Studying and Detecting of Security Attacks on Fog Computing Systems using Blockchain

Dr. Ahmed Saqr Ahmed [*]
Dr. Inas Laila [**]
Hussein Ali Shaaban [***]

(Received 9 / 3 / 2024. Accepted 6 / 8 / 2024)

□ ABSTRACT □

Fog computing extends cloud computing capabilities to the edge of the network, bringing computing and storage closer to users and devices as this distributed architecture improves the efficiency of data processing and analysis while reducing latency.
In the context of security, fog computing faces many challenges such as securing communication between distributed devices, ensuring data integrity, and protecting against malicious attacks. It has been shown that traditional security measures may not be sufficient to address these challenges due to the dynamic and decentralized nature of fog computing systems. Hence the use of block chain technology in fog computing, where a secure and tamper-resistant distributed ledger (Distributed Ledger Technology (DLT)) can be used to verify the integrity of data and transactions. Blockchain's decentralized consensus mechanism enhances the reliability and resilience of fog computing networks, making them more robust against security attacks. In this research, we studied and evaluated security attacks on fog computing networks and studied the impact of integrating block chains to enhance security measures in fog computing systems through the use of smart contracts. We used IfogSim to simulate fog computing, and the LOIC TOOLS tool to implement security attacks. The results showed the benefit of the block chain. This reduces the effectiveness of attacks by improving performance and network utilization by 68.17% and reducing delay by 68.26% in the presence of a DDOS attack.

Keywords: cloud computing - fog computing - block chain - smart contract – DDOS ATTACK

[*]**Doctor - Department of Computer Systems and Networks Engineering - Faculty of Information Engineering - Tishreen University - Lattakia – Syria--Email Address : ahmad.s.ahmad@tishreen.edu.sy**
**** Doctor- Department of Computer Systems and Networks Engineering - Faculty of Information Engineering - Tishreen University - Lattakia – Syria-Email Address : Dr.inas.laila8@gmail.com**
*****Graduate student - Master's - Department of Computer Systems and Networks - Faculty of Information Engineering - Tishreen University - Lattakia - Syria -Email Address : Husianshaban19962981@gmail.com**

دراسة وكشف الهجمات الأمنية على أنظمة الحوسبة الضبابية باستخدام سلسلة الكتل

د. أحمد صقر أحمد*

د. إناس ليلى**

حسين علي شعبان***

(تاريخ الإيداع 9 / 3 / 2024. قُبِل للنشر في 6/ 8 / 2024)

□ ملخّص □

تعمل الحوسبة الضبابية على توسيع قدرات الحوسبة السحابية إلى حافة الشبكة، مما يجعل الحوسبة والتخزين أقرب إلى المستخدمين والأجهزة حيث تعمل هذه البنية الموزعة على تحسين كفاءة معالجة البيانات وتحليلها مع تقليل زمن الوصول. في سياق الأمن، تواجه الحوسبة الضبابية العديد من التحديات مثل تأمين الاتصال بين الأجهزة الموزعة، وضمان سلامة البيانات، والحماية من الهجمات الضارة وقد تبين أن التدابير الأمنية التقليدية قد لا تكون كافية لمواجهة هذه التحديات بسبب الطبيعة الديناميكية واللامركزية لأنظمة حوسبة الضباب. ومنه ظهر استخدام تقنية سلسلة الكتل في الحوسبة الضبابية حيث يمكن استخدام دفتر أستاذ موزع (**Distributed Ledger Technology (DLT)**)آمن ومقاوم للتلاعب للتحقق من سلامة البيانات والمعاملات. تعمل آلية الإجماع اللامركزية الخاصة بسلسلة الكتل على تعزيز موثوقية ومرونة شبكات الحوسبة الضبابية، مما يجعلها أكثر قوة ضد الهجمات الأمنية . حيث قمنا في هذا البحث بدراسة وتقييم الهجمات الأمنية على شبكات الحوسبة الضبابية ودراسة تأثير دمج سلاسل الكتل لتعزيز التدابير الأمنية في أنظمة الحوسبة الضبابية وذلك من خلال استخدام العقود الذكية، حيث استخدمنا IfogSim لمحاكاة الحوسبة الضبابية، وأداة LOIC TOOLS لتنفيذ الهجمات الأمنية ،أظهرت النتائج فائدة سلسلة الكتل في تخفيف فعالية الهجمات ذلك من خلال تحسين الأداء واستخدامية الشبكة بنسبة 68.17% وتقليل التأخير بنسبة 68.26% بوجود هجومDDOS.

الكلمات المفتاحية :الحوسبة السحابية –الحوسبة الضبابية – سلسلة الكتل – العقد الذكي – هجوم DDOS

* دكتور– قسم هندسة النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية
ahmad.s.ahmad@tishreen.edu.sy

** دكتور مشرف– قسم هندسة النظم والشبكات الحاسوبية – كلية الهندسة المعلوماتية – جامعة تشرين – اللاذقية – سورية
Dr.inas.laila8@gmail.com

*** طالب دراسات عليا – ماجستير – قسم النظم والشبكات الحاسوبية – كلية الهندسة المعلومايتة – جامعة تشرين – اللاذقية – سورية
Husainshaban19962981@gmail.com

مقدمة:

