شجرة القرار

تعد خوارزمية شجرة القرار خوارزمية مستخدمة على نطاق واسع للتصنيف، والتي تستخدم قيم السمات لتقسيم مساحة القرار إلى مساحات فرعية أصغر بطريقة تكرارية، يمكن تمثيل عمليات اتخاذ القرار مثل كشف الشذوذ بيانياً كشجرة [5].

8.2 الغابة العشوائية

هي مجموعة من أشجار القرار التي تم إنشاؤها من مجموعة البيانات يتم تجميع كل شجرة على حدة لإنتاج تنبؤ فريد بالإجماع على كشف الشذوذ. يتم تمثيل الفكرة الأساسية للغابات العشوائية بشكل تخطيطي في الشكل 1:



شكل1 الفكرة الأساسية للغابة العشوائية

8.3 خوارزمية اقرب جار

تجد الخوارزمية أكثر الملاحظات تشابهاً مع تلك التي يجب أن تتنبأ بها والتي تستمد منها حدساً جيداً للإجابة المحتملة عن طريق حساب متوسط القيم المجاورة، أو عن طريق اختيار فئة الإجابة الأكثر شيوعاً فيما بينها. يمكن لـ KNN التعامل بسهولة مع مئات التسميات [9]. عادة، يعمل KNN على معرفة جيران الملاحظة بعد استخدام مقياس المسافة مثل الإقليدية (الخيار الأكثر شيوعاً)[8] . على سبيل المثال في حال كانت نقطة بيانات معينة يجب التنبؤ بها بأنها شاذة او طبيعية فيتم النظر الى أقرب جيرانها لتصنيف هذه النقطة.

8.4 الانحدار اللوجستي

تقدر الانحدارات اللوجستية احتمالية وقوع حدث ما، مثل التصويت أو عدم التصويت، استنادًا إلى مجموعة بيانات معينة من المتغيرات المستقلة. غالباً ما يستخدم هذا النوع من النماذج الإحصائية (المعروف أيضاً باسم نموذج اللوغاريتم) للتصنيف والتحليلات التنبؤية. نظراً لأن النتيجة هي احتمالية، فإن المتغير التابع محصور بين 0 و1. في الانحدار اللوجستي [18].

8.5 مصنف الانتخاب voting

تم دمج المصنفات الثلاثة الأفضل وهي KNN,RF,DT للحصول على مصنف انتخابي بين هذه الخوارزميات بحيث يتم تصنيف البيانات الشاذة والطبيعة بناء على غالبية الأصوات بدلاً من الاعتماد على خوارزمية واحدة.

9. معايير الأداء

تم الاعتماد على المعايير التالية نظراً لكون المشكلة هي مشكلة تصنيف البيانات على انها طبيعية او شاذة وذلك في مرحلة اختبار الخوارزميات.

- **دقة التصنيف accuracy**

دقة التصنيف هي ما نعنيه عادةً عندما نستخدم مصطلح الدقة. إنها نسبة عدد التنبؤات الصحيحة إلى العدد الإجمالي لعينات الإدخال [10]. وتعطى الدقة بالمعادلة 1:

$$\text{Accuracy}= \frac{\text{number of correct predictions}}{\text{total number of predictions}} \ldots(1)$$

- **مصفوفة الارتباك Confusion Matrix**

مصفوفة الارتباك كما يوحي الاسم تعطي مصفوفة كإخراج وتصف الأداء الكامل للنموذج. يوضح الشكل 2 مصفوفة الارتباك:

		Predicted	
		Negative	**Positive**
Actual	**Negative**	True Negative	False Positive
	Positive	False Negative	True Positive

شكل 2 مصفوفة الارتباك [11]

يمكن حساب دقة المصفوفة بأخذ متوسط القيم الموجودة عبر "القطر الرئيسي" كما هو موضح بالمعادلة 2:

$$\text{Accuracy} = \frac{\text{TruePositive+TrueNegative}}{\text{TotalSample}} \ldots(2)$$

- **الدقة Precision**

هي عدد النتائج الإيجابية الصحيحة مقسوماً على عدد النتائج الإيجابية التي تنبأ بها المصنف كما هو موضح في المعادلة 3، بعبارات أبسط، الدقة هي النسبة بين الإيجابيات الحقيقية وجميع الإيجابيات.

$$\text{Precision} = \frac{\text{TruePositive}}{\text{TotalPredicted Positive}} \ldots(3)$$

- **الاسترجاع Recall**

هو عدد النتائج الإيجابية الصحيحة مقسوماً على عدد جميع العينات ذات الصلة (جميع العينات التي كان ينبغي تحديدها على أنها إيجابية). الاسترجاع هو مقياس النموذج الذي يحدد الإيجابيات الحقيقية بشكل صحيح. رياضياً موضح بالمعادلة 4:

$$Recall=\frac{TruePositive}{TruePositive+FasleNegative} \quad ...(4)$$

- **F1 Score**

F1 Score هو المتوسط التوافقي بين الدقة والاسترجاع. نطاق نقاط F1 هو [0، 1]. يخبر بمدى دقة المصنف(عدد الحالات التي يصنفها بشكل صحيح). رياضياً f1score موضح بالمعادلة 5.

$$F1score=\frac{2*Precision*Recall}{Precision+Recall} \quad ...(5)$$

10. الاعداد التجريبي

يجدر الذكر بأنه تم استخدام جهاز حاسوب محمول بالمواصفات التالية كما يوضح الجدول 2.

جدول 2 مواصفات الحاسوب المستخدم

المواصفة	القيمة
تردد المعالج	2.5 HZ
الذاكرة العشوائية RAM	8 GB
عدد الأنوية	3
جيل الحاسوب	7

.11 التطبيق العملي

11.1 مجموعة البيانات المستخدمة

تم استخدام مجموعة بيانات Metaverse Financial Transactions Dataset توفر مجموعة البيانات هذه المعاملات القائمة على تقنية سلاسل الكتل، بهدف توفير مجموعة غنية ومتنوعة وواقعية من البيانات لتطوير واختبار نماذج الكشف عن الشذوذ، وتحليل الاحتيال[4].

تم تصميم مجموعة البيانات هذه لمجموعة واسعة من الاستخدامات، بما في ذلك على سبيل المثال لا الحصر:

- الكشف عن الشذوذ وتحليل الاحتيال في معاملات سلاسل الكتل.
- البحث في إدارة الأصول الرقمية الآمنة والشفافة.
- تطوير واختبار الخوارزميات لتقييم المخاطر والتحقق من المستخدم.

تتضمن مجموعة البيانات 78600 سجل، يمثل كل منها معاملة بالميزات التالية الموضحة بالجدول 3.

جدول 3 ميزات مجموعة البيانات

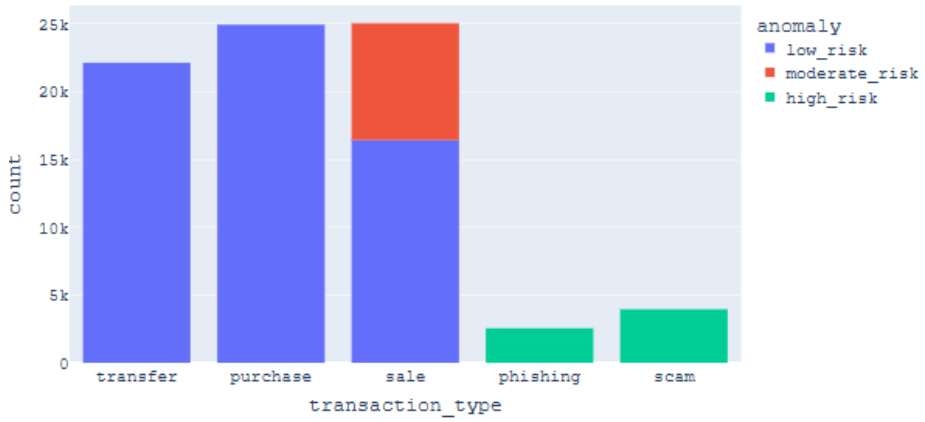
الميزة	الشرح
Timestamp	تاريخ ووقت المعاملة.
Hour of Day	جزء الساعة من الطابع الزمني للمعاملة.
Sending Address	عنوان المرسل.
Receiving Address	عنوان المستقبل.
Amount	مبلغ المعاملة.
Transaction Type	تصنيف المعاملة (على سبيل المثال، التحويل، البيع، الشراء، الاحتيال، التصيد الاحتيالي).
Location Region	المنطقة الجغرافية المحاكاة للمعاملة.
PrefixIP	بادئة عنوان IP المحاكاة للمعاملة.
Login Frequency	تردد جلسات تسجيل الدخول للمستخدم، ويختلف حسب الفئة العمرية.

Session Duration	مدة جلسات النشاط بالدقائق.
Purchase Pattern	النمط السلوكي للمشتريات (على سبيل المثال، مركّزة، عشوائية، عالية القيمة).
Age Group	تصنيف المستخدمين إلى جدد، وراسخين، وقدامى بناءً على تاريخ نشاطهم.
Risk Score	درجة المخاطرة المحسوبة بناءً على خصائص المعاملة وسلوك المستخدم.
Anomaly	تقييم مستوى المخاطرة (على سبيل المثال، مخاطرة عالية، مخاطرة معتدلة، مخاطرة منخفضة).

من ثم تم التحقق من عدم وجود القيم الفارغة والمكررة في مجموعة البيانات.

11.1.1 تحليل البيانات

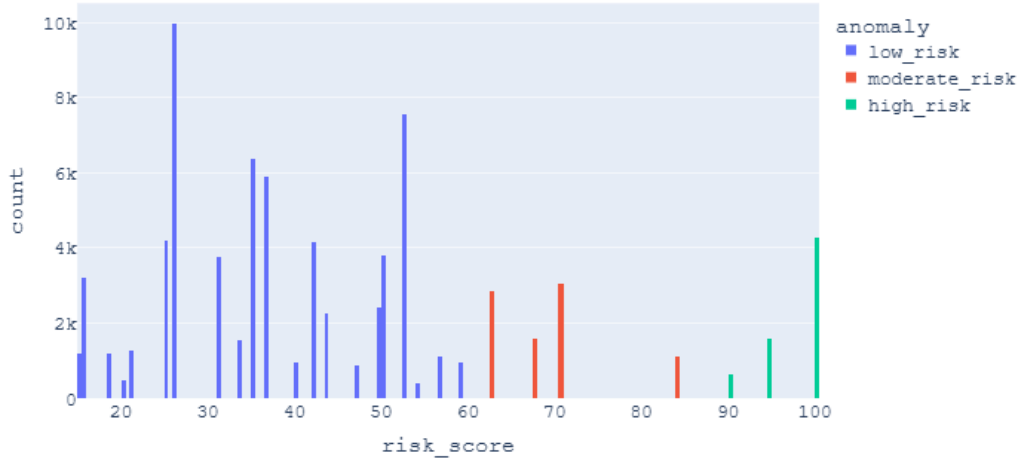
يوضح الشكل 3 أنواع خطورة المعاملات وفق الشذوذ، التصيد والاحتيال من أنواع المعاملات عالية المخاطر، حيث أن حوالي 50% من معاملات البيع تكون ذات مخاطرة متوسطة



شكل 3 انواع خطورة المعاملات وفق الشذوذ

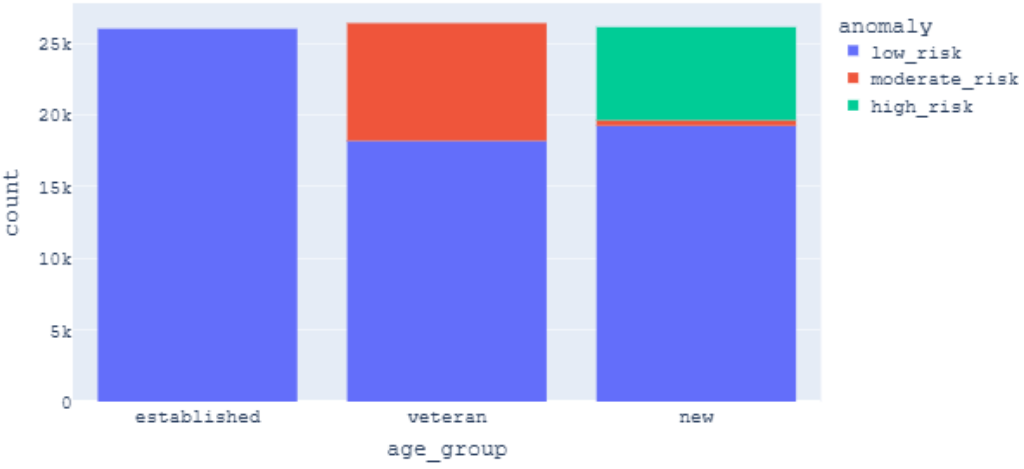
يوضح الشكل 4 درجة خطورة المعاملات (وهي قيمة بين 0 و 100 تشير القيم الدنيا الى ان الخطورة قليلة والقيم العالية على ان الخطورة اكبر وهي قيمة محسوبة بناءً على خصائص المعاملة وسلوك المستخدم وفق ما ورد بوصف مجموعة البيانات بالجدول 3)، أقل من 60 هي معاملات

ذات خطورة منخفضة، وبين 60 و 85 هي معاملات ذات خطورة متوسطة، وأعلى من 85 هي معاملات ذات خطورة عالية.



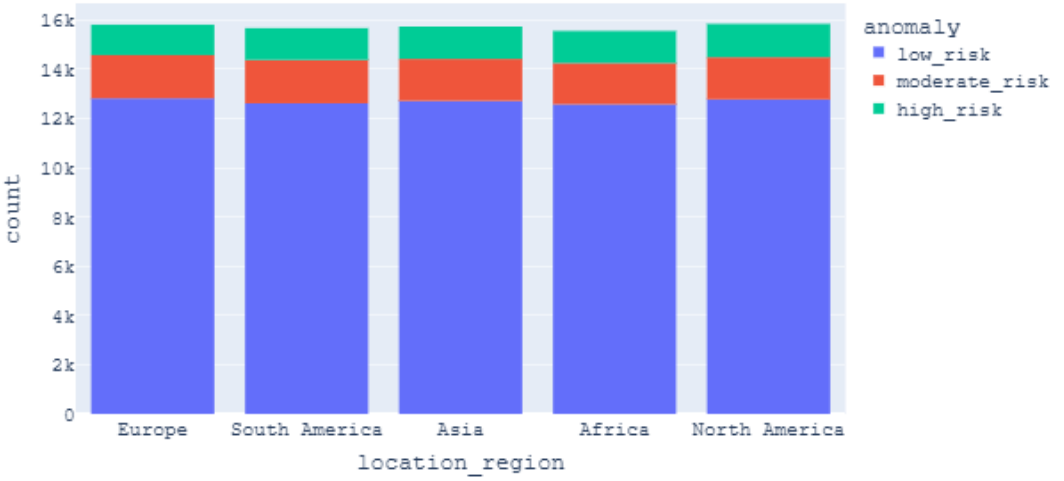
شكل 4 درجة خطورة المعاملات

يوضح الشكل 5 خطورة المعاملة وفق الفئة العمرية، هناك مخاطر عالية للمستخدمين الجدد لإجراء معاملات احتيالية، ومخاطر معتدلة للمستخدمين المخضرمين في حين أن المخاطر منخفضة للمستخدمين الحاليين.



شكل 5 خطورة المعاملة وفق الفئة العمرية

يوضح الشكل 6 خطورة المعاملة وفق المنطقة، يوجد عدد متساوٍ تقريبًا من نقاط البيانات من كل منطقة موقع بها نفس القدر من المخاطر.



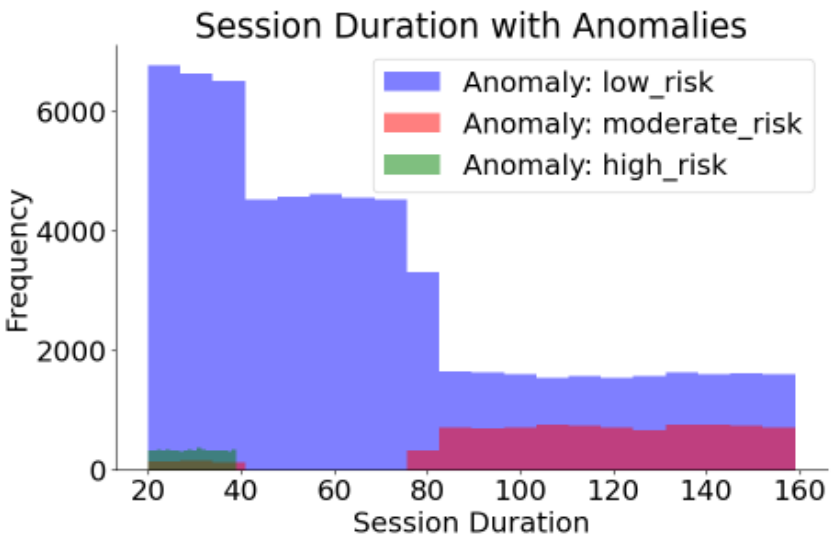
شكل 6 خطورة المعاملة وفق المنطقة

يوضح الشكل 7 خطورة المعاملة وفق مدة الجلسة:

• المعاملات عالية المخاطر لها مدة جلسة قصيرة تتراوح بين 20 إلى 40 دقيقة.

• المعاملات متوسطة المخاطر لها مدة جلسة إما قصيرة (20–40 دقيقة) أو طويلة جدًا (75–160 دقيقة).

• المعاملات منخفضة المخاطر لها علاقة عكسية بمدة الجلسة، فكلما زادت المدة انخفض عدد المعاملات منخفضة المخاطر.



شكل 7 خطورة المعاملة وفق مدة الجلسة

ليتم بعدها إنشاء مجموعة ميزات جديدة لإعطاء وزن للقيم التي تؤثر في التنبؤ بنتيجة المخاطر (risk score) واضافتها الى مجموعة البيانات:

1. تم إنشاء ميزة ثنائية لمعاملات البريد العشوائي والتصيد الاحتيالي (spam, phishing) من الميزة transaction_type وهي:
   - is_phishing_transaction لتحديد إذا ماكانت المعاملة تصيد أم لا.
   - Is_spam_transaction لتحديد إذا ماكانت المعاملة spam أم لا.
2. إنشاء ميزة ثنائية لمعاملات age_group لتحديد المعاملات المرتبطة بالفئات العمرية وهي:
   - is_new_transaction لتحديد إذا ماكانت المعاملة من قبل مستخدمين جدد أم لا.
   - is_veteran_transaction لتحديد إذا ماكانت المعاملة من قبل مستخدمين قدامى أم لا.
3. حساب القيمة العشرية لعنوان IPv4 من الميزة ip_prefix:

- تم تحويل كل ثمانية بتات إلى قيمتها العشرية ثم إضافة كل قيمة عشرية لتحقيق المكافئ العشري لعنوان IP.

يظهر الشكل 8 إضافة مجموعة الميزات الجديدة الى مجموعة البيانات.

age_group	risk_score	anomaly	is_spam_transaction	is_phishing_transaction	is_new_transaction	is_veteran_transaction	ip_prefix_numeric
established	18.75	low_risk	0	0	0	0	3221225472
established	25.00	low_risk	0	0	0	0	2885681152
established	31.25	low_risk	0	0	0	0	3232235520
veteran	36.75	low_risk	0	0	0	1	2885681152
veteran	62.50	moderate_risk	0	0	0	1	2886729728

شكل 8 إضافة مجموعة الميزات الجديدة الى مجموعة البيانات

ثم تطبيق عملية ترميز البيانات على الميزات الفئوية وهي:

- transaction_type
- ip_prefix_numeric
- sending_address
- receiving_address
- age_group

يوضح الشكل 9 مجموعة البيانات بعد عملية الترميز:

age_group	risk_score	anomaly	is_spam_transaction	is_phishing_transaction	is_new_transaction	is_veteran_transaction	ip_prefix_numeric
0	18.75	low_risk	0	0	0	0	3
0	25.00	low_risk	0	0	0	0	1
0	31.25	low_risk	0	0	0	0	4
2	36.75	low_risk	0	0	0	1	1
2	62.50	moderate_risk	0	0	0	1	2

شكل 9 مجموعة البيانات بعد عملية الترميز

وبعدها تمت عملية حذف الميزات التالية:

- age_group: كونه تم الحصول على الميزات الجديدة الخاصة بالفئات العمرية.
- location_region: يوجد عدد متساوٍ تقريباً من نقاط البيانات من كل منطقة موقع بها نفس القدر من المخاطر، وبالتالي يتم إسقاطها لأنها لن تؤثر على التنبؤ (موضح بالشكل 9).

وبعدها عملية تطبيع البيانات للميزات الرقمية باستخدام StandardScaler وهي الميزات التالية:

- Amount
- session_duration

لتصبح بعدها البيانات جاهزة لإجراء التجارب.**11.2 العتبة الموزونة (Threshold Balancing Mechanism – TBM)**

شرح الطريقة (TBM)

تقوم TBMعلى الجمع بين تقنيات موازنة البيانات وتحديد العتبة المثلى للمخاطر في تصنيف المعاملات في سلاسل الكتل على النحو التالي:

- **موازنة البيانات**
  - في البداية، يتم تطبيق تقنيات موازنة البيانات مثل RandomOverSampler، بهدف التعامل مع مشكلة عدم التوازن في البيانات، حيث تميل المعاملات ذات الخطورة العالية (high risk) إلى أن تكون أقل بكثير مقارنة بالمعاملات ذات الخطورة المتوسطة أو المنخفضة.
  - هذه الموازنة تعمل على زيادة تكرار المعاملات ذات الخطورة العالية بحيث تكون متوازنة مع المعاملات ذات الخطورة المتوسطة والمنخفضة، مما يتيح

لنموذج التعلم الآلي فهماً أفضل للأنماط الشاذة المرتبطة بالمعاملات عالية الخطورة.

- **تحديد العتبة المثلى (Threshold)**
  - بمجرد موازنة البيانات، يتم تحديد عتبة الشذوذ بناءً على درجة الخطورة .يتم اعتبار المعاملات التي تقع فوق العتبة المحددة (مثلاً المعاملات التي تتجاوز درجة خطورة 85) كمعاملات شاذة.
  - يتم تحديد هذه العتبة بناءً على أداء المصنفات المختلفة وتجربة أفضل نتائج النماذج عبر التجارب، حيث تكون العتبة التي تُحسن دقة التصنيف و الـ F1 Scoreهي الأنسب.
- **مزايا الآلية**
  - تحسين دقة المصنفات: بتطبيق موازنة البيانات، يمكن تقليل التأثير السلبي للبيانات غير المتوازنة، مما يحسن قدرة النموذج على التعرف على الشذوذ بشكل دقيق.
  - اكتشاف شذوذ أفضل: تحديد العتبة المثلى يساعد على تحسين الكشف عن الشذوذ في المعاملات ذات الخطورة العالية، مما يزيد من دقة تصنيف المعاملات الشاذة.
  - توفير وقت وموارد: من خلال تحسين الأداء باستخدام RandomOverSampler، يمكن تقليل الحاجة إلى معالجات إضافية ومعقدة، مما يحسن الكفاءة العامة للنظام.
- **تطبيق الآلية**
  - المرحلة الأولى: تطبيق RandomOverSampler على البيانات لتوازن توزيع المعاملات.

- المرحلة الثانية: تحديد العتبة المثلى بناءً على التجارب والمقارنات بين دقة المصنفات في حالات مختلفة.
- المرحلة الثالثة: استخدام هذه العتبة لتصنيف المعاملات كـ شاذة أو طبيعية بناءً على درجة الخطورة.

11.3 التجارب

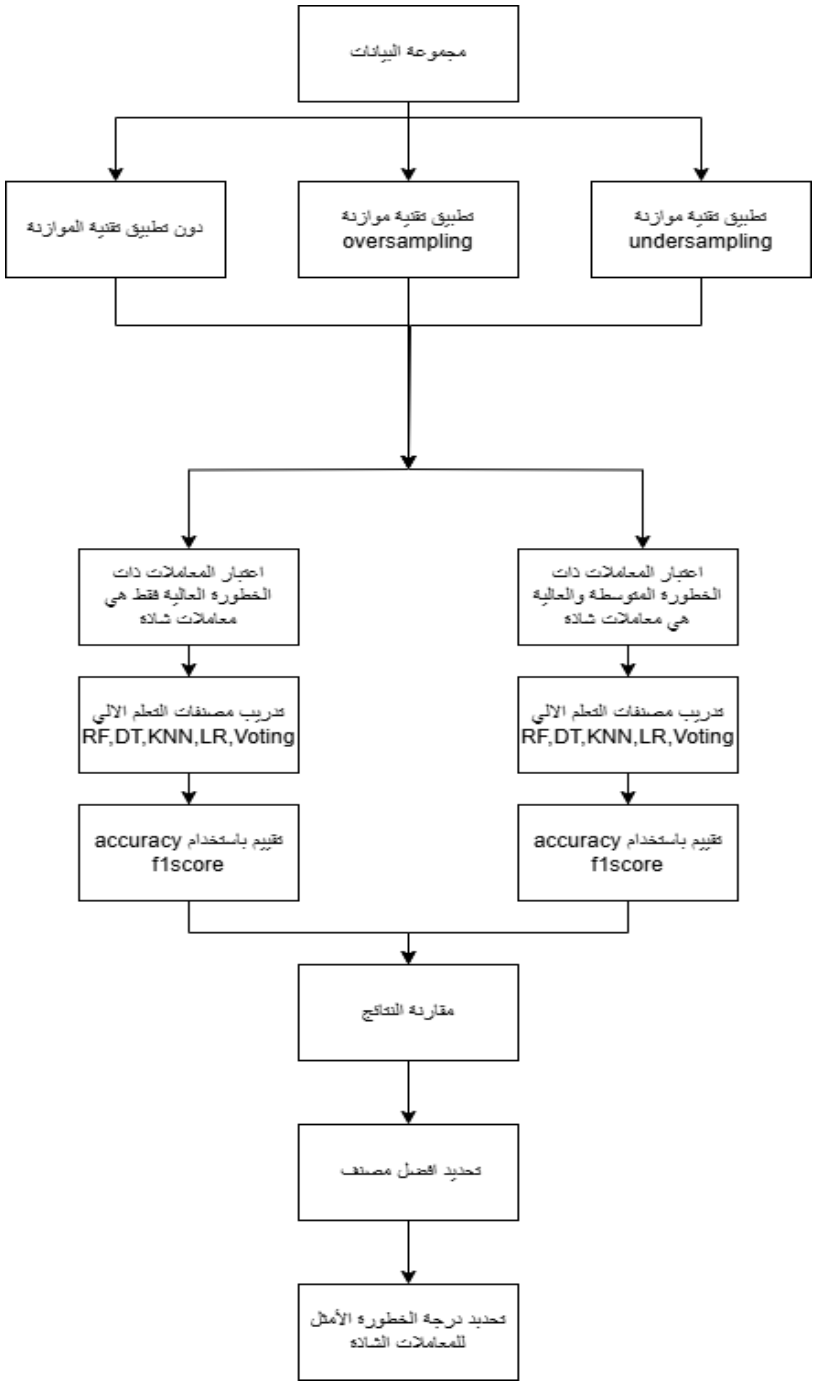
تم إجراء ثلاث تجارب: في التجربة الأولى لم يتم تطبيق أي تقنية موازنة وفي التجربة الثانية تم تطبيق تقنية موازنة البيانات RandomUnderSampler وفي التجربة الثالثة تم تطبيق تقنية موازنة البيانات RandomOverSampler

وذلك من اجل تحديد عتبة الشذوذ الأمثل الشذوذ في سلاسل الكتل.

وفي كل تجربة:

- يتم اعتبار المعاملات التي درجة خطورتها عالية كمعاملات شاذة وتدريب نماذج التعلم الآلي وتقييم اداءها.
- يتم اعتبار المعاملات التي درجة خطورتها متوسطة وعالية كمعاملات شاذة وتدريب نماذج التعلم الآلي وتقييم اداءها.

وبعدها يتم مقارنة أداء كافة المصنفات وتحديد درجة الخطورة الأمثل بناء على نتائج المصنفات، يوضح الشكل 10 تدفق العمل في البحث.



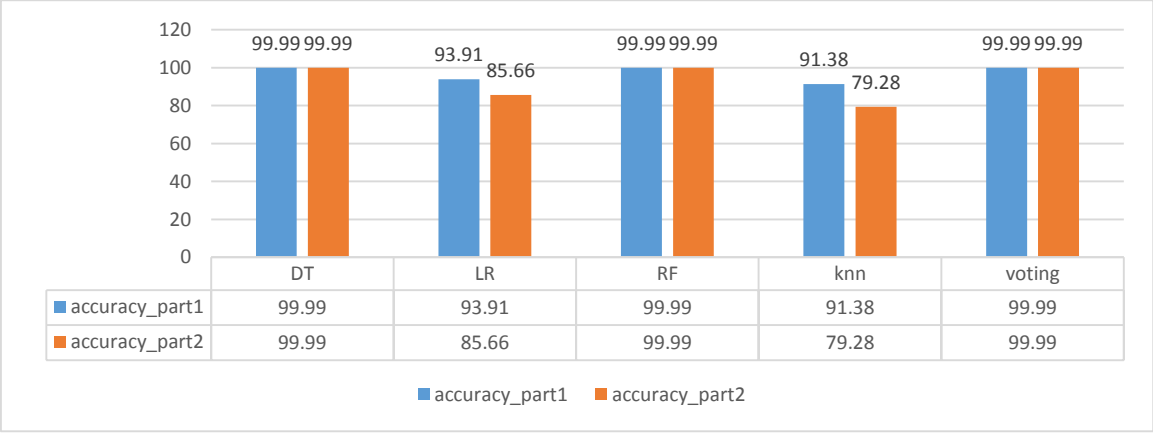
شكل 10 مخطط العمل في البحث

11.3.1 التجربة الأولى

تم استخدام مجموعة البيانات دون تقنيات موازنة

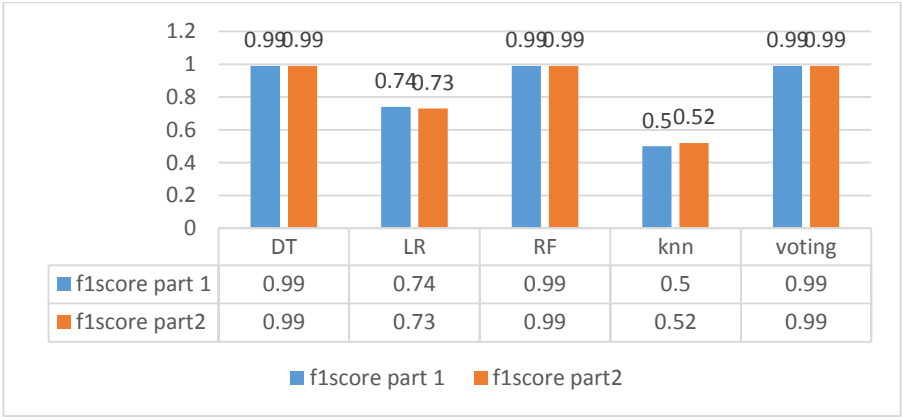
- **على اعتبار ان المعاملات الشاذة هي فقط high risk (في المخطط تمت تسميتها part 1).**
- **على اعتبار ان المعاملات الشاذة هي high risk, mid risk (في المخطط تمت تسميتها part 2).**

يوضح الشكل 11 تجميع دقة المصنفات في التجربة الأولى، **نتائج المصنفات في part 1 هي الأفضل لكن لايمكن الاعتماد على هذا المعيار لوحدة لعدم توازن البيانات**



شكل 11 تجميع دقة المصنفات في التجربة الاولى

يوضح الشكل 12 تجميع f1score للمصنفات في التجربة الأولى **نتائج المصنفات متقاربة في part 1 و part 2.**



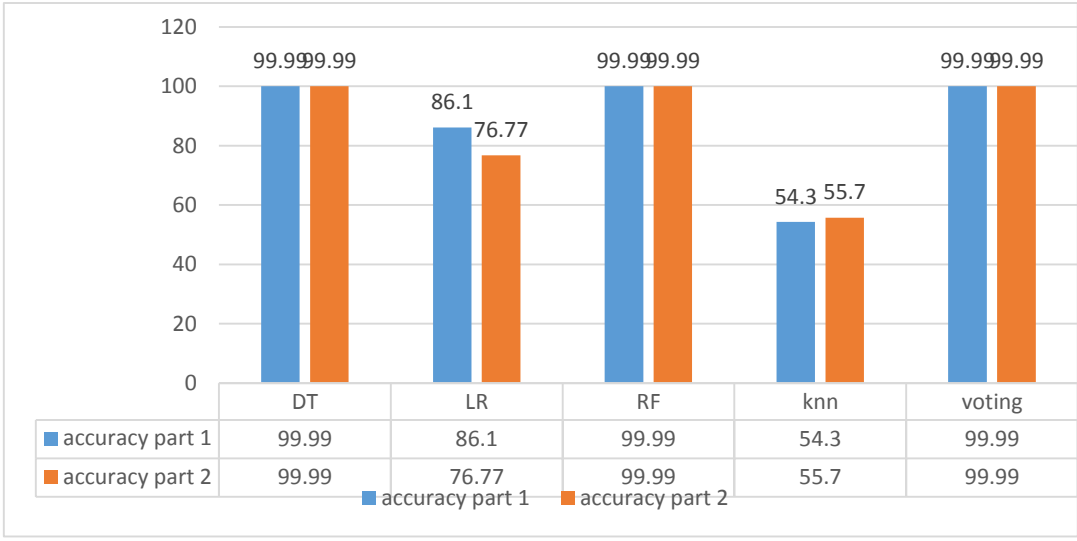
شكل 12 تجميع f1score المصنفات في التجربة الأولى

11.3.2 التجربة الثانية

تم استخدام تقنية موازنة البيانات RandomUnderSampler

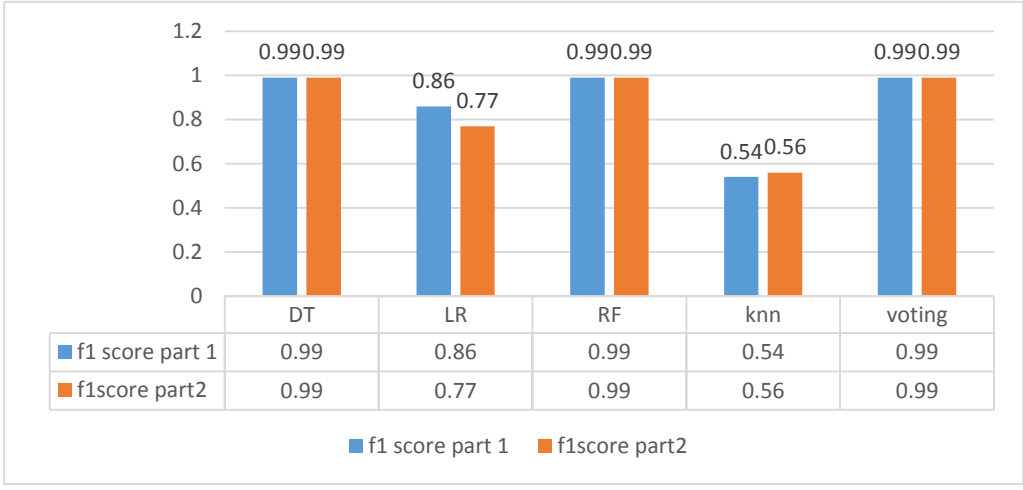
- **على اعتبار ان المعاملات الشاذة هي فقط high risk (في المخطط تمت تسميتها part 1)**
- **على اعتبار ان المعاملات الشاذة هي high risk, mid risk (في المخطط تمت تسميتها part 2)**

يوضح الشكل 13 تجميع دقة مصنفات التجربة الثانية **نتائج المصنفات في part 1 هي الأفضل وتم تحسين الأداء عن التجربة الأولى بالنسبة لخوارزميتي LR , KNN لكن لايمكن الاعتماد على هذا المعيار لوحدة لعدم توازن البيانات.**



شكل 13 تجميع دقة مصنفات التجربة الثانية

يوضح الشكل 14 تجميع f1score للمصنفات في التجربة الثانية، **نتائج المصنفات في part 1 هي الأفضل وتم تحسين الأداء عن التجربة الأولى بالنسبة لخوارزميتي LR , KNN.**