اكتسبت الحوسبة السحابية أهمية كبيرة في السنوات الأخيرة وأصبحت ركيزة مهمة في عمل التطبيقات والأجهزة بحيث تم نقل أعباء الأعمال والتطبيقات والأجهزة العديدة المتصلة بالشبكة من مراكز البيانات إلى المراكز الكبرى للسحابة، ومع انتشار تقنيات إنترنت الأشياء IoT تزايدت أهمية الحوسبة السحابية، فأصبح اعتماد الأجهزة والتطبيقات عليها كبيراً جداً، ولكن نظراً لكثرة الأجهزة التي تولد كميات كبيرة من البيانات وتتطلب سرعة كبيرة من السحابة أصبحت الأخيرة تواجه صعوبات عديدة مع نمو هذه الأجهزة وتطورها وزيادة أعداد الأجهزة الذكية المتصلة بالشبكة، يضاف لذلك حاجة إنترنت الأشياء لنطاق تردد عريض لا تستطيع شبكة الإنترنت الحاليّة توفيره، مما يخلق مشاكل كبيرة في إرسال البيانات للسحابة، لذلك أتت فكرة الحوسبة الضبابية Fog Computing لحل هذه المشكلة من خلال إرسال البيانات لأجهزة قريبة واستلام الرد منها في وقت قصير حيث تقدم الحوسبة الضبابية زمن قليل لنقل المعلومات وسرعة كبيرة في أداء الأعمال ووقت استجابة قليل بالمقارنة بالحوسبة السحابية بالاضافة إلى توفير الطاقة وانخفاض تكاليف التشغيل من خلال تخفيض حركة البيانات عبر الشبكة ، حيث يضفي نموذج الحوسبة الضبابية اللامركزية على الخدمات التي تقدمها السحابة و يتيح الضباب تصفية البيانات وتجميعها ومعالجتها على حافة الشبكة مما يؤدي إلى تحسين جودة الخدمة (QoS) [1].

إن ظهور الحوسبة الضبابية ساعد في حل هذه المشاكل التي تواجهها الحوسبة السحابية وترتب عليه بعض المشاكل في الموثوقية والأمان بين أجهزة انترنت الأشياء ومخدمات الحوسبة الضبابية ومن هنا ظهر فكرت دمج سلسلة الكتل مع حوسبة الضباب لحل جميع مشاكل الأمان والموثوقية [2]. بالتعريف سلسلة الكتل هي شبكة مستقلة، ولا تخضع لأيّ سلطة مركزية, لأنها في الأساس سجل مُشترك وغير قابل للتغيير، والمعلومات الموجودة فيها مفتوحة ومُتاحة لأيّ شخص لكي يطّلع عليها ولكن حرية التعديل ليست متاحة للجميع. إن البنية الأساسية التي تعتمد عليها سلسلة الكتل في عملها هي العقد الذكي وهو كود قابل للتنفيذ يتم تشغيله على شبكة سلسلة الكتل لتسهيل شروط الاتفاقية بين الأطراف غير الموثوق بها ، مقارنة بالعقود التقليدية ، لا تعتمد العقود الذكية على طرف ثالث موثوق به للعمل ، مما يؤدي إلى انخفاض مصاريف التحويلات حيث أن العقد الذكي هو في الواقع عقد ذاتي التنفيذ مع كتابة شروط الاتفاقية بين طرفي الاستخدام مباشرة في سطور من التعليمات البرمجية [3].

عند اكتشاف هجوم DDOS محتمل ، تتفاعل عقدة الضباب مع العقد الذكي المنتشر على شبكة سلسلة الكتل (باستخدام Ganache) لتشغيل بروتوكول منع DDOS المحدد مسبقاً، ترسل عقدة الضباب المعلومات ذات الصلة حول الهجوم مثل عناوين IP المصدر ، وخصائص الهجوم إلى العقد الذكي.

لتخفيف DDOS ينفذ العقد الذكي مجموعة من القواعد والسياسات المبرمجة مسبقاً حيث يمكنه توزيع حركة المرور الواردة ديناميكياً ، أو تصفية الحزم الضارة ، أو إعادة توجيه حركة المرور إلى عقد مختلفة. تعتمد عملية صنع القرار هذه على تحليل المعلومات المستلمة والمنطق المحدد مسبقاً المشفر في العقد الذكي[3] .

وعموماً ، فإن الجمع بين الحوسبة الضبابية والعقود الذكية يوفر آلية قوية لتخفيف هجمات DDOS، من خلال الاستفادة من قوة المعالجة لعقد الضباب والتنفيذ الثابت للعقود الذكية ، يمكن تحديد الهجمات المحتملة وتحليلها والتخفيف منها بطريقة استباقية وفعّالة، ومنه يضمن نموذج الحوسبة الضبابية خدمات زمن انتقال منخفض لتطبيقات إنترنت الأشياء أثناء تحسين استخدام الشبكة ، بينما توفر تقنية سلسلة الكتل طريقة لامركزية لضمان سلامة البيانات والثقة والأمان.

أهمية البحث وأهدافه:

تكمن أهمية الحوسبة الضبابية مع انترنت الأشياء في تقليل زمن نقل المعلومات إلى مراكز الحوسبة السحابية للتخزين والمعالجة والتحليل مما يترتب عليه من سرعة كبيرة في أداء الاعمال ووقت استجابة قليل وتحقيق مستوى عالي من الأمان والموثوقية باستخدام سلاسل الكتل مع الحوسبة الضبابية .

يهدف هذا البحث إلى دراسة وتقييم الهجمات الأمنية على شبكات الحوسبة الضبابية والدور الاساسي للبلوكشين في تخفيف هجمات DDOS باستخدام العقود الذكية .

طرائق البحث ومواده:

يقضي الناس الكثير من الوقت في العثور على أماكن انتظار السيارات الشاغرة مما يؤدي بشكل أساسي إلى انبعاث ثاني أكسيد الكربون وإهدار الوقت و الوقود. لذلك زاد الاهتمام بمشاكل وقوف السيارات في السنوات القليلة الماضية واقترحت العديد من الأبحاث حلول مواقف السيارات القائمة على إنترنت الأشياء حيث سنقوم في هذا البحث بتصميم موقف سيارات ذكي قائم على مجموعه من الكاميرات وعقد الضباب ثم سنقوم بتطبيق هجوم DDOS على البنية السابقة وسنقوم بدراسة أثر الهجوم على عمل العقد الضبابية في حال إضافة سلاسل الكتل وفي حال عدم تطبيقها .

1-الدراسات المرجعية:

تعددت الدراسات المرجعية التي تناولت الحوسبة السحابية وفائدتها وضرورة الاعتماد على الحوسبة الضبابية بسبب الزيادة المستمره في عدد الأجهزة الذكية في جميع المجالات نتيجة لذلك كان لابد من الاهتمام بمجال الأمن في الحوسبة الضبابية وأهميه سلسلة الكتل في تخفيف الهجمات الأمنية والحماية من أي تهديد بسبب الطبيعة اللامركزية لها.

حيث قام الباحثون في [4] بدراسة حوسبة الضباب، والمقارنة مع الحوسبة السحابية وأثبتت الدارسة على الرغم من أن كل من السحابة والضباب يقدمان موارد وخدمات مماثلة، إلا أن الضبابية تتميز بزمن وصول منخفض مع انتشار أوسع وعقد موزعة جغرافيا لدعم التنقل والتفاعل في الزمن الحقيقي . كما وضّح الباحثون في [5] القيود المختلفة للحوسبة السحابية مثل التأخير العالي واستهلاك النطاق الترددي للمعلومات المرسلة، كان إنشاء حوسبة الضباب أمرا ضرورياً وركز هذا البحث على استخدام الحوسبة الضبابية كنهج دفاعي ضد التهديدات الأمنية المتزايدة يوما بعد يوم وخاصة هجمات DDoS في الحوسبة السحابية. اقترح الباحثون في [6] طريقة لكشف هجمات DDOS في الزمن الحقيقي باستخدام نهج يجمع بين قياس العشوائية لحركة المرور مع خوارزمية التعلم الآلي للجيران الأقرب (KNN) حيث تم تحليل جميع الحزم الواردة، واستخراج أربع بارمترات من كل حزمة (عنوان IP المصدر، وعنوان IP الوجهة، ومنفذ المصدر، ومنفذ الوجهة)، وحساب الاحتمالية، ثم حساب الإنتروبيا، ثم إرسال البيانات إلى طريقة الجوار k الأقرب لتقييم ما إذا كان هناك هجوم أم لا.

وقام الباحثون في [7] باقتراح نموذج Ethereum blockchain لاكتشاف ومنع هجمات DDoS ضد أنظمة إنترنت الأشياء. وبرهنوا إمكانية استخدام النظام المقترح لحل مشكلة نقاط الفشل الفردية (التبعيات على أطراف ثالثة) والخصوصية والأمان في أنظمة إنترنت الأشياء حيث تم تتبع وتسجيل عناوين IP للأجهزة الضارة داخل blockchain لمنعها من الاتصال والتواصل مع شبكات إنترنت الأشياء.

وفي [8] تم اقتراح نظام Fog Computing based Security (FOCUS) لحماية إنترنت الأشياء من الهجمات الإلكترونية للبرامج الضارة حيث تم تعين عتبه لعدد الحزم الواردة من جهة ما وحظرها في حال زاد عدد الطلبات عن العتبه المعطاة حيث تم استخدام VPN لتصفية الهجمات ومنعها .

في [9] اقترح الباحثون بنية Fog–Cloud التي تمكن Blockchain من ضمان الأمان وقابلية التوسع والخصوصية لأجهزة إنترنت الأشياء المتصلة عن بعد. حيث كانت البنية المقترحة تعمل على حل المشكلات الشائعة مثل التأخير المتزايد باستمرار واستهلاك الطاقة الذي يأتي مع تكامل Blockchain في بنية Fog–Cloud ، نستخدم شبكةBlockchain Ethereum في الطبقة الثانية والتي تعمل كطبقة ضباب مؤمنة لضمان زيادة الأمان .

كما اقترح الباحثون في [3] نظام مكتبي ذكي يعتمد على الحوسبة الضبابية. يتم تطبيق Blockchain لضمان أمان النظام بشكل عام ومصادقة المستخدم من خلال إنشاء محافظ في نظام blockchain. تم تنفيذ عملية المعاملة الشاملة باستخدام طريقة البيتكوين الشائعة حيث تم تنفيذ مشاركة المعلومات بمساعدة خوارزمية RSA ونظام التوقيع الرقمي. اي تم تحقيق الامان والموثوقية من خلال التوقيع الرقمي واستخدام خوارزميات التشفير .

و اقترح الباحثون في[10] استخدام Blockchain في بنية سحابة الضباب،بدلاً من استخدامها في طبقة الضباب وهذا يعني تقليل استخدام وحدة المعالجة المركزية بشكل كبير في طبقة الضباب مما يزيد من معالجة البيانات إلى الحد الأقصى.حيث يمكن لطبقة الضباب استدعاء أي منطق عقد ذكي إذا لزم الأمر .

ونلاحظ أن أغلب الدراسات المرجعية ركزت على الانتقال بالخدمات من الحوسبة السحابية إلى الضابية وأهمية الحوسبة الضبابية والتركيز على زيادة الهجمات الأمنية على الحوسبة الضبابية بسبب قربها من المستخدم بالإضافة لعملية دمج الحوسبة مع سلسلة الكتل لتنظيم العمل ومنه سنقوم في هذا البحث :

تطبيق هجمات DDOS على الحوسبة الضبابية ودراسة تأثيرها على التأخير واستخدامية الشبكة ووسنقوم بدراسة تأثير تطبيق سلسلة الكتل وميزاتها للتخفيف من ضرر المهاجمين على بيئة الحوسبة الضبابية .

2–الدراسة التجريبية :

أ–السيناريو الاول :

❖ –سنقوم ببناء نموذج لموقف سيارات ذكي يستخدم الحوسبة الضبابية وسيتم ذلك باستخدام محاكي Ifogsim وسنقوم بدراسة تأثير هجوم DDOSعليه وتقييم الأداء بناء على المعيارين التأخير و استخدامية الشبكة.

تتكون بنية مواقف السيارات القائمة على الضباب مما يلي[11]:

1–كاميرات ذكية : مهمتها التقاط الصور لأماكن وقوف السيارات بشكل دوري وإرسال الصور إلى العقد الضبابية .

2– عُقد الضباب : مهمتها معالجة الصور وتحديد الأماكن المتوفرة لوقوف السيارات وتوجيه السائقين لاقرب موقف متوفر .