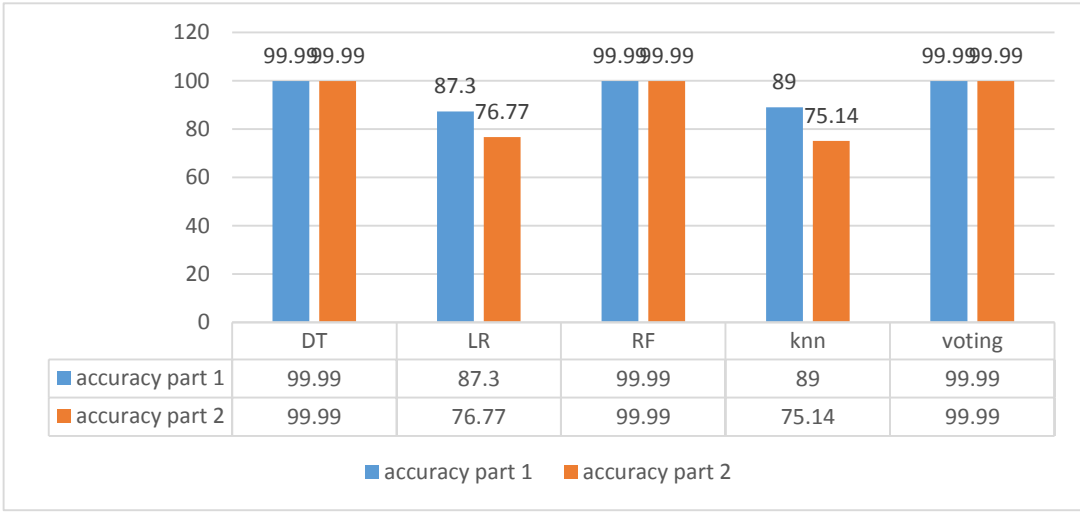
شكل 14 تجميع f1score المصنفات في التجربة الثانية

11.3.3 التجربة الثالثة

تم استخدام تقنية موازنة البيانات RandomOverSampler

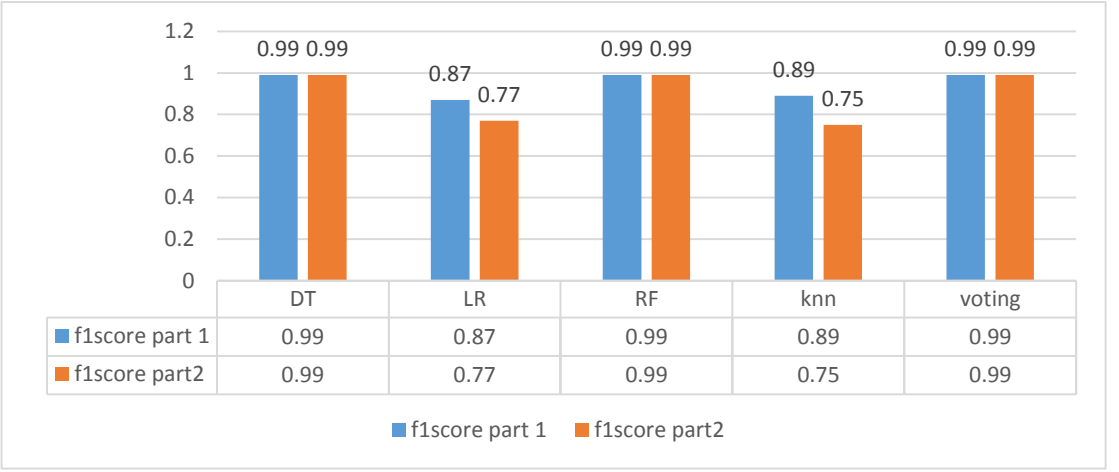
- **على اعتبار ان المعاملات الشاذة هي فقط high risk (في المخطط تمت تسميتها part 1)**
- **على اعتبار ان المعاملات الشاذة هي high risk, mid risk (في المخطط تمت تسميتها part 2)**

يوضح الشكل 15 تجميع دقة مصنفات التجربة الثالثة، **نتائج المصنفات في part 1 هي الأفضل وتم تحسين الأداء عن التجارب السابقة بالنسبة لخوارزميتي KNN , LR**



شكل 15 تجميع دقة مصنفات التجربة الثالثة

يوضح الشكل 16 تجميع f1score لمصنفات التجربة الثالثة، **نتائج المصنفات في part 1 هي الأفضل وتم تحسين الأداء عن التجارب السابقة بالنسبة لخوارزميتي KNN , LR**



شكل 16 تجميع f1score المصنفات في التجربة الثالثة

وبناء على ما سبق تم استنتاج ما يلي:

1. في كافة التجارب السابقة كان أداء كافة المصنفات أفضل على اعتبار ان المعاملات الشاذة هي فقط high risk .
2. في كافة التجارب السابقة كانت مصنفات DT,RF,Voting ذات دقة عالية وصلت لـ 99%.
3. في تجربة موازنة البيانات باستخدام تقنية RandomOverSampler حققت الخوارزميات اعلى نتائج مقارنة ببقية التجارب:

- تم تحسين أداء خوارزمية LR بالنسبة لمعيار f1score بمقدار 0.13 عن التجربة الاولى.
- تم تحسين أداء خوارزمية KNN بالنسبة لمعيار f1score بمقدار 0.39 عن التجربة الأولى.
- تم تحسين أداء خوارزمية LR بالنسبة لمعيار f1score بمقدار 0.01 عن التجربة الثانية.

- تم تحسين أداء خوارزمية KNN بالنسبة لمعيار f1score بمقدار 0.35 عن التجربة الثانية.

4. المعاملات التي درجة خطورتها أعلى من 85 هي المعاملات التي سيتم اعتبارها شاذة وكل ما دون درجة الخطوة هذه يعتبر معاملة طبيعية

12. الخلاصة والعمل المستقبلي

تم في هذا البحث تحديد عتبة للمعاملات الشاذة في سلاسل الكتل باستخدام التعلم الآلي عن طريق تدريب خمس مصنفات وهي شجرة القرار والغابة العشوائية والانحدار اللوجستي وأقرب جار ومصنف الانتخاب بين أفضل ثلاثة خوارزميات على مجموعة البيانات قبل تطبيق تقنيات موازنة عليها وبعد تطبيق تقنيات موازنة البيانات عليها، ومقارنة أداء الخوارزميات باستخدام معيار الدقة accuracy و f1score ، وقد اثبتت النتائج ان أفضل عتبة خطورة للمعاملات الشاذة هي فوق 85 high) risk) وذلك في كافة التجارب المطبقة وخصوصاً في موازنة البيانات باستخدام تقنية RandomOverSampler حيث وصلت الخوارزميات الى اعلى النتائج مقارنة ببقية التجارب فحققت مصنفات شجرة القرار والغابة العشوائية والانتخاب على دقة 99.99 و f1score مساوياً 0.99 وتم تحسين أداء مصنفي الانحدار اللوجستي واقرب جار بالنسبة لمقياس f1score بمقدار يقارب 13 % و 39 % على التوالي.

بالنسبة للعمل المستقبلي من الممكن تطبيق تقنيات التعلم العميق او ادخال عملية هندسة الميزات المتطورة وايضاً دراسة استهلاك الموارد مثل الذاكرة ونسبة استهلاك المعالج والتخزين من قبل هذه الخوارزميات لتحقيق أفضل موازنة بين الأداء واستهلاك الموارد.

13. جدول الاختصارات

AI	**Artificial Intelligence**
DT	**Decision Tree**
KNN	**K-Nearest Neighbor**
LR	**Logistic Regression**
MI	**Machine learning**
NN	**Neural network**
RF	**Random forest**
SGD	**Stochastic Gradient Descent**

المراجع

[1] Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2022). Blockchain for the metaverse: A review. arXiv preprint arXiv:2203.09738.

[2] Nechiti, Alexandru-Tudor. Anomaly Detection in Blockchain Networks. BS thesis. University of Twente, 2023

[3] Pendino, Stephanie R. BLOCKCHAIN NETWORK BEHAVIOR-BASED ANOMALY DETECTION. Diss. Monterey, CA; Naval Postgraduate School, 2019.

[4] https://www.kaggle.com/datasets/faizaniftikharjanjua/metaverse-financial-transactions-dataset

[5] L. Rokach, O. Maimon, Decision trees, in: O. Maimon, L. Rokach (Eds.), "Data Mining and Knowledge Discovery Handbook" , Springer, Boston, MA, pp. 165–192, 2005.

[6]Siddamsetti, S., Tejaswi, C., & Maddula, P. (2024). Anomaly detection in blockchain using machine learning. Journal of Electrical Systems, 20(3), 619-634.

[7] Anthony, Njoku ThankGod, et al. "Anomaly detection system for Ethereum blockchain using machine learning." Proceedings of the 19th International Conference on Manufacturing Research. Vol. 25. IOS Press, 2022.

[8]Introduction to Algorithms for Data Mining and Machine Learning Xin-She Yang Middlesex University School of Science and Technology London, United Kingdom.

[9] John Wiley & Sons, "Machine Learning For Dummies" Published by: New Jersey Media and software compilation 2016

[10] https://towardsdatascience.com/metrics-to-evaluate-your-machine-learning-algorithm-f10ba6e38234

[11] https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9

[12] Ehsan et al., "Enhanced Anomaly Detection in Ethereum: Unveiling and Classifying Threats With Machine Learning," in IEEE Access, vol. 12, pp. 176440-176456, 2024, doi: 10.1109/ACCESS.2024.3504300

[13] Mehra, Sidharth & Hasanuzzaman, Mohammed, "Detection of Offensive Language in Social Media Posts", 2020.

[14] Mohammad Hasan, Mohammad Shahriar Rahman, Helge Janicke, Iqbal H. Sarker, Detecting anomalies in blockchain transactions using machine learning classifiers and

explainability analysis, Blockchain: Research and Applications, Volume 5, Issue 3, 2024, 100207

[15] Shin Morishima, Scalable anomaly detection in blockchain using graphics processing unit, Computers & Electrical Engineering, Volume 92, 2021.

[16] Demertzis, K., Iliadis, L., Tziritas, N., & Kikiras, P. (2020). Anomaly detection via blockchained deep learning smart contracts in industry 4.0. Neural Computing and Applications. doi:10.1007/s00521-020-05189-8

[17] Liang, Wei, et al. "Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems." IEEE Internet of Things Journal 9.16 (2021): 14741-14751

[18] https://www.ibm.com/think/topics/logistic-regression

[19] Ashfaq T, Khalid R, Yahaya AS, Aslam S, Azar AT, Alsafari S, Hameed IA. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors (Basel). 2022 Sep 21;22(19):7162. doi: 10.3390/s22197162. PMID: 36236255; PMCID: PMC9572131.

[20] Ali Yassin, Dr. Kamal Al-Salloum, Dr. Wassim Ramadan Selecting the Optimal Combination of Hyperparameter Tuning and Feature Selection to Improve the Performance of Anomaly Detection Systems Eng. Mechanical, Homs University Journal. Volume 44, Issue 5, 2022

[21] Eng. Ali Yassin, Dr. Kamal Al-Salloum, Dr. Wassim Ramadan, Selecting the Optimal Classification Threshold Dynamically in Early Anomaly Detection Systems Based on Deep Learning, Homs University Journal, Volume 44, Issue 8, 2022.

دراسة تجريبية لتأثير نوع عملية الصقل على السلوك الميكانيكي للفولاذ الكربوني

*م. محسن عدره

ملخص

تتعرض الأجزاء التي تعمل في ظروف تلامس لتدهور ناتج عن ظاهرة التآكل. لذلك، فهي تتطلب مواد ذات خصائص عالية للطبقات السطحية ونطاق تصنيع متقدم للغاية. يمكن لعمليتي الصقل بالكرة والصقل بالدحروج أن تمنحا المادة مظهراً سطحياً جديداً سواء من الناحية الميكروهندسية أو الفيزيائية. يهدف هذا العمل إلى تحديد تأثيرات كل من هاتين العمليتين على خصائص الفولاذ الكربوني. بالإضافة إلى ذلك، تم دراسة تأثيرات مختلف معايير نظام التشكيل على الخشونة والصلابة. حيث أظهرت النتائج أن المظهر السطحي الجديد المطلوب يتميز بمؤشر تقني اقتصادي ملحوظ. حيث تتصرف الطبقات السطحية المعالجة كسطوح مصقولة مع خشونة Ra تتراوح بين 0.22 و 0.9 مايكرومتر ومعالجة بالتصليد مع صلادة HRB تتراوح بين 87 و 90 .هذه التأثيرات المثلى تنتج عن نظام عمل محدد لكل خاصية ولكل عملية. وهذا يسمح بتحسين مقاومة التآكل لهذه الطبقات بنسبة تصل إلى حوالي 98% وتصنيفها كأسطح مصقولة.

كلمات مفتاحية: التشغيل ، الخشونة ، الصلابة ، التآكل ، الصقل بالدحروج، الصقل بالكرة.

- حاصل على شهادة الماجستير 2023 في اختصاص المعدات والآليات –كلية الهندسة التقنية–جامعة طرطوس–سورية

Experimental study of the effect of polishing process type on the mechanical behavior of carbon steel

Abstract

Parts operating in contact conditions are subjected to corrosion-induced degradation. Therefore, they require materials with high surface properties and a very advanced manufacturing range. Ball and roller polishing processes can give the material a new surface appearance both from a micro-engineering and a physical point of view. This work aims to determine the effects of each of these two processes on the properties of carbon steel. In addition, the effects of different farming system parameters on roughness and hardness were studied. The results showed that the required new surface appearance has a remarkable techno-economic index. The treated surface layers behave as polished surfaces with a Ra roughness between 0.22 and 0.9 μm and as hardening-treated with an HRB hardness between 87 and 90. These optimum effects result from a specific working system for each property and each process. This allows us to improve the corrosion resistance of these layers by up to about 98% and classify them as polished surfaces.

Keywords: machining, roughness, hardness, wear, roller polishing, ball polishing.

1 المقدمة:

تعتبر عمليات التشكيل من أهم العمليات التي تستخدم في الصناعة ومن أجل ضمان إنهاء قطعة ما، غالباً ما يتم اللجوء إلى سلسلة من عمليات التشغيل النهائية [1] التي قد تتطلب في بعض الأحيان تكلفة مرتفعة. وبناءً على ذلك، تعتبر الطبقات السطحية، هي الأكثر تعرضاً للإجهاد أثناء الخدمة، وايضاً الأكثر تعرضاً للتآكل نتيجة للتفاعل مع الأجزاء المتزاوجة أو مع البيئة المحيطة[2]. تحت تأثير الاحتكاك، تتعرض هذه الطبقات للتآكل [5–4]. حالياً، يتم فقدان 50٪ من الطاقة المقدمة بسبب الاحتكاك الناتج عن الحركة النسبية بين عناصر الآلات. وفي الوقت الحاضر، تتطلب عمليات التحسين وتعزيز المواد التي تتعرض للإجهاد الشديد استخدام طرق حديثة تشمل المعالجة الميكانيكية مثل الصقل بالدحروج [6]. أو الصقل بالكرة [7]. حيث تعمل هاتان الطريقتان على تطبيق تشوه لدن (التشكيل بالبارد) على الطبقات السطحية، وتؤثران على الخصائص الهندسية والفيزيائية على حد سواء.

تختلف البارامترات المؤثرة على هذه العمليات ، ويمكن تلخيصها عادةً بالعناصر المتعلقة بنظام العمل مثل السرعة، والتغذية، وجهد التشكيل، وعدد التمريرات [11–8–7]. وفي كثير من الأحيان، يتم إدخال بارامترات أخرى مثل: عمق التغلغل [7]، وتوقيت العملية [9]، أو حتى الحالة الأولية للطبقات السطحية [13–12]. كما يتم أحياناً أخذ شكل الأداة وهندستها في عين الاعتبار–7] .14]

تتمحور الاستجابات الناتجة بشكل أكبر حول مظهر السطح [15–8]، وحالة الإجهادات المتبقية على السطح [15–12–9]، وبشكل أكثر تحديداً، مقاومة الطبقات السطحية. حيث أظهرت بعض الدراسات أنه يمكن تحقيق نتائج مثيرة للاهتمام في ظروف معينة فيما يتعلق بالخصائص الميكانيكية مثل خشونة السطح وصلابته [15–14–7] أو مقاومته للتآكل [5]. بالإضافة إلى هذه التأثيرات الإيجابية، فإن الصقل بالكرة والصقل بالدحروج يسببان ضغوطاً متبقية ، حيث يمكن تحديد القيم القصوى على عمق يتراوح بين 40 إلى 200 ميكرومتر [20–18–9]. وهذا يؤدي إلى تحسين جيد

في مقاومة بدء وتطور الشقوق [18]، وبالتالي تحسين في مقاومة التعب بنسبة تتراوح بين 10 إلى 300٪ [19]. ومع ذلك، فإن هذه النتائج مرتبطة ارتباطاً وثيقاً بظروف العمل التي قد تكون محدودة أحياناً بتصميم الأدوات [17]، والمواد المراد معالجتها [18–17]، والحالة الأولية لهذه الطبقات والتي يؤثر عليها فعالية المعالجة [20–7].

2 المواد وطرائق البحث:

2.1المواد

المادة المدروسة هي فولاذ متوسط الكربون. حيث أظهرت التحاليل الكيميائية التركيب الذري لهذا الفولاذ المستخدم.، الجدول (1):

الجدول (1): التركيب الكيميائي للفولاذ متوسط الكربون

العنصر	V	Mo	Ni	Cu	Cr	Fe	P	S	Si	Mn	C
المحتوى (%)	0.51	1.61	0.15	0.08	4.78	0.60	0.021	0.03	0,16	1,25	0,34

وتم أيضاً إجراء اختبار الشد على ثلاثة قضبان من الفولاذ، وذلك بهدف الحصول على بعض القيم للخصائص الميكانيكية من خلال أخذ القيمة المتوسطة. حيث وجدنا أن:

Re = 447,4 MPa, (حد المرونة)

Rr = 612,5 MPa (مقاومة الكسر)

A% = 13,5 % (الاستطالة عند الكسر)

Ex=210 Gpa (معمل يونغ)

من أجل تطبيق عملية التلميع، تم تحضير قضبان أسطوانية من خلال عملية الخراطة باستخدام أداة قطع من كربيد معدني من درجة M20 .حيث يتميز السطح الناتج من عملية الدوران بخشونة (Ra = 1.9–3.64 μm) وصلادة(HRB = 80–86) ، بعد الدوران يتم تقسيم العينة إلى جزئين. الجزء الثاني مخصص، حسب الحالة، لخضوعه لعملية الصقل بالكرة أو الصقل بالدحروج. وأخيراً، يتم تطبيق اختبار التآكل على كل من الجزئيين.