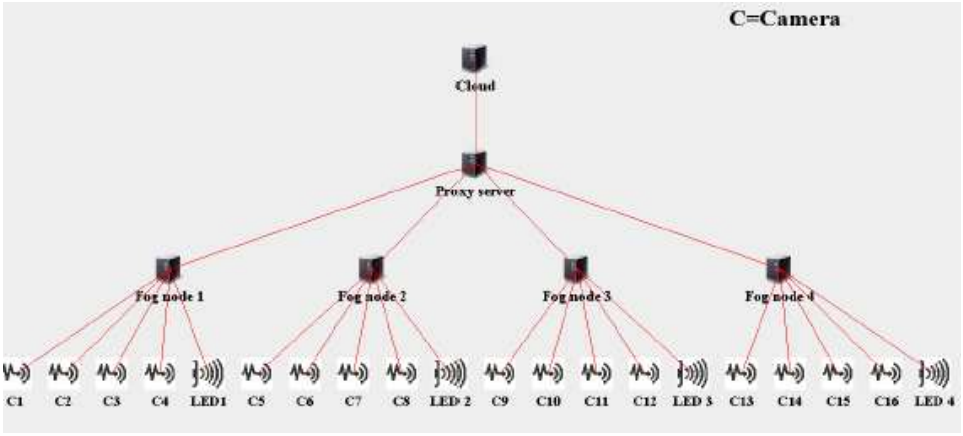
3– شاشات عرض الصمام الثنائي الباعث للضوء (LED) : تحديد فيما إذا كان الموقف متوفر أو مشغول من سيارة أخرى .

4– خادم وكيل: مهمته الربط بين عقد الحوسبة الضبابية والمساعدة على نقل المعلومات بين العقد الضبابية أي تنسيق عمل العقد الضبابية مع بعضها ثم إرسال تقرير بشكل دوري إلى الحوسبة السحابية .

5– خادم سحابي : مهمته معالجة وتخزين التقارير الدورية التي ترسلها العقد الضبابية .

تنتشر الكاميرات الذكية في كافه أنحاء المدينة والتي تلتقط صور أماكن وقوف السيارات وتنقل الصور إلى عقدة الضباب وذلك كل خمس ثواني ، والتي تقوم بدورها بتنفيذ خوارزمية معالجة الصور لتحديد أماكن الانتظار الشاغرة، وعليه يتم تحديث معلومات خانات الانتظار على مؤشر LED، ويتم تخزين البيانات في عقدة الضباب لفترة زمنية محدودة ، ثم يتم نقلها إلى الخادم السحابي بشكل دائم.

يوضح الشكل (1) البنية التي استخدمناها والمكونه من عقدة حوسبة سحابية مع خادم وسيط وأربع عقد ضبابية وعدد متغير من الكاميرات يتراوح عددها في بحثنا بين 16 الى 40 كاميرا .



الشكل (1) بنية الكراج الذكي

عندما تصل المركبة إلى بوابة الموقف المتوفر يتم تحديث المعلومات الموجودة على مؤشر LED ويعلن أن الموقف غير متوفر حاليا وبكل فاصل زمني مدته خمس ثوان يتم تحديث المعلومات على LED وإرسالها للعقد الضبابية لقراءة حالة الموقف بشكل دائم [11].

ونتيجة أننا في بيئات تتطلب أداء عالٍ في الزمن الحقيقي ستقوم الحوسبة الضبابية بتقليل التأخير وذلك بتخفيف الوصول المتكرر إلى السحابة وتنفذ العمليات في حافة الشبكة لتوفير استجابة سريعة لجهاز العميل وبالتالي تقليل التأخير حيث يتم إرسال صور مواقف السيارات إلى عقد الضباب للمعالجة المتواجدة في حافة الشبكة ، ومنه تم تعريف التأخير : أنه الزمن الذي تستغرقه الإشارات للتنقل في البنية التحتية للشبكة بمعنى مقدار الوقت الذي تستغرقه حزمة البيانات للانتقال من نقطة إلى أخرى ويحسب بالعلاقة (1) :

$$Latency = \alpha + \mu + \phi \qquad (1)$$

حيث أن :

- α : هو تأخير تنفيذ وحدة المعالجة المركزية Tuple للالتقاط الصور .
- μ : هو الوقت اللازم لتحميل الصور على عقدة الضباب للمعالجة .
- ϕ : هو الوقت المستغرق للعرض المعلومات إلى LED بعد معالجتها في عقدة الضباب.

وكما تعرف استخدامية الشبكة(Network Usage) بكمية البيانات التي يتم نقلها عبر الشبكة والذي يعد أمرا مهماً لأنه يؤثر على الأداء العام للنظام [11] وتعطى بالعلاقة (2) :

$$Network\ usage = Latency * \partial \qquad (2)$$

حيث تعرف ∂ بانها : حجم البيانات المراد نقلها وقد يشمل حجم الرسائل أو البيانات التي ترسل عبر الشبكة

بعد إجراء المحاكات وحساب قيم التأخير واستخدامية الشبكة في الحوسبة الضبابية وذلك مع تزايد عدد الكاميرات من 16 الى 40 مع المحافظة على عدد عقد الضباب الموجودة بدون وجود أي هجوم ، نلاحظ أن التأخير واستخدامية الشبكة يتزايدان بزيادة عدد الكاميرات من وذلك بسبب تزايد عدد الطلبات التي يتم إرسالها الى خوادم الحوسبة الضبابية يوضح الجدول (1) قيم التأخير واستخدامية الشبكة مع تزايد عدد الكاميرات :

الجدول (1) التأخير واستخدامية الشبكة في الحوسبة الضبابية

Camera	Latency (MS)	Total network usage (KB)
16	767	2371
20	861	3271
24	953	4332
28	1034	5500
32	1256	7636
36	1384	8892
40	1464	11126

سنقوم الان بدراسة تأثير هجوم DDOS على القعد الضبابية، والذي يحاول فيه المهاجم جعل خدمة معينة غير متاحة عن طريق توجيه حركة مرور مستمرة وكبيرة من أنظمة نهائية متعددة. والذي يدعو إلى استخدام موارد الشبكة في خدمة طلبات تلك الأنظمة الطرفية الخاطئة ، بحيث يتعذر على المستخدم الشرعي الحصول على الخدمة التي كانت متاحة له [4].