2.2 الأجهزة والطرق التشغيلية:

2.2.1 جهاز المعالجة الميكانيكية

يمكن تنفيذ عمليات الصقل بالكرة والصقل بالدحروج باستخدام جهاز واحد مصمم خصيصاً لهذا الغرض؛ حيث يتم تغيير الجزء النشط فقط حسب الحالة. يتميز هذا الجهاز ببساطة التركيب على البرج في آلة الخراطة العامة الشكل (a–1)، وبناءً على ذلك، فإن الصقل بالكرة باستخدام رأس ماسي بنصف قطر rp = 1.5mm يحاكي عملية الخراطة؛ ويتم الحصول على حركة التشكيل من خلال تدوير القطعة، بينما يتم نقل حركة التقدم إلى الأداة عبر النقل الطولي الشكل (b–1)، بالمقابل فإن الصقل بالدحروج يتم باستخدام الأسطوانة الدوارة بقطر dG = 36mm ، فيحاكي عملية التنعيم الأسطواني؛ وبالتالي، يتطلب أيضاً حركة دورانية للأسطوانة. في كلا الطريقتين، يتمثل حركة التوغل في تأثير الرأس الماسي أو الأسطوانة الدوارة التي تمارس على القطعة جهداً P من التشكيل يتم ضبطه مسبقًا على الجهاز بالاضافةالى ذلك يتم تنفيذ التلميع، تمامًا مثل التشكيل، في ظروف تزييت وفقاً لنظام موصى به يعتمد على الصلابة الأولية. حيث بارامترات هذا النظام موضحة في الجدول (2) .

لتقدير تأثير هذه البارامترات، تم إجراء الاختبارات تحت أنظمة مختلفة، حيث تُحدد مجموعة البارامترات الجدول (3) بواسطة طريقة التخطيط متعددة العوامل للتجارب.

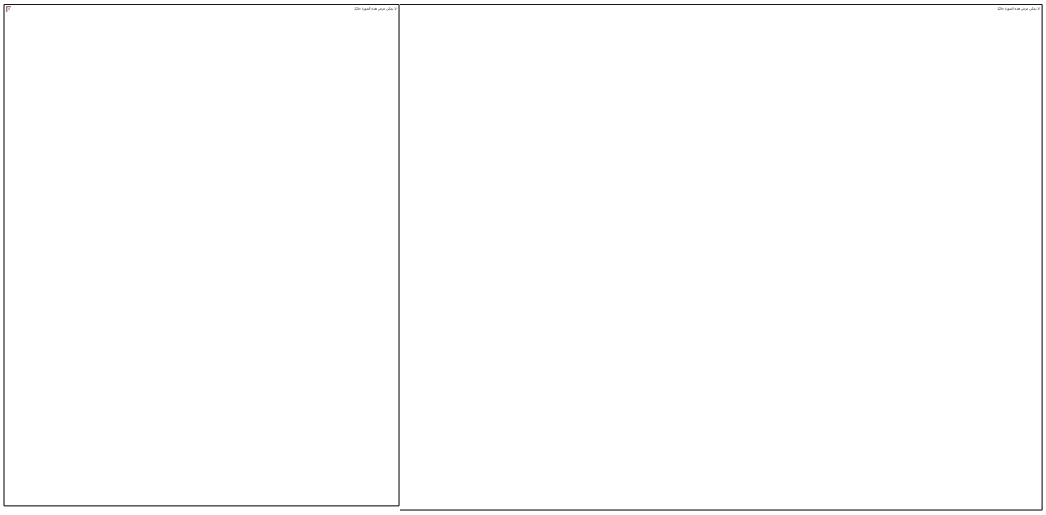
2.2.2اختبار التآكل

الغرض من هذه الاختبارات هو تقدير مقاومة المادة للتآكل بعد عملية التفريز أو بعد خضوعها لإحدى عمليات التشكيل. يحدث ظاهرة التآكل من خلال التآكل الثلاثي، حيث يتم حقن جزيئات من المادة الكاشطة، المنقولة بواسطة زيت التشحيم، في منطقة التلامس بين الأداة والقطعة. حيث تجرى الاختبار على مخرطة موازية باستخدام جهاز كما يبين في الشكل (2) ، مزود بمحمل يطبق ضغطاً خفيفاً على القطعة. بمجرد تأسيس التلامس، يتم تشغيل المحمل لتدويره، مما يتسبب في احتكاك مع القطعة التي تم تحديد سرعة تدويرها عند 500 دورة في الدقيقة. في كل اختبار، يتم ضبط الوقت وقياس وزن العينة باستخدام ميزان دقيق.

يتم تسجيل فقدان الكتلة Δm على السطح، والذي يمثل الفرق بين الكتلة m_{i-1} قبل الاختبار و m_i بعد الاختبار. يتم تقييم القيمة التراكمية لـ Δm باستخدام العلاقة:

$$\Delta m = m_{i-1} - m_i + \Delta m_{i-1}$$

تُميز قيمة Δm فعلياً التآكل الناتج عن تلامس الأداة–المادة الكاشطة–القطعة خلال فترة زمنية محددة. وقد تم اختيار العينات المستخدمة في اختبارات التآكل بناءً على أفضل قيم الخشونة والصلابة الناتجة عن كل من عمليتي التشكيل.

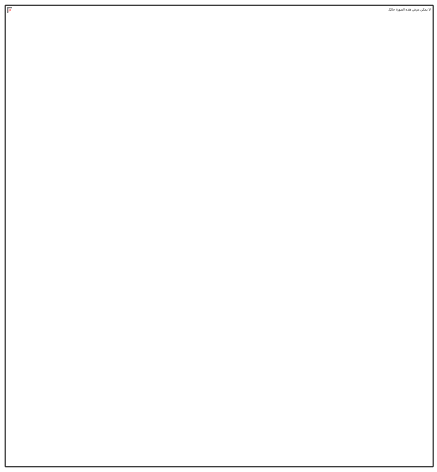


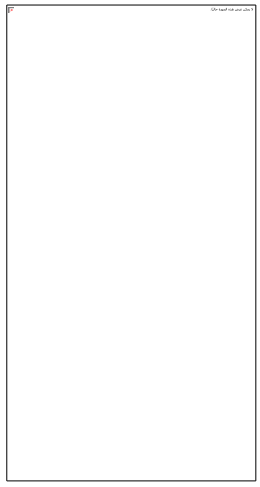
الشكل (1). جهاز التشكيلa) صورة لتركيب الجهاز على المخرطة، b) مخطط عملية التلميع: 1–قضيب؛2–الماسك؛3–الجسم؛4–غلاف التوجيه؛5–الزنبرك؛6–المكبح؛7–برغي التعديل؛8–اللوح.

الجدول (2). أنظمة العمل في المعالجة الميكانيكية.

الأختبار N	بارامترات				
	V(m.min−1)	n (tr.min−1)	P (kgf)	f (mm.tr−1)	l (شوط)
1	10	180	20	0,075	2
2	45	710	20	0,075	2
3	80	1000	20	0,075	2
4	45	710	20	0,05	2

5	45	710	20	0,075	2
6	45	710	20	0,100	2
7	45	710	05	0,075	2
8	45	710	15	0,075	2
9	45	710	20	0,075	2
10	45	710	15	0,075	1
11	45	710	15	0,075	2
12	45	710	15	0.075	3





الشكل (2). جهاز اختبار التآكل. 1) الجسم؛ 2) الحلقة؛ 3) المحمل؛ 4) الحلقة؛ 5) واشر التثبيت؛ 6) صامولةM8 ؛ 7) المحور؛ 8) صامولةM8 ؛ 9) واشر

3 .النتائج

3.1 تأثيرات المعالجات

المظهر الأولي للطبقات السطحية هو نتيجة عملية الخراطة، حيث تم تحديد نظام القطع الأمثل باستخدام التحجيم لتحقيق خشونة أولية قدرها 3.2 ميكرومتر. تعتبر هذه الحالة الجيومترية موصى بها [7]. ولذلك لتحقيق أفضل فعالية للمعالجة. وبناءً على ذلك، قدّمت التوليفات المختلفة للبارامترات المعالجة خشونة Ra تتراوح بين 0.22 و0.9 ميكرومتر وصلابة HRB تتراوح بين 87 و90 كما يوضح في الجدول (3). وبناءً على ذلك، فإن أقصى تأثير يتم تحقيقه على كل من الخصائص المذكورة كما يوضح في الشكل (3)، بينما النظام يتطلب عمل محدد لكل معالجة.

من خلال عملية الصقل بالكرة، ومع ثبات السرعة $V = 45\ m.min^{-1}$،والجهد $P = 15\ daN$، وسرعة التغذية $f = 0{,}075\ mm.tr^{-1}$، حيث تتيح المعالجة بثلاث تمريرات تحسين الصلابة بنسبة تقارب 10−12%. بالمقابل، إذا تم تقليص المعالجة إلى تمريرين فقط، فإن الخشونة Ra تتحسن بنسبة تقارب 70%.

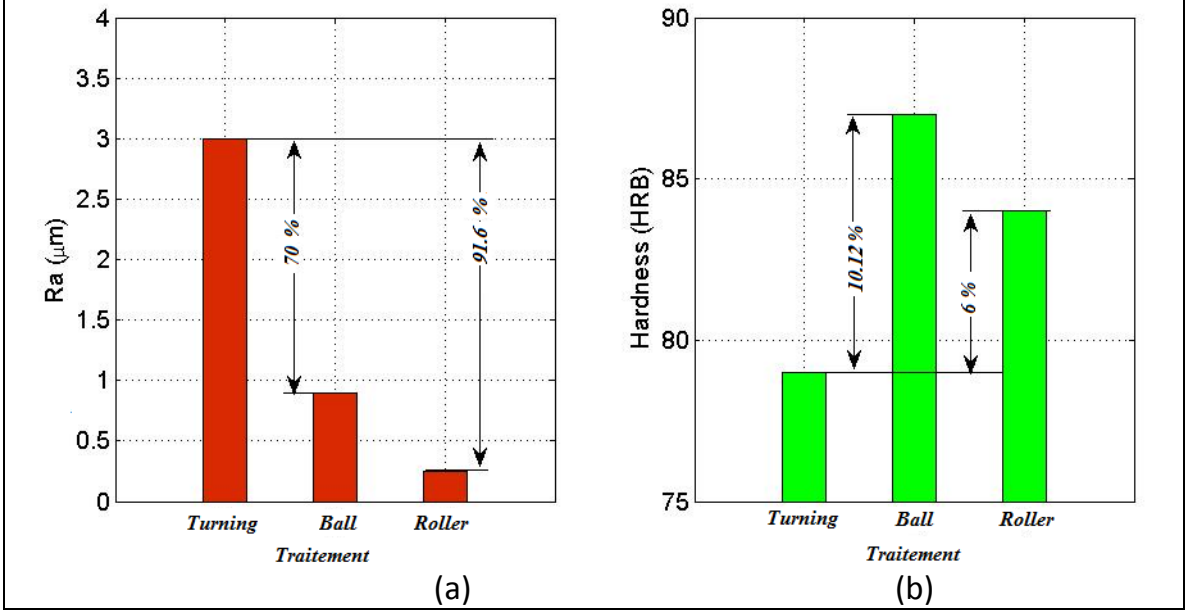
في حالة التدوير، يعتبر النظام الأكثر فائدة من حيث Ra وHRB هو أيضاً محدد بواسطة القيم المتوسطة لـ V و f ،وبناءً لذلك عند دمج هذه القيم مع جهد قدره 20 daN في تمريرين (شوطين)، تتحسن الخشونة بنسبة 92%. وعلى العكس، عندما يتم تقليص جهد التشكيل إلى 15daN ويزداد عدد الأشواط إلى ثلاث، فإن الصلابة تزيد بنسبة تصل إلى 6%.

الجدول (3) . تأثير الصقل يالدحروج و الصقل بالكرة على الخشونة والصلابة

N	Ra [µm]					[HRB]				
	بعد الخراطة	بعد الصقل بالكرة	الفرق (%)	بعد الصقل بالدحروج.	الفرق (%)	بعد الخراطة	بعد الصقل بالكرة	الفرق (%)	بعد الصقل يالدحروج	الفرق (%)
1	2,4	1,9	20,83	0,32	86,66	82	87	6,09	86	4,87

2		1,6	33,33	0,29	87,91		85	3,65	85	3,65
3		1,5	37,50	0,22	90,83		84	2,43	84	2,43
4		1,1	38,88	0,22	87,77		89	7,22	85	2,40
5	1,8	1,4	22,22	0,25	86,11	83	85	2,40	85	2,40
6		1,6	11,11	0,37	79,44		84	1,20	85	2,40
7		1,1	63,33	1,84	38,66		85	2,40	83	0,00
8	3,0	0,9	70,00	0,39	87,00	83	86	3,61	85	2,40
9		1,1	63,33	0,25	91,66		90	8,43	87	4,82
10		1,8	05,26	0,46	75,78		84	6,32	82	3,79
11	1,9	1,4	26,31	0,30	84,21	79	85	7,60	83	5,06
12		1.3	11,40	0,24	87,36		87	10,12	84	6,32

الصقل بالكرة: $V=45m/mn$ ، $f=0,075mm/tr$ ، $i=3$ ،$P=15kgf$ الصقل بالدحروج: $V=45m/mn$ ، $i=3$ ، $P=15kgf$ ،$f=0,075mm/tr$	الصقل بالكرة : $V=45m/mn$ ، f , $i=2$ ، $P=15kgf$ =0,075mm/tr, الصقل بالدحروج: $V=45m/mn$ ، f , $i=2$ ، $P=20kgf$ ، =0,075mm/tr



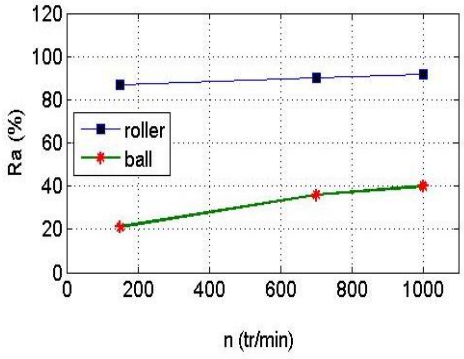
الشكل (3). تأثير عمليات التشكيل على: الخشونة و القساوة

3.2 تأثير نظام المعالجة

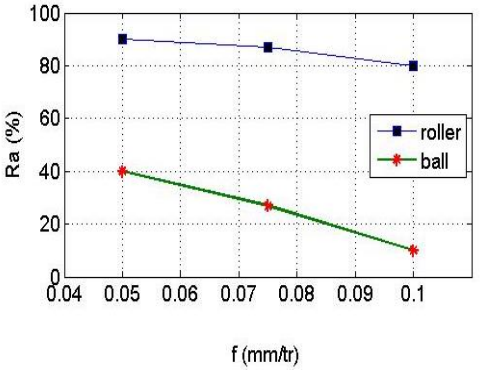
يوضح الشكل (4)تأثير البارامترات المعالجة على معدل زيادة الخشونة بعد تطبيق الطريقتين. حيث الطريقتان تتأثران بشكل ضئيل بتغير تردد الدوران أو سرعة التقدم كما هو مبين في الشكل (4– a, b)، على الرغم من أن زيادة التقدم تقلل من فعالية الصقل بالكرة. إن زيادة جهد التشكيل وعدد التمريرات أثناء الصقل يالدحروج كما يبين الشكل (4–c–d) ، حيث تعزز بشكل أكبر من المظهر الهندسي للسطح، وهذه التحسينات تكون أقل وضوحاً أثناء الصقل بالكرة. لذا، لا يُفضل زيادة هذين المعلمين بشكل مفرط لتجنب تقليل فعالية الصقل بالكرة. بالإضافة يوضح الشكل (5) المنحنيات التي تأثير البارامترات نظام المعالجة على الصلابة تتشابه في كلا الطريقتين. ومن تحليل هذه المنحنيات يتبين أن معدل زيادة الصلابة ينخفض مع زيادة تردد الدوران ، الشكل (5–a) أو حتى

سرعة التقدم كما يوضح في الشكل (5–b) .بالمقابل، تساهم زيادة جهد التشكيل كما في الشكل (5–c)وعدد التمريرات الشكل (5–d)في تحسين الصلابة، وتكون هذه التحسينات أكثر وضوحاً بعد الصقل بالكرة.

f = 0,075mm/tr ; P = 20 daN ; i = 2 Rai = 2,4µm	***n = 710 tr/min ; P = 20 daN ; i = 2 Rai = 1,8µm***

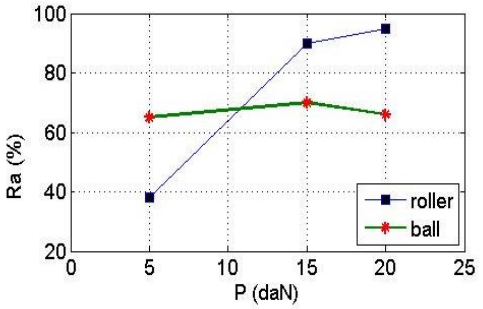


(a)

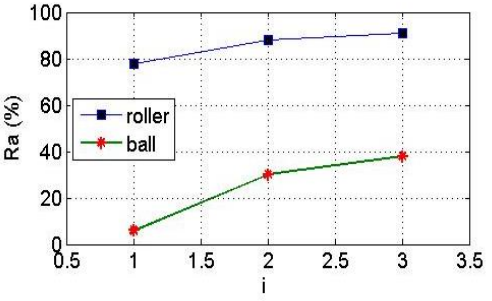


(b)

n = 710 tr/min ; f = 0,075 mm/tr ; i = 2 Rai = 3µm	***n=710 tr/min; f=0,075 mm/tr;P=15 daN Rai = 1,9 µm***