سنقوم باستخدام الأداة LOIC TOOLS لتنفيذ الهجوم والتي نحدد فيها عنوان IP الخاص بعقدة الوصل والربط بين العقد الضبابية proxy node والتي تربط وتنقل المعلومات بين عقد الضبابية لتعمل كوحدة متكاملة معاً حيث نقوم بتنفيذ الهجوم بعدد مهاجمين و زمن نقوم بتحديده من خلال هذه الأداة حيث يوضح الشكل (2) تنفيذ هجوم DDOS على العنوان 192.168.1.100 بعدد مهاجمين 1000 مهاجم :

الشكل (2) هجوم DDOS

اظهرت نتائج المحاكاة بعد تنفيذ هجمات DDOS إلى زيادة التأخير بشكل كبير وذلك بسبب إغراق البنية التحتية للحوسبة بكمية هائلة من الطلبات أو حركة المرور الزائفة. ونتيجة لذلك، تعاني حزم البيانات المشروعة من تأخيرات في المعالجة والنقل.

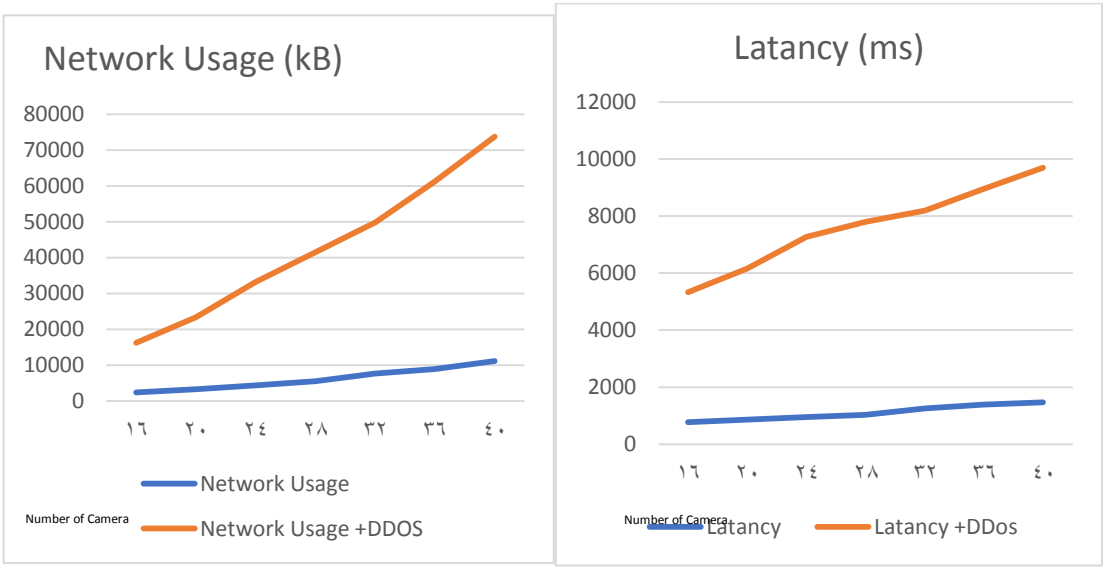
كما نلاحظ ارتفاع استخدامية الشبكة حيث تحاول البنية التحتية للحوسبة الضبابية التعامل مع الحجم الزائد للطلبات الواردة والصادرة. مما يؤدي إلى الازدحام، وبطء نقل البيانات، وانقطاع الخدمة المحتمل للمستخدمين الشرعيين.

يوضح الجدول (2) التأخير واستخدامية الشبكة عند تطبيق هجوم DDOS في الحوسبة الضبابية .

الجدول (2) التاخير واستخدامية الشبكة في الحوسبة الضبابية مع هجوم DDOS

Camera	Latency (MS)	Total Network Usage(KB)
16	5334	16215
20	6159	23402
24	7274	33169
28	7801	41501
32	8192	49807
36	8954	61243
40	9701	73727

يوضح الشكل (3) التأخير واستخدامية الشبكة في الحوسبة الضبابية وذلك مع هجوم DDOS وبدونه حيث توضح النتائج التأثير الكبير للهجوم على كل من التأخير واستخدامية الشبكة وازديادها بشكل ملحوظ , وهذا بسبب الطلبات الزائفة المولدة بسبب الهجوم.



الشكل (3) التاخير واستخدامية الشبكة في الحوسبة الضبابية مع هجوم DDOS وبدونه

ب-السيناريو الثاني :

سنقوو في هذا السيناريو بدراسة تأثير تطبيق سلسلة الكتل والعقود الذكية في تخفيف تأثير هجوم DDOS في الحوسبة الضبابية

إ-سلسلة الكتل (البلوكشين)

سلسلة الكتل: هو نظام تسجيل مشترك لامركزي يستخدم لتخزين وتبادل البيانات أو العملات الرقمية، ويتميز بأنه لا يمكن تعديل السجل المنشور فيه ولا يُمكن إضافة أو حذف أي بيانات منه دون موافقة معظم المستخدمين في النظام. ويعتمد هذا النظام على تقنية التشفير المعروفة باسم "Cryptographic Hash" لحفظ بيانات العمليات والتعاملات بشكل آمن وغير قابل للاختراق أو التلاعب بها، ويستخدم في عدد من المجالات وخاصة في تبادل العملات الرقمية مثل البيتكوين[12-13].

يمكن تنفيذ تقنية سلسلة الكتل لحماية الحوسبة الضبابية Fog computing من الهجمات DDoS بالطرق التالية:

1. استخدام سلسلة الكتل المصرح بها: يمكن لـ Fog nodes التواصل عبر شبكات سلسلة الكتل المصرح بها التي يسمح الوصول إليها فقط للجهات المعتمدة. وهذا يعزز الأمان بالمقارنة مع شبكات سلسلة الكتل العامة لأنه يضمن أن العُقد المعتمدة فقط يمكنها التفاعل مع سلسلة الكتل.