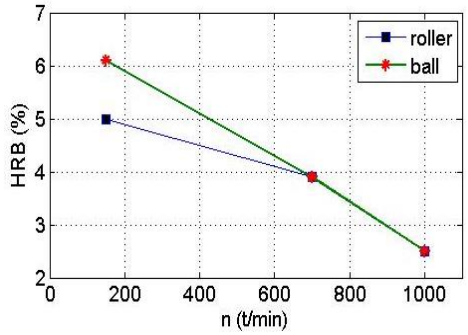
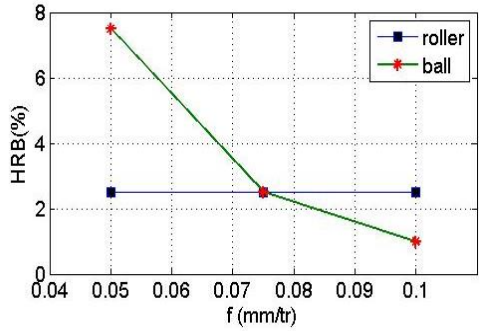
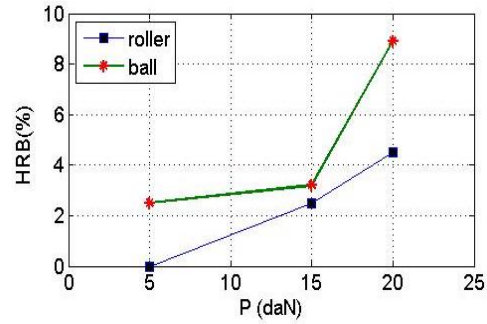
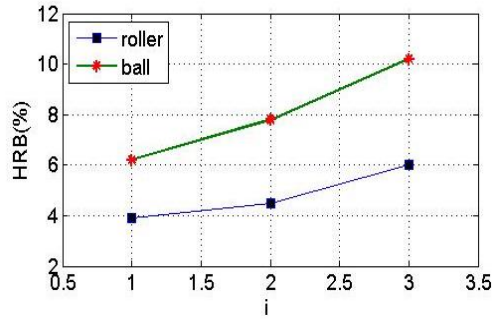


(c)



(d)

الشكل (4). تأثير عناصر نظام المعالجة على نسبة تحسن الخشونة

f = 0,075 mm/rev ; P = 20 daN ; i = 2 ***HRBi = 82***	***n = 710 tr/min ; P = 20 daN ; i = 2*** ***HRBi = 83***
 (a)	 b
n = 710 tr/min ; f = 0,075 mm/tr ; i = 2 ***HRBi= 3µm***	***n=710 tr/min;f=0,075mm/tr;P=15 daN*** ***HRBi = 79***
 (c)	 (d)

الشكل (5) . تأثير عناصر نظام المعالجة على نسبة تحسن القساوة

3.3 مقاومة التآكل

تم إجراء التجارب لمدة محددة قدرها 60 دقيقة، حيث كانت الخسارة النسبية في الكتلة ($\Delta m/m_0$) المسجلة على العينات في الحالة المدورة تتراوح بين 1.94% و3.32%. بعد التدوير، كانت خسارة الكتلة تمثل 0.21% كما يبين في الجدول (4) ، بينما بعد الصقل بالكرة انخفضت هذه النسبة إلى 0.05% كما يبين في الجدول (5). في هذه الحالة، تحسن كل من الطريقتين في مقاومة التآكل،

مع كون التحسن أكثر وضوحاً في الصقل بالكرة 98% مقارنة بالصقل التدحرج 89% كما في الشكل (6)،بينما يوضح الشكل (7) تطور التآكل مع مرور الوقت، بينما تكشف منحنيات التآكل عن القوانين الكلاسيكية للتآكل، حيث يمكن تسليط الضوء على المراحل الثلاث الكلاسيكية للتآكل.

المرحلة الأولى، التي تتميز بصقل نتوءات الخشونة، تظهر حتى الدقائق العشرين الأولى من التجربة، وهذه المرحلة تكون أكثر تسارعاً أثناء الصقل بالدحروج. المرحلة الثانية تمثل التآكل النظامي الطبيعي، حيث يتطور بشكل أكثر أو أقل وفقاً لقانون خطي. المرحلة الثالثة تميز نفسها بعد مرور 60 دقيقة من التجربة، حيث تتسارع خسارة الكتلة بشكل ملحوظ، مما يشير إلى أن التآكل دخل في نطاقه الكارثي. مما تؤدي الى تتدهور المادة بشكل شديد عند ملامستها للأداة.

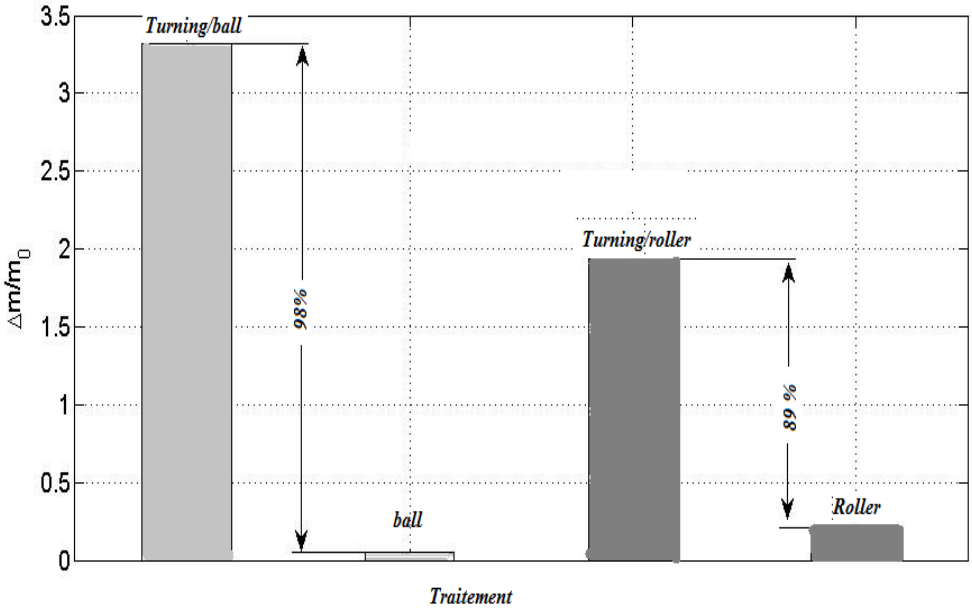
الجدول (4). نتائج اختبارات التآكل بعد الصقل بالدحاريج

N ◦	Δti [min]	t_{i-1} + Δt [min]	m_i (g)	Δm_i (g)	$\Delta m_i/m_0$ (%)	m_i (g)	Δm_i (g)	$\Delta m_i/m_0$ (%)
			خراطة m_0 = 77,8380 g			صقل الدحاريج m_0 = 78,0053 g		
01	10	10	77,4960	0,3420	0,440	78,0024	0,0029	0,004
02	5	15	77,3496	0,4884	0,627	78,0010	0,0043	0,005
03	5	20	77,0960	0,7420	0,953	77,9472	0,0581	0,074
04	5	25	77,0842	0,7538	0,970	77,9335	0,0718	0,092
05	5	30	76,9790	0,8590	1,103	77,9243	0,0810	0,104
06	10	40	76,8520	0,9860	1,266	77,9001	0,1052	0,134
07	5	45	76,4350	1,4030	1,802	77,8947	0,1106	0,142

08	5	50	76,4240	1,4140	1,816	77,8625	0,1428	0,183
09	5	55	76,3974	1,4406	1,850	77,8909	0,1444	0,185
10	5	60	76,3231	1,5149	1,946	77,8380	0,1673	0,214

الجدول (5). نتائج اختبارات التآكل بعد الصقل بالكرة

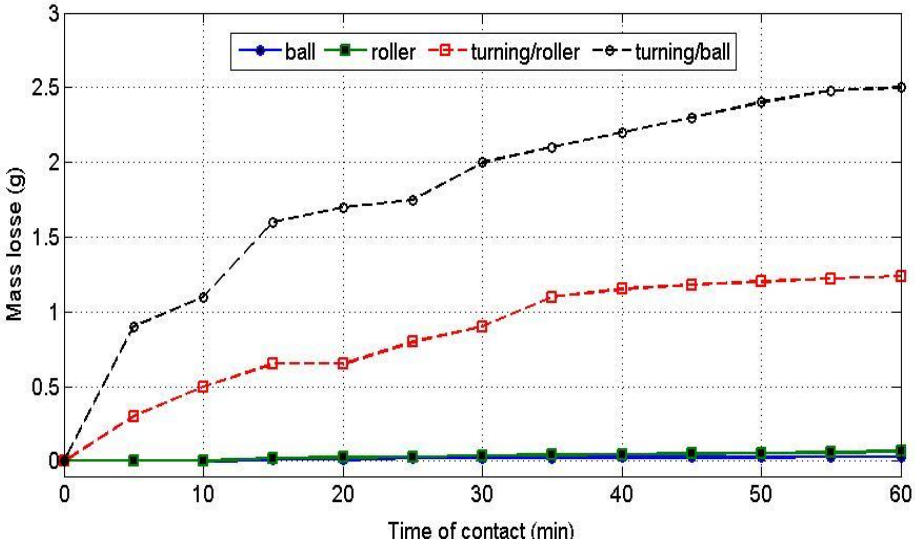
N°	Δt_i [min]	$t_{i-1} + \Delta t$ [min]	m_i (g)	Δm_i (g)	$\Delta m_i/m_0$ (%)	m_i (g)	Δm_i (g)	$\Delta m_i/m_0$ (%)
			m0 = 71,8800 g : خراطة			m0 = 71,9180 g : صقل بالكرة		
01	10	10	70,9850	0,8950	1,245	71,9153	0,0027	0,004
02	5	15	70,6820	1,1980	1,666	71,9129	0,0051	0,007
03	5	20	70,1933	1,6867	2,346	71,9123	0,0057	0,008
04	5	25	70,0831	1,7969	2,500	71,9104	0,0076	0,010
05	5	30	70,0725	1,8075	2,514	71,9100	0,0080	0,011
06	10	40	69,9730	1,9070	2,653	71,9097	0,0083	0,011
07	5	45	69,7402	2,1398	2,977	71,9031	0,0149	0,021
08	5	50	69,6402	2,2398	3,116	71,8980	0,0200	0,028
09	5	55	69,5382	2,3418	3,258	71,8913	0,0267	0,037
10	5	60	69,4892	2,3908	3,326	71,8800	0,0380	0,053



الشكل (6). تأثير المعالجة على مقاومة التآكل.

الصقل بالكرة: i=2 , P=20 daN, f = 0,05mm/tr, V = 10m/mn

الصقل بالدحروج: i=2 ,P=20 daN, f = 0,05mm/tr, V = 10m/mn



الشكل (7). تطور فقدان الكتلة مع مرور الوقت. نظام المعالجة

4 المناقشة:

4.1 تحليل النتائج

تعمل عمليات التشكيل على تنفيذ التشوه اللدن للطبقات السطحية وتعديل بعض الجوانب الفيزيائية والهندسية لهذه الطبقات. يؤدي هذا التشوه إلى تسوية قمم الخشونة الناتجة عن التشغيل الميكانيكي لملء تجاويف والأخاديد. بشكل أفضل. هذه القمم التي تم تسويتها بفعل مرور الأدوات تترك خلفها سطحاً مصقولاً تماماً بخشونة مماثلة لتلك التي توفرها عمليات التشغيل النهائية التقليدية.

تعتبر أهمية نصف قطر الصقل التدحرج مقارنة بنصف قطر أداة الصقل بالكرة ومساحة التلامس بين الأداة والقطعة من العوامل التي تجعل الكرة أكثر فعالية في تسوية الخشونة وتحسين حالة السطح (تقليل Ra بحوالي 90 %)هذا التحسن يكون أقل وضوحاً عند الصقل بالكرة، حيث كانت نسبة تقليل الخشونة حوالي 70%. في الواقع، فإن طرف الأداة الماسي يتفاعل مع القطعة بطريقة مشابهة لأداة القطع، ويكون تأثير التطبيق الموضعي للأداة أقل فعالية مقارنة بالصقل بالكرة. كما

يتضح من تحليل النتائج أن الحصول على خشونة مثالية يعتمد على حالة السطح الأولية (نتيجة عملية الدوران) وأيضاً على النظام الخاص المطبق أثناء المعالجة.

في الواقع، أفضل النتائج التي توفر أقل خشونة قبل وبعد المعالجة تم تسجيلها عندما كانت خشونة السطح الأولية حوالي 3 ميكرومتر الشكل (a–3)، وهي قيمة تتوافق مع القيم التي أوصت بها بعض الدراسات

[7–11]. وهذا ينطبق على كل من الصقل بالكرة والصقل بالدحروج.

للحصول على خشونة سطح مثالية، تختلف الأنظمة الخاصة بكلا العمليتين فقط في اختيار قوة التشكيلP حيث يتم تحقيق أفضل تأثير عند قوة 15 daN أثناء الصقل بالدحروج الشكل (4– c). يبدو أن مساحة التلامس الصغيرة بين الأداة والقطعة أثناء الصقل بالكرة تسهم في زيادة اختراق الأداة للقطعة مع زيادة قوة .P وبالتالي، تزداد صلابة القطعة نتيجة لارتفاع معدل التصليد الناجم عن التشوه للطبقات السطحية. يؤدي تصلب السطح إلى تدهوره عن طريق التقشر عند تلامس الأداة، مما يغير من مظهره الذي يحتفظ رغم ذلك بميزة كونه أفضل مقارنة بالحالة الأولية.

أثناء الصقل بالدحروج، تساهم عرض البكرة في زيادة مساحة التلامس مما يؤدي إلى تقليل ضغط التلامس من جهة ومن جهة أخرى إلى تدفق منتظم الأخدود إلى التجاويف. من هذه التأثيرات، ينتج سطح ذو خشونة منخفضة. ومع ذلك، طالما أن قوة التشكيل منخفضة(P < 10 daN) يظل الصقل بالكرة الأداة الأكثر فائدة من حيث الخشونة. لذلك، يظهر الشكل (c–4) تداخلًا بين العمليتين.

بالمقابل يساهم زيادة معدل الدوران ضمن نطاق السرعات المختار في زيادة معدل تحسين الخشونة الشكل (a–4). حيث أن درجة الحرارة في منطقة التشكيل تزداد مع السرعة قبل أن تستقر في لحظة معينة. حيث تميل الطبقات السطحية إلى اكتساب مظهر أكثر لزوجة مما يقلل من الاحتكاك بين الأداة والقطعة وبالتالي تتحسن الخشونة أكثر. يتم الحصول على أفضل نتيجة في الصقل بالكرة نظرًا لصلابة الأداة أثناء العمل. ومع ذلك، فإن زيادة معدل الدوران غير مرغوبة بعد حد معين بسبب عدم استقرار الأداة، وانخفاض التشوه اللدن، وعدم كفاية وقت التزييت [15]، بالإضافة إلى ظاهرة الاهتزاز التي تتسبب في تدهور السطح[14]. إذ إن زيادة سرعة التقدم كما في الشكل (4–

b) تزيد من مسافة الخطوط الناتجة عن أداة التشغيل، مما يؤدي إلى تدهور الخشونة. يتأثر معدل التحسن بشكل أكبر بانخفاض الخشونة أثناء عملية الصقل بالكرة. في هذه الحالة، يوفر التشكيل بالدرفلة أفضل النتائج بفضل شكل الأداة (وبالتالي الاتصال بين الأداة والقطعة)، والذي يعمل بطريقة توليد خطيّة وحركة دوران إضافية للجزء النشط من الأداة، مما يساهم في تسوية أفضل للخشونة. بالإضافة الى زيادة عدد التمريرات تساهم في تحسين معدل تحسين الخشونة الشكل (4–d). يبدو أن تأثير عدد التمريرات مشابه لتأثير جهد التشكيل. ومع ذلك، ليس من المستحسن زيادة عدد التمريرات بشكل مفرط خشية أن يتعرض المادة للإجهاد المفرط بسبب التصلب، مما قد يؤدي إلى تدهور السطح بمجرد تجاوز القدرة على التشوه اللدن للمادة [8].

4.2 تطور الصلادة:

تحسين الصلادة هو نتيجة لتصلب الطبقات السطحية بسبب التشكيل اللدن لها. يعتبر الصقل بالكرة بواسطة رأس الماس أكثر فعالية في تصلب المادة مقارنة بالصقل بالدحروج، على الرغم من أن الصلادة المثلى الناتجة عن العمليتين تكون في نفس المستوى الشكل (5–b). تظهر القيم المثلى مع نفس نظام المعالجة. أثناء الصقل بالكرة، يختلف النظام الخاص بالصلادة المثلى عن ذلك المتعلق بالخشونة فقط من حيث عدد التمريرات، حيث يتغير من 2 إلى 3.

من ناحية أخرى، في حالة التلميع، إذا كان الهدف هو الحصول على خشونة أو صلادة مثالية، يجب مراعاة العاملين الحاسمين P وi. يتم التحكم في تأثير هذين العاملين على الصلادة بنفس الظواهر. يؤدي زيادة جهد التشكيل وكذلك زيادة عدد التمريرات إلى تشكيل المادة بشكل أكبر، مما يؤدي إلى تصلبها عن طريق التشكيل. باستخدام رأسه الماسي، يؤثر أداة الصقل بالكرة بعمق أكبر على الطبقات السطحية ويقدم بالتالي أفضل نتيجة. ومع ذلك، كما هو موصى به [8]. يجب تحديد هذه القيم لتجنب التشبع الزائد للمادة بالتصلب، خوفاً من تطور التشققات الدقيقة في المادة.

بالمقابل فإن زيادة سرعة الدوران وتقدم العمل تقلل من التأثيرات الإيجابية للمعالجتين فيما يتعلق بالصلادة كما يبين بالشكل (5–a, b) يبدو أنه عند السرعات العالية، يكون معدل تشوه المادة غير كافٍ لتعزيزها بشكل كافٍ. وينطبق نفس الأمر على التقدم الذي يرتبط بسرعة الدوران من خلال السلسلة الحركية لآلة التشغيل. مع زيادة السرعة، يتصرف الصقل بالكرة بطريقة مشابهة للصقل بالدحروج، في حين أنه بزيادة التقدم، يمكن ملاحظة تداخل بين العمليتين. عند التقدمات الصغيرة، يكون الصقل بالدحروج أكثر حساسية تجاه الصلادة، بينما يصبح أقل حساسية عند القيم الكبيرة.