2. عدم القابلية للتغيير: تضمن تكنولوجيا سلسلة الكتل عدم إمكانية حذف أو تعديل البيانات. يمكن لعقد الضباب استخدام تقنية سلسلة الكتل لتخزين المعلومات حول من يستخدم الشبكة، ومتى ترسل عقدة طلباً، أو متى تقوم عقدة معينة بتنفيذ عملية محددة.

3. لامركزية الحساب والتخزين: يخدم الدفتر اللامركزي لشبكة سلسلة الكتل كمنصة مثالية لنشر أنواع مختلفة من التطبيقات والخدمات التي تكون لامركزية، وديناميكية، وقابلة للتوسع. يمكن للامركزية الحساب والتخزين تقليل بشكل كبير من خطر هجمات DDoS، حيث توفر الأنظمة الموزعة بشكل طبيعي مزيدا من المرونة والتخفيف من اثر للهجمات.

4. استخدام العقود الذكية: يمكن استخدام العقود الذكية لفرض سياسات التحكم في الوصول والأمان مثل منع العُقَد غير المصرح بها من الانضمام إلى الشبكة أو تحديد حجم الموارد الحسابية التي يمكن لعقدة ما استخدامها. يمكن للعقود الذكية الكشف عن هجمات DDoS والاستجابة لها تلقائيا. إذا حدد النظام طلبات غريبة يمكن أن تكون هجوما DDoS (على سبيل المثال، طلبات متعددة من عنوان IP نفسه في وقت قصير جدا)، فسيتم رفض الطلب تلقائيا.

من خلال استغلال تقنية سلسلة الكتل ، يمكن للحوسبة الضبابية تحقيق درجات عالية في الأمن والصمود ضد هجمات DDOS ومنه تم استخدام العقد الذكي[14] .

العقود الذكية هي عقود ذاتية التنفيذ مع شروط الاتفاقية مكتوبة مباشرة في التعليمات البرمجية. إنهم يفرضون تلقائيا القواعد والشروط المحددة مسبقا ، مما يضمن تنفيذها الشفاف وغير القابل للتغيير. في حالة منع DDOS ، يمكن استخدام العقود الذكية لتنفيذ مجموعة من القواعد والسياسات للكشف عن مثل هذه الهجمات والتخفيف منها.

لنوضح الأن ألية عمل الحوسبة الضبابية مع العقود الذكية لمنع الهجوم :

عند اكتشاف هجوم DDOS محتمل ، تتفاعل عقدة الضباب مع العقد الذكي المنتشر على شبكة سلسلة الكتل (باستخدام Ganache) لتشغيل بروتوكول منع DDOS المحدد مسبقا. ترسل عقدة الضباب المعلومات ذات الصلة حول الهجوم مثل عناوين IP المصدر ، وخصائص الهجوم ، وما إلى ذلك، إلى العقد الذكي.

ينفذ العقد الذكي مجموعة من القواعد المبرمجة مسبقا حيث يمكنه توزيع حركة المرور الواردة ديناميكيا ، أو تصفية الحزم الضارة ، أو إعادة توجيه حركة المرور إلى عقد مختلفة. [15]

بعد تطبيق تدابير التخفيف اللازمة ، يقوم العقد الذكي بتحديث عقدة الضباب بمعلومات تتعلق بالإجراء المتخذ. يمكن لعقدة الضباب إبلاغ مالكي الأجهزة بالهجوم المكتشف وخطوات التخفيف التي تم إجراؤها.

وعموما ، فإن الجمع بين الحوسبة الضبابية والعقود الذكية يوفر آلية قوية لمنع هجمات DDOS. من خلال الاستفادة من قوة المعالجة لعقد الضباب والتنفيذ الثابت للعقود الذكية ، يمكن تحديد الهجمات المحتملة وتحليلها والتخفيف منها بطريقة استباقية وفعالة.

سنقوم بكتابة عقد ذكي (Smart Contract) يقوم بما يلي :

عندما يصل من ip معين عدد طلبات أكثر من عتبه نقوم بتحديدها وليكن 1000 طلب خلال مدة نقوم بتحديدها يعتبر هذه الشخص مهاجم وعند ذلك يتم إضافته الى اللائحه السوداء ويتم منع جميع الطلبات التي تأتي منه .

-خطوات تنفيذ العقد الذكي [16]:

- Smart contract: نستخدم لغة SOLIDTY لكتابته .
- Migration : الهجرة وهي عملية الاختبار الأولية للعقد الذكي للتأكد من صحته وقابلية نشره .
- Test Contract : الاختبار أو النشر بحيث يصبح العقد غير قابل للتعديل بمعنى بعد هذه الخطوة يصبح هناك نسخة من العقد موثقة ومنتشرة على مجموعه من العقد المخولة لها باحتواء نسخه منه .

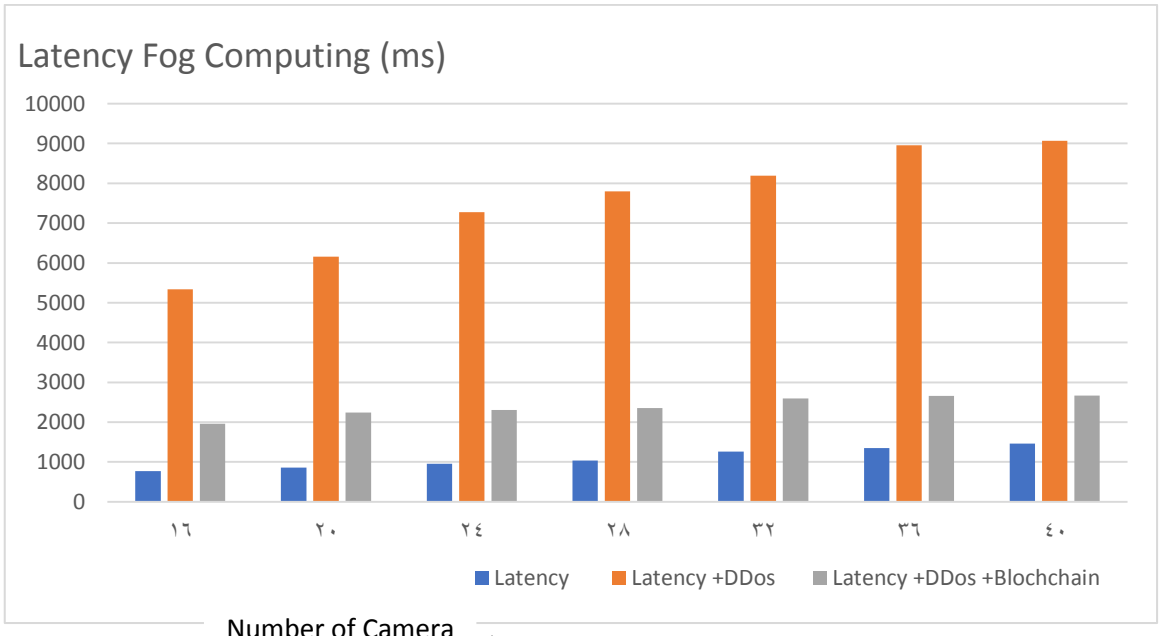
ونلاحظ أنه بعد كتابة العقد الذكي ونشره في الشبكة وتطبيق هجوم DDOSعليه أن التأخير في الشبكة قد انخفض واستخدامية الشبكة قد تحسنت ويعود ذلك الى القواعد التي تم كتابتها في العقد الذكي والتي عملت على حظر المستخدمين الذين قاموا بإرسال طلبات تجاوزت العتبة المحددة واعتبارهم مهاجمين .

يوضح الجدول (4) التأخير واستخدامية الشبكة عند تطبيق العقد الذكي في الشبكة المعرضة للهجوم .

الجدول (4) التأخير واستخدامية الشبكة بعد تطبيق العقد الذكي

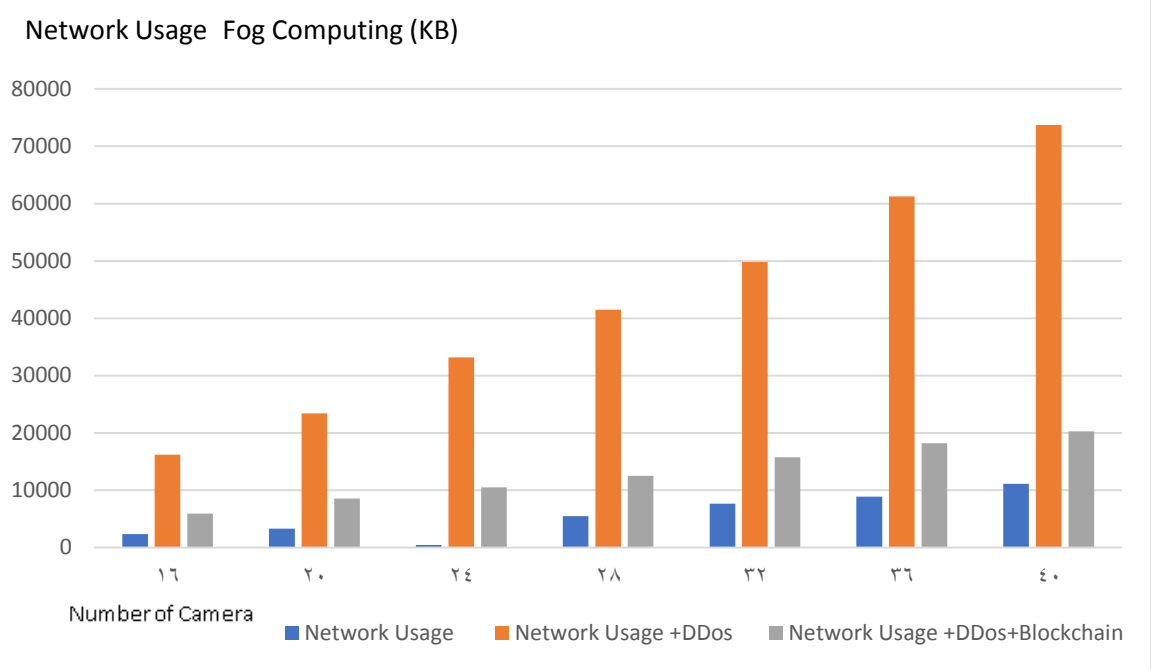
Camer	Latency fog(MS)	Network Usage fog (KB)
16	1957	5949
20	2242	8519
24	2301	10492
28	2354	12523
32	2595	15777
36	2660	18194
40	2666	20261

يوضح الشكل (4) التأخير في الحوسبة الضبابية في ثلاث حالات ، الحالة العادية بدون وجود هجوم وعند وجود هجوم DDOS وعند تطبيق العقود الذكية مع وجود الهجوم مما يوضح التأثير الإيجابي لتطبيق العقد الذكي في التقليل من تأثير الهجوم .



الشكل (4) التاخير في الحوسبة

كما يوضح الشكل (5) حساب لاستخدامية الشبكة في الحوسبة الضبابية في الحالة العادية وعند وجود هجوم DDOS وعند تطبيق العقود الذكية لتخفيف هذه الهجمات حيث نصت فكرة العقد الذكي على منع الطلبات المرسله من أي جهة ترسل أكثر من 1000 طلب في الثانية واعتبرها هجوم وبالتالي نلاحظ انخفاض لاستخدامية الشبكة مع استمرار الهجوم لكن بالحدود الدنيا والذي سوف نسعى إليه بدراستنا المستقبلة لمنع الهجوم مباشره من أول سلوك للمهاجم ونسعى للوصل إلى أفضل قيمه مقاربة لاستخدامية الشبكة في الحالة العادية .