4.3 مقاومة التآكل

يبدو أن تحسين مقاومة التآكل كما يبين في الشكل (6) من خلال المعالجتين هو نتيجة مباشرة لنعومة السطح وصلادة الطبقات السطحية الناتجة عن العمليتين [5].إذ تقع منحنى فقدان الكتلة كما في الشكل (7) الناتج عن عملية الصقل بالكرة أسفل المنحنى الناتج عن عملية التشكيل، مما يفسر أن عملية الصقل بالدحروج توفر أفضل النتائج فيما يتعلق بمقاومة التآكل التي تحسنت بنسبة تصل إلى 98٪ في هذه الحالة.

الطبقات السطحية المعالجة بالصقل الكرة أكثر صلادة من تلك المعالجة بالتشكيل، مما يجعلها أكثر مقاومة للتآكل. مما يُفسر أفضل نعومة للسطح الناتجة عن التشكيل بمرحلة التآكل الطفيف على منحنى التآكل الذي يتطابق مع المنحنى الخاص بالصقل بالكرة.

في مرحلة التآكل العادي، تتطور المنحنيات الخاصة بالعمليتين بنفس الطريقة. ويتطور المنحنى المتعلق بالصقل بالكرة بميل أقل حدة مما يؤكد فعالية هذه العملية. بعد هذه المرحلة، تتدهور الطبقة المتصلدة تحت تأثير الاحتكاك مع الأداة ويتكثف التآكل بشكل كارثي.

5 . الخلاصة

يُعَدّ كل من الصقل بالدحروج والكرة عمليتين ميكانيكيتين لمعالجة الأسطح على البارد من خلال التشوه اللدن للطبقات السطحية. توفر هاتان الطريقتان تلميعاً عبر ضغط المادة. حيث يتسبب هذا

الضغط في حدوث زحف على سطح المادة حيث تتشكل موجة معدنية أمام الأداة وتجدد سطحاً جديداً خلفها. تعمل الطريقتان على تحسين حالة السطح وزيادة الصلابة.

تُعَدّ أدنى خشونة سطحية متاحة بواسطة الصقل بالدحروج؛ هذا النتيجة تكون أفضل كلما كانت الخشونة الأولية قريبة من 3 ميكرومتر. في حين أن أفضل نتيجة للصلابة يتم الحصول عليها عبر الصقل بالكرة. وبناءً على ذلك، يتم تنظيم الكفاءة المثلى لكل عملية من خلال نظام محدد حيث تكون العوامل المهمة هي جهد التشكيل وعدد التمريرات. للحصول على خشونة أفضل، يُوصى بتقييد عدد التمريرات إلى 2؛ أما لتحقيق صلابة أعلى، يمكن زيادة هذا العامل إلى 3 تمريرات مع جهد قدره 15 daN. يؤثر جهد التشكيل على الخشونة، مما يؤدي إلى تفاعل بين الطريقتين ضمن حدود النطاق المختار.

في ظل ظروف الاختبار هذه، على الرغم من أنها تسعى لتحقيق الإنتاجية وكفاءة العملية، إلا أن زيادة السرعة والتقدم لا تؤثر بشكل كبير على الخشونة والصلابة. كما تتصرف الطبقات السطحية المعالجة بالصقل بالكرة والصقل بالدحروج كأنها أسطح مصقولة وتظهر مقاومة جيدة للتآكل، كما يُعَدّ لصقل بالكرة أكثر فائدة في هذا السياق.

6 .المراجع:

[1] Liao .L, Zhang .Z, Liu. J, Li .Y, Cui. X, Liu .L ,2020- A novel process of chemical mechanical polishing for FV520B steel. Journal of Manufacturing Processes, 51–57P.

[2] Maximov. J , Duncheva . G, Anchev .A, Dunchev. V , Anastasov.K and Daskalova .P ,2024- Effect of Roller Burnishing and Slide Roller Burnishing on Surface Integrity of AISI 316 Steel: Theoretical and Experimental Comparative Analysis, MDPI ,machines, 12-51P. doi.org/10.3390/machines12010051.

[3] Dwivedi, D.K. Surface Engineering2018. In Enhancing Life of Tribological

Components; Korzynski, M., Ed.; Springer: New Delhi, India,; ISBN 978-81-322-3779-2.

[5] A.M. Hassan, A.D. 1999-Suleiman, Improvement in the wear resistance of brass components by ball burnishing process, J. Mater. Process. Technol. 96 . 73–80p.

[6] Maximov, J.T.; Duncheva, G.V.; Anchev, A.P.; Dunchev, V.P. 2020-Slide burnishing versus deep rolling A comparative analysis. Int. J. Mach. Tools Manuf., 110, 1923–1939p.

[7]. Loh N.H,. Tam S.C,. Miyazama S, 1990-Surface hardening by ball burnishing, Proc. Engng.vol 23 ,413–417p .

[8] Hassan A. M, 1997-The effect of ball and roller burnishing on the surface roughness of some non-ferrous metals, J. Mat. Proc. Tech. vol 72 ,385–391p.

[9] M. Fattouh, M.M. El-Khabeery, Residual stress distribution in burnishing solution treated and aged 7075 Al alloy, Int. J. Mach. Tools Manufact. 29 (1989). 153–160

[10] V.M. Braslavski, A.A. Baraz, Deformation strengthening of machinery parts, Vestnik Machinostroeniya 63 (1983) 46–51 .

[11] M.H. El-Axir, An investigation into roller burnishing, Int. J. Mach. Tools Manufact. 40 (2003) 1603–1617 .

[12] P.I. Kudryavstsev, Surface work-hardening delays fatigue development, Russian Eng. J. LII (1983) 61–65 .

[13] Maximov, J.T.; Duncheva, G.V.; Anchev, A.P.; Dunchev, V.P.; Argirov, Y.B. 2022-Effect of Diamond Burnishing on Fatigue Behaviour of

AISI 304 Chromium-Nickel Austenitic Stainless Steel. Materials, vol 15.

[14] Hassan A.M, 1997-An investigation into the characteristics of burnished cast Al-Cu alloy, Int. J. Mach. Tools Manufact. Vol 37 , 813–821p .

[15] Khabeery M.M, El-Axir M.H, 2001-Experimental techniques for studying the effects of milling roller burnishing parameter on surface integrity, Mach. Tools Manufact. Vol 41 , 1705–1719p .

[16] Wang ,K.H, Blunt L.A, Stout K.J, 1998-The 3D characterization of the surface topography of the ballizing process, Int. J. Mach. Tools Manufact. Vol 38 , 419–423 p.

[17]. El-Axir M.H,. El Khabeery M.M, 2003-Influence of orthogonal burnishing parameters on surface characteristics for various material, J. Mat. Proc. Tech. vol 132 , 82–89p .

[18] Wagner L, 1999-Mechanical surface treatments on Ti, Al and Mg alloys, Mat. Sce. Ingng. A263 , 210–216p .

[19] Zhang P, Lindemann J, 2005-Effect of roller burnishing on high cycle fatigue performance of the high-strength wrought magnesium alloy AZ80, Scr. Mat. Vol 52 ,1011–1015p .

[20] . Klocke F, Lierman J, 1998-Roller burnishing of hard turned surfaces, Int. J. Mach. Tools Manufact. Vol 38 , 419–423p .

تصميم خوارزمية كشف الاحتيال في مواقع التجارة الإلكترونية بهدف تحسين الدقة والسرعة في عمليات الكشف

الطالب: علي إبراهيم

إشراف:د.بسيم عمران

ملخص

تعتبر أنظمة الكشف عن الاحتيال من أهم الأنظمة المستخدمة في مواقع التجارة الإلكترونية، وذلك بهدف حماية الموقع والمستهلك والشركات التي تعرض منتجاتها عبر مواقع التجارة الإلكترونية من الهجمات الاحتيالية، وعليه تقوم معظم مواقع التجارة الإلكترونية العالمية بتخصيص مبالغ مادية كبيرة بهدف تحسين وتطوير بنية أنظمة كشف الاحتيال لديها بهدف جعل النظام أكثر دقة و كفاءة.ولكن على الرغم من التطور الكبير في مجال الكشف عن الاحتيال إلا أن أغلب الحلول المقدمة ما تزال تعاني من مشكلتي الدقة والسرعة في التنفيذ، وعليه قام الباحث بتقديم نظام لكشف الاحتيال يعتمد بشكل أساسي على دراسة سلوك المستخدم ضمن الموقع، وتطبيق الحل على مجموعة بيانات Kaggle.com على مرحلتين ، الأولى تطبيق الحل على قاعدة البيانات الأساسية ، والثانية تطبيق الحل على قاعد البيانات الموسعة حيث قام الباحث بزيادة عدد السجلات وقام بتقديم نتائج الدقة ومقارنتها مع نتائج خوارزميات التنقيب عن المعرفة في قواعد البيانات المعرفية والتي تستخدم بشكل كبير في مجال الكشف عن الاحتيال في مواقع التجارة الإلكترونية.تقدم هذه المقالة حلاً ديناميكياً للاحتيال يعتمد على دراسة سلوك المستخدم ضمن موقع التجارة الإلكترونية، ومن ثم مقارنة

نتائج الحل المقترح من قبل الباحث مع الحلول الثابتة المعتمدة على خوارزميات تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية، كما توضح المقالة أثر أخذ الخصائص المناسبة وإضافتها على مجموعة البيانات Kaggle (وهي جدول يحتوي على مناقلات خاصة بموقع تجارة إلكترونية)، حيث تم دراسة أثر أخذ الخصائص المناسبة بعين الاعتبار وأثرها على الدقة مع ازدياد عدد السجلات(عدد المناقلات الخاصة بكل مستخدم ضمن الموقع)، كما قام الباحث بتقديم هيكلية تقوم بجمع المعلومات المطلوبة عن تفاعل المستخدم مع الموقع، ومن ثم مقارنة السلوك الحالي للمستخدم مع السلوك السابق المخزن ضمن قاعدة البيانات لتحديد هل المناقلة الحالية شرعية أم أنها عملية احتيالية.

Abstract:

Fraud detection system is one of the most important systems used in e-commerce sites، which protect e-commerce website، consumers and companies from fraudulent attacks .Most e-commerce website spent a lot of money in improving the architecture of its fraud detection system to make it more accurate and efficient. However، despite the great development in the field of fraud detection، most of the solutions presented still have accuracy and speed problems، therefore the researcher presented a fraud detection system that relies primarily on studying user behavior within the site in two stages ,First stage is applying the solution to the primary database، second stage is applying the solution to the database after increasing the number of records، after that researcher presents accuracy and efficiency of system. This article presents dynamic solution for fraud depending on studying users' behavior in E-commerce website and comparing results of suggestion solution with other static results of KDD's

algorithms. This article explains the benefits of adding required attributes to kaggle dataset and studies the benefits of adding required attributes at accuracy of fraud detection in e-commerce website.Within the articles, The researcher provides structure of fraud detection system which collect data about user's interaction with e-commerce website and compare the current user's behavior with previous stored user's behavior to determine if the current transaction is fraud or not.

مقدمة

ازداد في الآونة الأخيرة استخدام أنظمة الكشف عن الاحتيال بشكل واسع وكبير، ليس فقط في مواقع التجارة الإلكترونية وانما تعداها الى استخدامات واسعة في مواقع التواصل الاجتماعي، أنظمة البورصة العالمية وغيرها ،وذلك بسبب الأثر السلبي والخسائر المادية الكبيرة التي تسببها مثل هذه النوعية من عمليه النصب الإلكتروني، إن الحد من الخسائر التي تتكبدها مواقع التجارة الإلكترونية سنوياً تعتبر أهم الأهداف لأنظمة كشف الاحتيال، إلا أن مثل هذه الأنظمة وعلى الرغم من التطورات الكبيرة التي طرأت عليها لا تزال تعاني من العديد من المشاكل نذكر[1] منها:

1- **مشكله الدقة:** تعتبر دقه أنظمة الكشف الاحتيالي لتحديد هل المناقلة الحالية شرعيه أم احتياليه العامل الأساسي لتقييم مثل هذه الأنظمة، وخاصة أن دقة مثل هذه الأنظمة تتأثر بشكل كبير بعدد السجلات، حيث ما تزال تعاني الأنظمة المعتمدة على تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية من مشكلة انخفاض الدقة بزيادة عدد السجلات وزيادة حجم قاعدة البيانات الخاصة بمواقع التجارة الإلكترونية وذلك في حال عدم أخذ الخصائص المناسبة بعين الاعتبار، وخاصة تلك الخصائص التي ترتبط ارتباطاً وثيقاً بسلوك المستخدم ضمن موقع التجارة الإلكترونية وتفاعلاته ضمن الموقع، حيث تقدم خوارزميات التنقيب عن المعرفة في قواعد البيانات المعرفية حلولاً ثابتة ستاتيكية لمشكلة الاحتيال والتي تتأثر دقتها بشكل كبير مع ازدياد عدد السجلات ضمن قاعدة البيانات .[2]

2- **مشكلة الأداء:** تعتمد بنية أغلب أنظمة الكشف عن الاحتيال في مواقع التجارة الإلكترونية المعتمدة على تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية على عملية مسح كامل لقاعدة البيانات ، وذلك لاتخاذ القرار المناسب هل المناقلة الحالية شرعية أم أنها عملية احتيالية الأمر الذي سيكلف الكثير من الوقت واستهلاك الموارد المادية للنظام، وخاصة أن قاعدة البيانات الخاصة بمواقع التجارة الإلكترونية تتزايد بشكل أسي بمرور الوقت.[3]

قام الباحث من خلال هذه المقالة بتصميم نظام لكشف الاحتيال في مواقع التجارة الإلكترونية بالاعتماد على دراسة سلوك المستخدم ضمن الموقع، وذلك من خلال قيام الباحث بدراسة وإضافة العديد من الخصائص التي ترتبط ارتباطاً وثيقاً بسلوك المستخدم، حيث يوجد العديد من هذه الخصائص لم تكن موجودة في الدراسات الخاصة بأنظمة الكشف عن الاحتيال ، ولكن الباحث اعتمد بشكل أساسي على أنظمة تحليل البيانات، وتحليل المحتوى، واستنتاج أهم الخصائص التي ترتبط بسلوك المستخدم ضمن الموقع ، كما وقام الباحث بعملية تحسين للأداء من خلال توزيع عملية جمع المعلومات المطلوبة على كامل النظام، وذلك عكس باقي الحلول المطروحة المعتمدة على تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية والتي تعتمد بشكل أساسي على جمع كل عمليات المقارنة وعمليات جمع المعلومات ضمن مرحلة واحدة ، الأمر الذي سيؤثر بشكل أساسي على زمن الانتظار الخاص بالمستخدم وذلك لتحديد هل المناقلة الحالية شرعية أم أنها عملية احتيالية. اعتمد الباحث بعد عملية جمع المعلومات عن المستخدم القيام بمقارنة سلوك المستخدم الحالي مع السلوك السابق له والمخزن ضمن قاعدة البيانات لتحديد هل المناقلة الحالية شرعية أم أنها عملية احتيالية، ومن ثم قام بدراسة دقة النظام المقدم ومقارنته مع أكثر خوارزميات كشف الاحتيال استخداماً وذلك باستخدام معايير الدقة الخاصة بأنظمة كشف الاحتيال، بحيث يحقق هذا النظام المقترح أعلى دقة وبأفضل أداء.

مشكلة البحث

تعاني أغلب الحلول المقدمة لحل مشكلة الاحتيال في مواقع التجارة الإلكترونية من مشكلة الدقة بمرور الزمن والمشكلة الثانية مشكلة الأداء أو سرعة التنفيذ(زمن الكشف عن الاحتيال) نتيجة اعتماد

أغلب الحلول المقدمة من قبل تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية على مسح كامل لقاعدة البيانات وذلك بهدف الحصول على نتائج دقيقة، علماً بأن حجم قواعد البيانات الخاصة بمواقع التجارة الإلكترونية تتزايد بشكل أسي بمرور الزمن الأمر الذي سيسبب مشكلة للحلول التي تعتمد على مسح كامل لقاعدة البيانات.

أهداف البحث

يهدف البحث إلى تقديم نظام لكشف الاحتيال يعتمد على تتبع سلوك المستخدم مع الموقع من خلال تسجيل تفاعلات المستخدم مع الموقع وتخزين أهم الخصائص الخاصة بالمستخدم وتفاعلاته ضمن موقع التجارة الإلكترونية بهدف الوصول إلى نظام يتميز بالدقة الجيدة وزمن الكشف الجيد (والمقصود بالدقة هو عدد المناقلات الاحتيالية التي تم كشفها من قبل النظام والمقصود بزمن الكشف هو الزمن اللازم للنظام لتحديد هل المناقلة الحالية شرعية أم أنها عملية احتيالية) ، كما يهدف البحث إلى المقارنة بين الحلول الديناميكية التي تعتمد على سلوك المستخدم ومقارنتها مع الحلول الثابتة المقدمة من تقنيات التنقيب عن المعرفة في قواعد البيانات المعرفية، حيث اعتمد الباحث على أخذ أهم الخصائص الخاصة بسلوك المستخدم ضمن موقع التجارة الإلكترونية اعتماداً على دراسات سابقة ، وإضافة خصائص جديدة مهمة ولها أثر في تحديد سلوك المستخدم بطريقة أكثر دقة وشمولية سيتم تحديدها في المقالة.

أهمية البحث

تأتي أهمية البحث من كون الحصـول على نظام دقيق وذو كفاءة عالية تتزايد بمرور الوقت نتيجة اعتماد النظام المقترح على سلوك المستخدم يعتبر حل جيد وذو دقة متزايدة بمرور الوقت.

منهج وفرضيات البحث

يعتمد هذا البحث على المنهج التطبيقي وذلك من خلال تصـميم نظام لكشـف الاحتيال وتطبيقه على مجموعة البيانات العالمية Kaggle[4] الأسـاسـية والموسـعة، والحصـول على نتائج الدقة باسـتخدام برنامجي Weka,RStutio وتقديم نتائج الدقة من خلال معايير الدقة المسـتخدمة في تقييم أنظمة كشف الاحتيال.

مجموعة البيانات Kaggle الأساسية والموسعة:

يقدم موقع kaggle.com عدد كبير من مجموعات البيانات الخاصة بمواقع التجارة الإلكترونية والتي تحتوي على جداول مناقلات خاصة بالمستخدمين ضمن الموقع، حيث قام الباحث باختيار مجموعة بيانات تحتوي هذه المجموعة على 284808 سجل خاصة بالمناقلات بين المستخدمين وموقع التجارة الإلكترونية، وتحتوي على 22 خاصية من الخاصيات من بينها المنتجات التي قام المستخدم بشرائها، يضاف لها الخصائص التالية:

1- الزمن Time: وهو الوقت الذي استغرقه المستخدم للقيام بعمليات الشراء عبر موقع التجارة الإلكترونية.
2- الكمية Amount: وهي كمية المنتجات التي قام بها صاحب البطاقة.
3- الصنف Class: هل هذه المناقلة هي مناقلة شرعية أم أنها عملية احتيالية.

حيث تم أخذ عينات من قاعدة البيانات التي تم جمعها ابتداءً من عام 2013 حتى عام 2022، وهي تحوي على عمود أخير يحدد فيما إذا كانت المناقلة الحالية شرعية أم لا، بغية مقارنة نتائج الحلول المقدمة والخوارزميات التي تتم تطبيقها على قاعدة البيانات واختبار الدقة. قام الباحث لجعل عملية التحليل واختبار الدقة الخاصة بعمليات المقارنة بين الحل المقترح من قبله والحلول السابقة بتوسعة قاعدة البيانات وذلك من خلال زيادة عدد السجلات المدروسة إلى 532251 من خلال دمج مجموعة بيانات أخرى لموقع Kaggle بنفس الخصائص ، ومن ثم قام الباحث بزيادة عدد الخصائص المدروسة والخاصة بسلوك المستخدم ضمن الموقع وذلك ضمن جدولين هما Complete_User_Behavior و User_profile والتي بعضها لم يكن موجود في دراسات سابقة (سيتم شرح هذين الجدولين في معرض المقالة)، واختبار الحل المقترح على قاعدة بيانات Kaggle الموسعة والمعدلة من قبل الباحث.

حيث قام الباحث بالاعتماد على محموعة البيانات kaggle وذلك لكونها مجموعة بيانات متوازنة واتساقية وخالية من الضجيج حيث لا يوجد حاجة إلى إعادة معالجة البيانات، حيث تمت دراسة سلوك نحو 4112 مستخدم ، والجدير بالذكر أن مجموعة البيانات Kaggle تحتوي على عمود

أخير يحدد هل المناقلة الحالية شرعية أم أنها احتيالية، بقيمة =1 للحالات الشرعية وقيمة =0 للحالات الاحتيالية، الأمر الذي مكن الباحث من التأكد من دقة النتائج،حيث تقدر عدد الحالات الاحتيالية ضمن مجموعة البيانات الأساسية ب 6222 حالة احتيالية و 278586مناقلة شرعية، أما في قاعدة البيانات الموسعة يوجد لدينا نفس عدد المستخدمين ، بينما تقدر عدد الحالات الاحتيالية ب13225 مناقلة احتيالية و 519026 مناقلة شرعية.يوضح الجدول التالي بينة مجموعة البيانات المقدمة من قبل kaggle:

Trans ID	User ID	Time	Amount	Class	Product1	Amount1	….	transType

الجدول (1) يوضح بنية مجموعة البيانات الخاصة بالمناقلات المقدمة من موقع kaggle

كما يوضح الجدول التالي بينة الجدول الخاص بمعلومات المستخدمين ضمن الموقع :

User ID	User Firstnamre	Last Name	Age	Education	Credit Card ID	User Name	Password

الجدول (2) يوضح معلومات المستخدمين ضمن موقع kaggle

كما يوضح الجدول التالي المعلومات الخاصة ببطاقات الائتمان :

Credit ID	User _Id	Credit _Card_Num	Credit Card password	Credit Card_ Bank

الجدول (3) يوضح معلومات بطاقات الإئتمان ضمن موقع kaggle

كما سيتم توضيح جدولي خصائص المستخدمين المضافة من قبل الباحث في معرض المقالة.

معايير الدقة والاختبار:

توجد العديد من معايير الدقة التي تستخدم في عمليات المقارنة بين خوارزميات الكشف عن الاحتيال في مواقع التجارة الإلكترونية، ولكن تم اعتماد أكثر هذه المعايير جودة وكفاءة وهي [5]:

1- TP Rate.

2- FP Rate.

3- $precision\ P = TP/(TP + FP)$

4- $Recall\ R = TP/(TP + FN)$

5- $F1 = 2 * Precision * Recall/(Precision + Recall)$

6- MCC.

7- Roc Area.

8- PRC Area.

أهم الدراسات المرجعية السابقة:

تم تقديم العديد من الأنظمة الخاصة بعمليات الكشف عن الاحتيال في مواقع التجارة الإلكترونية، نذكر منها:

1- RAPTIDAR,R, 2021 [6] : قام Fraud Detection using GA and AI الباحث بالدمج بين الشبكات العصبونية والخوارزميات الجينية وقسم الحل على ثلاث مراحل حيث تم في المرحلة الأولى تدريب الشبكة العصبونية كما قام الباحث بالاعتماد في المرحلة الثانية على خوارزمية SVM لزيادة الدقة، وطبق خرج خوارزمية SVM على الخوارزمية الجينية كمرحلة ثالثة، واختبر دقة الحل على قاعدة بيانات Kaggl، وعلى الرغم من الدقة التي تم الحصول عليها(95.923%) إلا أن النظام يتميز بالتعقيد وزمن التنفيذ العال، كونه اعتمد على ثلاثة مراحل للوصول للحل إضافة إلى الصعوبة في التطوير والتعديل على الحل، حيث اعتمد الباحث على دراسة عدد الحالات الاحتيالية

المكتشفة كمعيار أساسي للدقة(لم يتطرق الباحث ضمن المقالة إلى زمن التنفيذ أو زمن الكشف عن الاحتيال).

2- Keveort,A -2018. Faud Dtection Using Decision tree and Smote Decision Tree[7]قام الباحث بتقديم نظام يعتمد على خوارزمية شجرة دعم القرار وشجرة دعم القرار المعدلة وقام بتطبيق الحل على قاعدة البياناتkaggle، حيث قسم الباحث الحل إلى مرحلتين : الأولى تعتمد على تطبيق خوارزمية شجرة أخذ القرار المعدلة، ومن ثم تطبيق خوارزمية شجرة دعم القرار وكانت دقة النتائج أقل من الحل السابق(94.281%) (حيث اعتمد في قياس الدقة على دراسة عدد حالات الاحتيال المكتشفة)، وبزيادة عدد السجلات سنحصل على دقة أقل وسيكون سرعة التنفيذ أكبر وبالتالي الحل غير مفيد في حال قواعد البيانات الضخمة بسبب اعتماد الباحث على خوارزميات ثابتة ولم يأخذ كامل الخصائص المناسبة ضمن الدراسة الخاصة بسلوك أو اهتمامات المستخدم بعين الاعتبار والتي تعتبر المقياس الأهم في تقييم هل المناقلة الحالية شرعية أم أنها عملية احتيالية.

3- Holland,J,2021- Using logistic Regression and KNN to detect fraud Transaction in e-Commerce: حيث قام الباحث بتقديم حل يعتمد على الدمج بين خوارزمية logistic Regression وخوارزمية الجار الأقرب [8] ، حيث اعتمد الباحث في المرحلة الأولى على استخدام خوارزمية الجار الأقرب ثم طبق خرج هذه المرحلة كدخل لخوارزمية Logistic Regression ،حيث أعطت نتائج أفضل من تطبيق كل خوارزمية على حدا وكانت الدقة (96.341%)، ولكن الحل المقترح لم يأخذ كامل الخصائص الواجب دراستها بعين الاعتبار، كما أن الحل المقدم يتميز بالتعقيد وزمن التنفيذ العاليين وصعوبة التطوير والتعديل على هذا النموذج.

نلاحظ أن أغلب الحلول المقدمة سابقاً والأكثر انتشاراً واستخداماً تعتمد بشكل أساسي على الخوارزميات التالية[9]:

1- KNN for K=3 and K=7.

2- SVM.

3- Decision Tree.

4- Smote Decision Tree.

5- Logistic Regression.

6- Navie Bayes.

7- Smote Navie Bayes.

8- Random Forest.

وعليه قام الباحث بتطبيق هذه الخوارزميات على قاعدتي بيانات Kaggle الأساسية والموسعة، حيث اعتمد في عمليات المقارنة على برنامجي Weka, RStudio[10] وكانت النتائج على النحو التالي:

Algorithms	Accuracy		AVG
	Weka	Rstudio	
K=3،KNN	95.433%	95.323 %	95.378%
K=7،KNN	95.593%	95.455%	95.524 %
Navie Bayes	95.813%	95.772%	95.7925%
Logistic Regression	96.632%	96.451%	96.5415%
SVM	97.491%	97.421%	97.456%
Navie SMOTE	92.029%	92.3738%	92.18645%
Decision Tree	93.199%	93.0856%	93.14223%
Random Forest	92.71103%	92.997%	92.854015%
Decision Tree SMOTE	91.09377%	90.2627%	90.678235%

الجدول(4): يوضح نتائج مقارنة الخوارزميات على قاعدة البيانات الأساسية

نلاحظ من الدراسة السابقة أن أفضل الخوارزميات المقدمة في حل مشكلة كشف الاحتيال هي خوارزمية SVM بمعدل دقة متوسطة يقدر ب97.456% وأن أسوء الخوارزميات المقدمة هي خوارزمية Decision Tree Smote بمعدل دقة يصل إلى 90.678%.

المرحلة الثانية: قام الباحث بالمقارنة بين الخوارزميات السابقة بتطبيقها على قاعدة بيانات kaggle الموسعة بحيث أصبح عدد السجلات فيها 532251 وكانت النتائج على النحو التالي:

	Accuracy		AVG
Algorithms	Weka	Rstudio	
K=3،KNN	92.325%	91.9952%	92.1385%
K=7،KNN	92.5598%	92.137%	92.3484%
Navie Bayes	91.926%	91.0725%	91.499%
Logistic Regression	94.6398%	94.1495%	94.3945%
SVM	95.599%	95.279%	95.4141%
Navie Bayes SMOTE	88.3139%	88.1379%	88.2259%
Decision Tree	84.951%	84.5426%	84.7468%
Random Forest	86.348%	85.42%	81.884%
Decision Tree SMOTE	81.74905%	80.969%	81.359025%

الجدول(5): يوضح نتائج مقارنة الخوارزميات على قاعدة البيانات المعدلة والموسعة من قبل الباحث

نلاحظ أنه بزيادة عدد السجلات فإن دقة الخوارزميات قد انخفضت بشكل كبير، وذلك بسبب عدم أخذ كل الخصائص المطلوبة بعين الاعتبار، الأمر الذي يؤثر بشكل كبير على درجة الدقة المطلوبة، حيث نلاحظ أن أكثر الخوارزميات تأثراً هي خوارزمية Decision Tree Smote وأقل الخوارزميات تأثراً هيٍ بمقدار 2.6% وعليه فإن دقة هذه الخوارزميات والتي تستخدم بشكل كبير في مجال كشف الاحتيال تتناقص بشكل ملحوظ كلما كبر حجم قاعدة البيانات لدينا، وبالتالي لحل هذه المشكلة،

ولجعل دقة النظام تزداد بمرور الوقت ، اقترح الباحث القيام بإضافة خصائص جديدة لقاعدة البيانات، هذه الخصائص مرتبطة بسلوك المستخدم ضمن قاعدة البيانات.

بنية النظام المقترح لحل مشكلة الاحتيال:

اعتمد الباحث في الحل المقترح على تسجيل سلوك المستخدم ضمن الموقع وتسجيل تفاعلات المستخدم ضمن جدولين:

الجدول الأول: هو Complete User behavior وهو يحتوي على المعلومات التالية:

Attribute	Description
User_Behavior_ID	رقم المستخدم ضمن الجدول
User_ID	رقم المستخدم من جدول المستخدمين
User_Type	نوع المستخدم وهو إما جديد أو يحتوي على عدد قليل من المناقلات أو يحتوي على عدد جيد من المناقلات
User_Name	اسم المستخدم
Average_Session_Time	المدة المتوسطة للجلسة
NPS(Net Promoter Score)	عدد النقرات التي يقوم بها المستخدم ضمن الجلسة
Summary_Reading	قراءة ملخص المنتج قبل شراءه
Reading_All_Summary	قراءة كل الملخصات قبل الشراء
Read_similar_product	قراءة منتجات مشابهة للمنتج الحالي
Speed_in_typing	سرعة المستخدم في الكتابة(وهي المتوسط الحسابي لعشر إدخالات للمستخدم في الجلسة الواحدة

amount_in_transaction	كمية الشراء التي يقوم بها المستخدم في الجلسة الواحدة هل هي كبيرة أو متوسطة أو قليلة
Changing_Ip	هل المستخدم يقوم بتغيير IP بشكل مستمر أم لا
Last_IP	آخر عنوان IP للمستخدم
Changing_Tanspotation_location	هل المستخدم يغير عنوان الشحن بشكل مستمر[11]
Direct_Purchase	هل المستخدم يقوم بالشراء مباشرة أم لا
Purchase_from_many_Credit_Cards	هل المستخدم يقوم بالشراء من أكثر من بطاقة ائتمانية
Required Discountig	هل المستخدم يطلب حسم أم لا
Times Between Transaction	الفترة الزمنية بين طلبي شراء(هل هنالك فترة زمنية بين طلبي شراء أم لا)
Purchase_Porduct	هل المستخدم يقوم بشراء منتجات ذات أسعار مرتفعة
Product_Type	هل المستخدم يقوم بشراء منتجات متنوعة في نفس الجلسة أم لا
Trasaction Type	هل المناقلة الحالية شرعية أم غير شرعية

الجدول(7) يوضح الخصائص المدروسة والمضافة من قبل الباحث

يضاف إلى الجدول السابق جدول ثان هو ملخص عن تفاعلات المستخدم ضمن الموقع وهو User Profile يتم فيها تسجيل وتعديل هذا السجل بشكل دوري بناء على تفاعلات المستخدم ، حيث يتم التعديل في حال كانت المناقلة الحالية للمستخدم شرعية، بحيث يتم أخذ متوسط حسابي لبعض الخصائص مثل: متوسط سرعة الكتابة، الفترة الزمنية بين جلستين، المدة الزمنية للجلسة، يضاف

إلى ما سبق التعديل على بعض الخصائص مثل: هل المستخدم قام بتغيير عنوان الشحن، هل المستخدم قام بتغيير IP البلد الذي يشتري أو يتصفح منها عادة، وغيرها من الأمور الأخرى.

حيث يتم إعطاء أوزان لهذه الخصائص ، بحيث يتم مقارنة سلوك المستخدم الحالي مع سلوك المستخدم ضمن قاعدة البيانات (السجل الموجود ضمن جدول User_Profile), ويتم اتخاذ القرار بناءً على قيم السلوك الحالي للمستخدم وهو:

1- فإذا كان وزن سجل المستخدم الحالي => حد العتبة وهو 7 من أصل عشرة تعتبر المناقلة الحالية مناقلة شرعية.
2- فإذا كان وزن سجل المستخدم الحالي < حد العتبة وهو 7 من أصل عشرة تعتبر المناقلة الحالية مناقلة احتيالية.

من الجدير بالذكر هنا أن النظام لدينا يبدأ بإعطاء نتائج ذات دقة مقبولة بعد قيام المستخدم ب 10 مناقلات مع الموقع سواء من ناحية الشراء أو التصفح أو غيرها من التفاعلات الأخرى.

كما يقدم البحث إضافة للحلول المطروحة التي تقوم بدراسة سلوك المستخدم وذلك من خلال ما يلي:

1- تم تسجيل كامل مناقلات المستخدم ضمن الموقع سواء أكانت المناقلة الحالية هي عملية شراء أو عملية تصفح أو أي عملية تفاعل بين المستخدم الحالي والموقع، الأمر الذي يسرع عملية الحصول على نتائج دقيقة من قبل النظام المطروح، حيث تقدر عدد المناقلات التي يقوم بها المستخدم وذلك للحصول على نتائج ذات دقة مقبولة بحوالي 10 مناقلات، وهذا الأمر يعتمد على مدى تفاعل المستخدم مع الموقع ضمن المناقلة الواحدة، هل قام بالكثير من التفاعلات أو كانت تفاعلاته قليلة.
2- قام الباحث بتوزيع عمليات جمع المعلومات على مستوى النظام ككل، وتسجيل كل تفاعل للمستخدم مع الموقع مع كل حركة يقوم بها المستخدم ضمن الموقع ووضع هذه المعلومات ضمن جدول Complete_User_Behavior، ومن ثم أخذ المتوسطات الحسابية لهذه التفاعلات وتسجيلها ضمن جدول User_profile وذلك لمقارنة السلوك الحالي للمستخدم

مع السلوك السابق والذي هو سجل واحد موجود في جدول User_profile الأمر الي يسرع عملية المقارنة ويحسن من زمن الكشف عن المناقلة الحالية هل هي شرعية أم أنها عملية احتيالية.