الشكل (5)استخدامية الشبكة في الحوسبة الضبابية

الاستنتاجات والتوصيات:

قمنا في هذا البحث بتحليل بنية سحابة الضباب القائمة علىblockchain حيث قمنا بتطبيق هجوم DDOS على البنية الخاصة بنا واستخدمنا العقد الذكي لتخفيف الهجوم واستنتجنا مما سبق :

- تأثر أداء الشبكة وازدياد التأخير والاستخدامية عند تطبيق هجوم DDOS .
- تعمل الحوسبة الضبابية على تحسين كفاءة معالجة البيانات وتقليل زمن الوصول.
- تحسن استخدامية الشبكة بنسبة 68.17% والتأخير بنسبة 68.26 عند استخدام العقود الذكية وسلسلة الكتل مع وجود هجوم DDOS مما ينعكس إيجابا على الشبكة .

➢ ومنه نوصي بما يلي :

- استخدام تقنية سلسلة الكتل وآلية الإجماع اللامركزية لتعزيز أمان وموثوقية الحوسبة الضبابية.
- تكامل العقود الذكية لتعزيز التدابير الأمنية في أنظمة الحوسبة الضبابية.
- الاستفادة من فوائد سلسلة الكتل في تخفيف فعالية الهجمات وتحسين الأداء والإنتاجية.
- توجيه الاهتمام نحو مزيد من البحوث والتطوير في مجال استخدام سلسلة الكتل في الحوسبة الضبابية لتعزيز الأمان والكفاءة.

ويمكننا دراسة تطبيق سلسلة الكتل في نماذج اخرى كالمدن الذكية. كما يمكن تطوير نظام مصادقة المستخدم بشكل أكبر لضمان التحكم في الوصول بشكل أفضل وكما يمكننا دراسة هجمات أمنية أخرى وليس فقط هجوم DDOS ومقارنة النتائج التي حصلنا عليها مع طرائق أخرى للكشف كاستخدام الذكاء الاصطناعي مع العقود الذكية في بيئة الحوسبة الضبابية .

References:

[1]- Osanaiye O, Chen S, Yan Z, Lu R, Choo K-KR, Dlodlo M. From cloud to fog computing: A review and a conceptual live VM migration framework. IEEE Access [Internet]. 2017;5:8284–300. Available from: https://ieeexplore.ieee.org/document/7896564

[2]- Ashik MH, Maswood MMS, Alharbi AG. Designing a fog-cloud architecture using blockchain and analyzing security improvements. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE; 2020,Available from: http://dx.doi.org/10.1109/ICECCE49384.2020.9179374

[3]- Tabassum A, Jeba HA, Mahi TK, Reza SMS, Hossain DA. Securely Transfer Information with RSA and Digital Signature by using the concept of Fog Computing and Blockchain. In: 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD). IEEE; 2021, Available from: http://dx.doi.org/10.1109/ICICT4SD50815.2021.9396987

[4]- Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Gener Comput Syst [Internet]. 2009;25(6):599–616. Available from: http://dx.doi.org/10.1016/j.future.2008.12.001

[5]-Khan A ur R, Othman M, Madani SA, Khan SU. A survey of mobile cloud computing application models. IEEE Commun Surv Tutor [Internet]. 2014;16(1):393–413. Available from: http://dx.doi.org/10.1109/surv.2013.062613.00160

[6]- Paharia B, Bhushan K. Fog computing as a defensive approach against distributed denial of service (DDoS): A proposed architecture. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE; 2018,Available from: https://doi.org/10.1109/ICCCNT.2018.8494060

[7]-Ibrahim RF, Abu Al-Haija Q, Ahmad A. DDoS attack prevention for Internet of thing devices using Ethereum blockchain technology. Sensors (Basel) [Internet]. 2022;22(18):6806. Available from: http://dx.doi.org/10.3390/s22186806

[8]-Hassan KF, Manaa ME. Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach. Bull Electr Eng Inform [Internet]. 2022;11(3):1604–13. Available from: http://dx.doi.org/10.11591/eei.v11i3.3643

[9]- Ashik MH, Maswood MMS, Alharbi AG. Designing a fog-cloud architecture using blockchain and analyzing security improvements. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE; 2020,Available from: http://dx.doi.org/10.1109/ICECCE49384.2020.9179374

[10]- Ashik MH, Islam T, Hasan K, Lim K. A blockchain-based secure fog-cloud architecture for internet of things. In: 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE; 2021, Available from: http://dx.doi.org/10.1109/CSCloud-EdgeCom52276.2021.00010

[11]- Awaisi KS, Abbas A, Zareei M, Khattak HA, Shahid Khan MU, Ali M, et al. Towards a fog enabled efficient car parking architecture. IEEE Access [Internet]. 2019;7:159100–11. Available from: http://dx.doi.org/10.1109/access.2019.2950950
[12]- Tkachuk R-V, Ilie D, Tutschku K, Robert R. A survey on blockchain-based telecommunication services marketplaces. IEEE Trans Netw Serv Manag [Internet]. 2022;19(1):228–55. Available from: http://dx.doi.org/10.1109/tnsm.2021.3123680
[13]- Sanghi N, Bhatnagar R, Kaur G, Jain V. BlockCloud: Blockchain with Cloud Computing. In: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE; 2018,Available from: http://dx.doi.org/10.1109/ICACCCN.2018.8748467
[14]- Ashik MH, Islam T, Hasan K, Lim K. A blockchain-based secure fog-cloud architecture for internet of things. In: 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE;2021, p. 1–3.Available from : http://dx.doi.org/10.1109/CSCloud-EdgeCom52276.2021.00010
[15]- Agarwal U, Rishiwal V, Tanwar S, Chaudhary R, Sharma G, Bokoro PN, et al. Blockchain technology for secure supply chain management: A comprehensive review. IEEE Access [Internet]. 2022;10:85493–517. Available from: http://dx.doi.org/10.1109/access.2022.3194319
[16]- Prabavathy S, Reddy IRP. Fog computing based distributed denial of service attack detection method for large-scale internet of things. In: 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE; 2023.;Available from : https://doi.org/10.1109/SPIN57001.2023.10116991