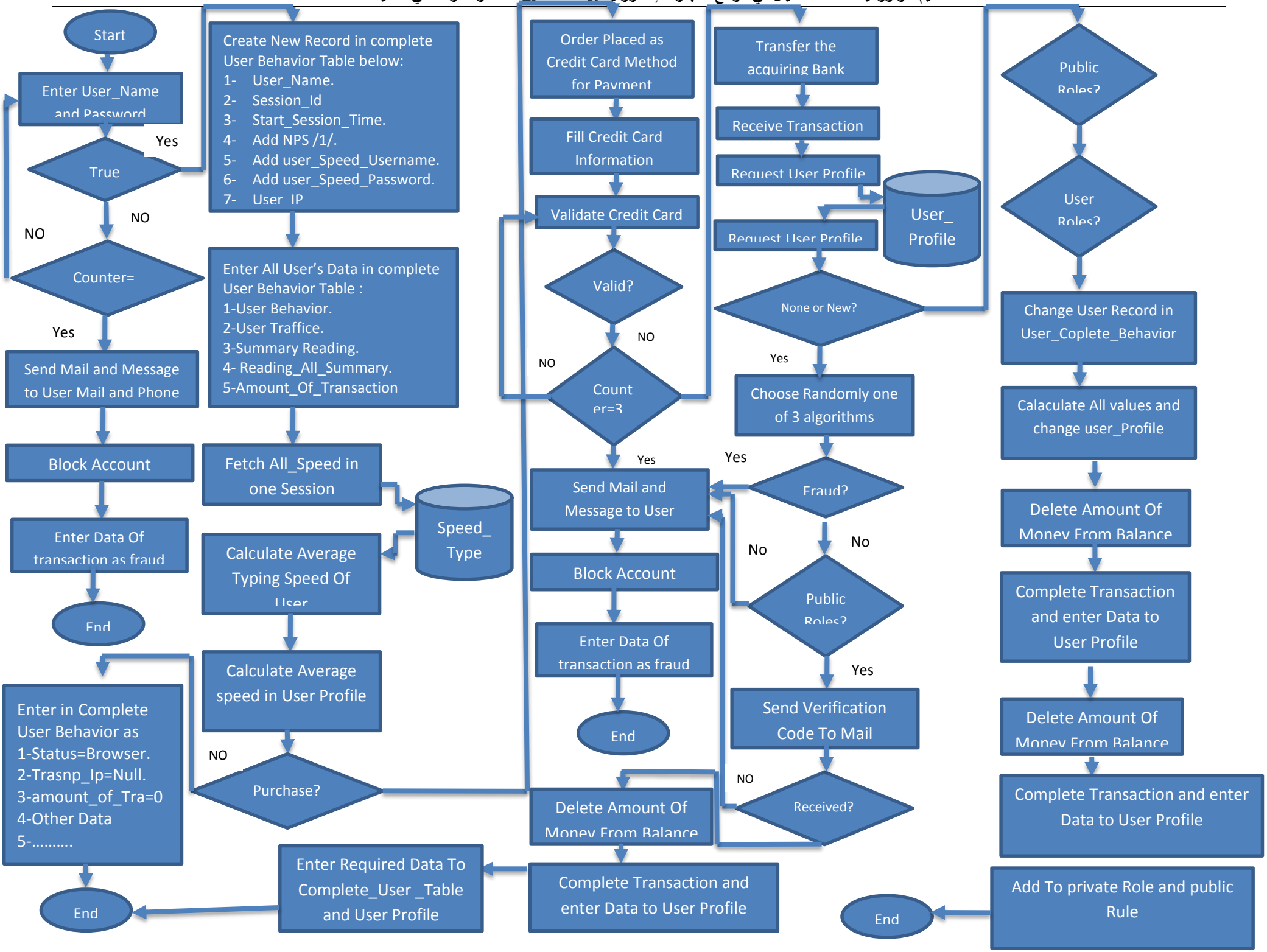
3- إعطاء بعض الخصائص أهمية أكثر من باقي الخصائص وهذه الخصائص هي:

- Speed_in_typing
- amount_in_transaction
- Average_Session_Time
- Direct_Purchase
- User_Type

وذلك من خلال تثقيل قيم هذه الخصائص بحيث يكون لها أثر أكبر من باقي الخصائص في تقييم المناقلة الحالية هل هي شرعية أم أنها عملية احتيالية.

نظراً لضرورة فهم آلية عمل النظام المقترح من قبل الباحث لا بد من شرح ألية عمله من خلال مخطط تدفقي للحل وإن كان المخطط كبير إلا أنه ضروري لفهم آلية عمل النظام المقترح:

تصميم خوارزمية كشف الاحتيال في مواقع التجارة الإلكترونية بهدف تحسين الدقة والسرعة في عمليات الكشف



قام الباحث باختبار النتائج التي قام بالحصول عليها بعد تطبيق النموذج المقترح على مجموعة بيانات kaggle

الأساسية والموسعة وذلك باستخدام كل من البرنامجين:

1- Weka: الذي يؤمن العديد من معايير الدقة التي يمكن الحصول عليها مباشرة من البرنامج، حيث يقوم البرنامج بأخذ عينات عشوائية من النتائج وتقييم الدقة بناءً على عدد حالات الاحتيالية المكتشفة، ويزودنا بقيم العديد من معايير الدقة المهمة.

2- Rstudio: والذي يعطي قيمة للدقة بشكل مباشر والتي تعبر عن عدد الحالات الاحتيالية المكتشفة الصحيحة .

ونظراً لكون مجموعة البيانات متوازنة ومتسقة وخالية من الضجيج بالتالي لم يكن من الضروري إدخال مجموعة البيانات في مرحلة معالجة البيانات ،وكانت النتائج على النحو التالي:

Correctly classified Instances	83725	97.9904%
Incorrectly Classified Instances	1717	2.0095469%
Kappa Statistic	0.7253	
Mean absolute error	0.00002	
Root mean squared error	0.0012	
Relative absolute error	11.9932%	
Root relative squared error	42.0012 %	
Total Number of Instances	85442	

===Detailed Accuracy By class ===

	TP	FP	Precision	Recall	F1	MCC	Roc	PRC	Class
	0.852	0.000	0.985	0.85	0.939	0.843	0.882	0.711	1
	1.000	0.112	1.000	1.000	1.000	0.843	0.882	1.000	0
AVG	0.979	0.235	0.979	0.999	0.979	0.843	0.8821	0.979	

الشكل(2) يوضح نتائج دقة الحل المقترح من قبل الباحث على قاعدة البيانات Kaggle باستخدام برنامج Weka

كما يظهر الشكل التالي نتائج تطبيق الحل المقترح على قاعدة البيانات بعد إضافة الخصائص المدروسة باستخدام برنامج RStudio وكانت النتائج على النحو التالي:

Confusion Matrix and Statistics

	Reference	
Prediction	Not Fraudulent	Fraudulent
Not Fraudulent	83695	1435
Fraudulent	0	31

الشكل(3) يوضح نتائج دقة الحل المقترح من قبل الباحث على قاعدة البيانات Kaggle باستخدام برنامج Rstudio

وبأخذ المتوسط الحسابي للدقة المقدمة من البرنامجين نلاحظ أن دقة الحل المقدم من قبل الباحث هي:

AVG Accuracy=(97.9904+97.955381)/2=97.97289%.

وبالتالي نلاحظ تحسن في الدقة من قبل الحل المقدم من قبل الباحث بفارق 0.516809% وهي دقة خوارزمية SVM، ولمزيد من الدقة قام الباحث بتطبيق الحل المقترح من قبله على قاعدة البيانات الموسعة واختبار النتائج على برنامجي WEKA,Rstudio وكانت النتائج على النحو التالي:

Correctly classified Instances	208842	98.5638 %
Incorrectly Classified Instances	2174	1.4361564%
Kappa Statistic	0.4125	
Mean absolute error	0.000252	
Root mean squared error	0.0092	
Relative absolute error	33.1263%	
Root relative squared error	46.0236 %	
Total Number of Instances	211885	

===Detailed Accuracy By class ===

	TP	TF	Precision	Recall	F−	MCC	Roc	PRC	Class
	0.786	0.000	0.953	0.686	0.999	0.804	0.912	0.911	1
	0932	0.533	0.999	0.953	0.999	0.804	0.912	0.994	0
AVG	0.982	0.522	0.988	0.953	0.999	0.804	0.912	0.995	

الشكل(4) يوضح نتائج دقة الحل المقترح من قبل الباحث على قاعدة البيانات Kaggle الموسعة باستخدام برنامج Weka

كما قام الباحث بتطبيق الحل المقترح على قاعدة البيانات الموسعة باستخدام برنامج Rstudio وكانت النتائج على النحو التالي:

Confusion Matrix and Statistics

	Reference	
Prediction	Not Fraudulent	Fraudulent
Not Fraudulent	208652	3002
Fraudulent	0	231

Accuracy : 98.4741732

الشكل(5)يوضح نتائج تطبيق الحل المقترح من قبل الباحث على قاعدة بياناتKaggle الموسعة

نلاحظ أن مقدار التحسن في الدقة عند تطبيق الحل المقترح من قبل الباحث على قاعدة البيانات الأساسية كان بمقدار 0. 516809% وفي المرة الثانية مقدار التحسن المتوسط للدقة بمقدار:

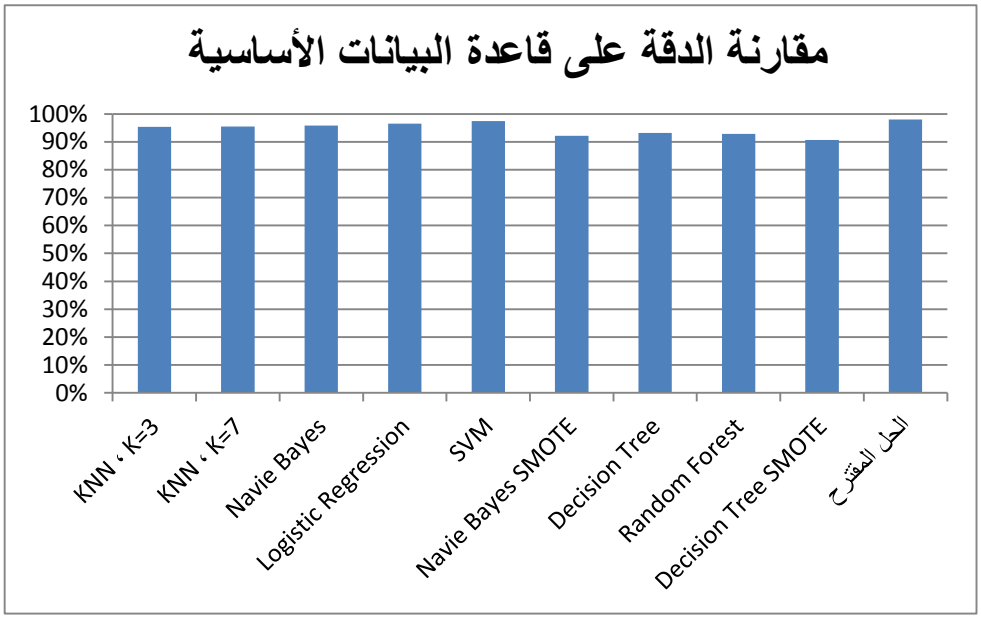
AVG Accuracy=(98.56938+98.4741732)/2=98.521776%

نلاحظ أن الدقة الناتجة عن الحل المقترح من قبل الباحث تتزايد بمرور الوقت والسبب هو زيادة عدد المعلومات الخاصة بالمستخدم ، حيث كلما زاد عدد مناقلات المستخدم مع الموقع كلما زادت الدقة لدينا نتيجة توفر معلومات أكثر عن المستخدم وبالتالي معرفة أكبر للنظام بسلوك المستخدم الحالي، وأن فرق الدقة بين الحل المقترح من قبل الباحث وبين أفضل خوارزمية يقدر بحوالي: 2.8819% وهذا مقدار كبير من ناحية الدقة، علماً بأن الحل المقترح من قبل الباحث ستتزايد دقته المقدمة بمرور الزمن.

مناقشة النتائج:

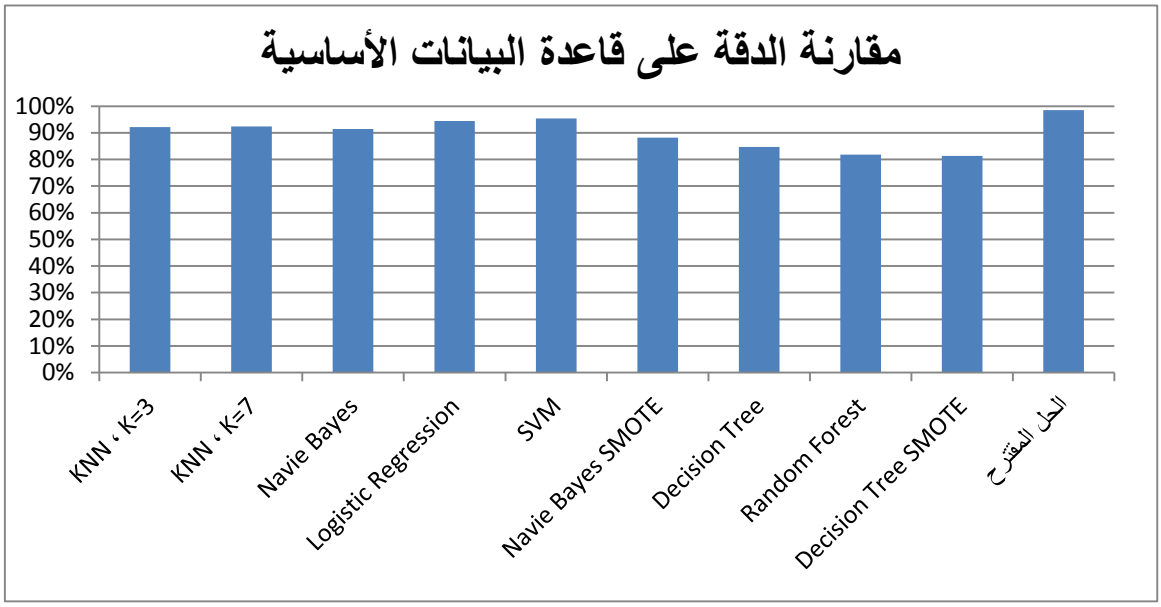
1- **الدقة:** تعتمد الدراسة والنظام المقدم من قبل الباحث على دراسة سلوك المستخدم وتفاعله مع الموقع لدينا، الأمر الذي يعطي النظام ميزة الدقة المتزايدة بمرور الوقت، حيث كلما ازدادت تفاعلات المستخدم مع النظام كلما تم الحصول على نتائج ذات دقة أعلى وكفاءة أفضل، حيث نلاحظ أن فرق الدقة بين الحل المقترح من قبل الباحث وأفضل خوارزمية كان بمقدار 0. 516809% عند تطبيق الحل على قاعدة البيانات الأساسية، وكان الفرق 2.8819% عند تطبيق الحل على قاعدة البيانات الموسعة، علماً بأن دقة الخوارزمية ازدادت بعد زيادة عدد سجلات قاعدة البيانات على عكس باقي الخوارزميات الأخرى والتي نقصت فيها الدقة بسبب عدم أخذ الخصائص المناسبة ضمن الحل، حيث كانت دقة الحل المقترح من قبل الباحث 97.97289% وأصبحت الدقة% 98.521776 بمقدار تحسن يبلغ 0.548886% .

يوضح الشكلان التاليان فرق الدقة بين الحل المقترح من قبل الباحث وبين الخوارزميات السابقة في مرحلتي المقارنة على قاعدة البيانات الأساسية وقاعدة بيانات **Kaggle:**



الشكل(6) يوضح مقارنة الدقة بين الحل المقترح والخوارزميات الأكثر استخداماً على قاعدة البيانات الأساسية

كما يظهر الشكل التالي مقارنة الدقة بين الحل المقترح من قبل الباحث والخوارزميات الأكثر استخداماً ،في حالة قاعدة البيانات الموسعة:



الشكل(7) يوضح مقارنة الدقة بين الحل المقترح والخوارزميات الأكثر استخداماً على قاعدة البيانات الموسعة

2- **السرعة:** تمت دراسة السرعة في هذا البحث من خلال ارتباط سرعة التنفيذ بعدد السجلات التي تقوم الخوارزميات بمسحها خلال كل عملية كشف للاحتيال، ومن المعروف أن عدد السجلات الموجودة في جدول المناقلات بين المستخدمين وموقع التجارة الإلكترونية أكبر بكثير من عدد سجلات جدول المستخدمين ضمن الموقع، ففي مجموعة البيانات الأساسية Kaggle كان عدد السجلات 284804 في جدول المناقلات بينما عدد السجلات الخاصة بالمستخدمين 4112 وفي مجموعة البيانات الموسعة عدد السجلات الخاصة بالمناقلات كانت ، وعليه فإن الحل المقدم من قبل الباحث يعتبر ذو سرعة أفضل من باقي

الخوارزميات من ناحية الزمن اللازم لمسح قاعدة البيانات حيث يقوم الحل المقترح من قبل الباحث على مسح جدول المستخدمين بينما تقوم باقي الخوارزميات بمسح كامل جدول المناقلات وذلك للكشف عن المناقلة الحالية هل هي شرعية أم أنها عملية احتيالية، وبالتالي فإن زمن التنفيذ الخاص بالحل المقترح من قبل الباحث أفضل بكثير من الخوارزميات السابقة.

لم يقم الباحث بدراسة تفصيلية للمقارنة بين زمن التنفيذ الخاص بالحل المقترح وبين زمن التنفيذ الخاص بالخوارزميات السابقة من الناحية العددية ، وعليه يجدر أن يكون هذا الأمر بحثاً مستقبلاً مهماً ولا سيما إذا أردنا التحسين على الخوارزميات السابقة أو على الحل المقترح من قبل الباحث.

3- **قابلية التطوير**: يتميز الحل المقدم من قبل الباحث بالاعتماد على مبدأ الاستقلالية في تقديم الحل ، حيث من الممكن التعديل على الحل بشكل كلي أو التطوير على جزء محدد دون الحاجة إلى إعادة بناء النظام ككل، حيث أن النظام يعتمد على جمع المعلومات عن المستخدم من خلال أجزاء برمجية مستقلة عن بعضها البعض وموزعة على كامل الموقع، وبالتالي فإن عملية التعديل على خاصية من الخصائص أو إضافة خاصية ما أو حذف خاصية يتطلب تعديل بسيط على قاعدة البيانات وتعديل على مكان واحد ضمن الموقع ، وبالتالي تتميز عملية التطوير بالسهولة والمرونة.

المراجع

1- PORWAL،U & MUKUND،S،2019- Credit card fraud detection in e-commerce. IEEE ،287P.

2- CAO، R & LIU، G& JIANG، C،2021- Two-level attention model of representation learning for fraud detection.IEEE، 1301P.

3- ZAHI،Y & SONG، W & LIU، X. &ZHAO، X،2018- A chi-square statistics based feature selection method in text classification. ICSESS،195P.

4- ALETH،K and SAMANTH،Y 2023-Using Kaggle.com database in fraud Detection System Using KNN and Navie Bayes. IEEE، P64.

5- PATIDAR،R & SHARMA،L،2021- Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering (IJSCE)، 112P.

6- RAPTIDAR ,R, 2021- Fraud Detection using GA and AI.IEEE, P128.

7- KEVORT,A-2018. Faud Dtection Using Decision tree and Smote Decision Tree. IEEE , P83.

8- HOLLAND,J-2021. Using logistic Regression and KNN to detect fraud Transaction in e-Commerce. IEEE, P32.

9- ALI، S &ABD AL RAZAK،K &Othman، H، & Al-Dhaqm، M،2022- Financial fraud detection based on machine learning.Appl. Sci، 98P.

10- PATIDAR،R & SHARMA،L،2021- Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering (IJSCE)، 112P.

11- LIUXGU، X، and SHANG،C، 2020-Quantitative detection of financial fraud based on deep learning with combination of E-commerce big data. IEEE P128.