العدد الخامس عشر
تاريخ الإصدار: 2 – كانون الثاني – 2020 م
www.ajsp.net
ISSN: 2663-5798

"دور المواقع السحابية وبوابات المستخدم القائمة على بلوكتشاين في وقاية الحاسب من الأخطار"

إعداد الباحثة

عزيزة عبدالله إبراهيم الصعب

وزارة التعليم السعودية

معلومات التواصل

azizahsaab@gmail.com

العدد الخامس عشر
تاريخ الإصدار: 2 – كانون الثاني – 2020 م
www.ajsp.net
ISSN: 2663-5798

الملخص

هدفت هذه الدراسة إلى معرفة مدى الحماية التي تقدمها المواقع السحابية وبوابات المستخدم القائمة على بلوكشين للحاسب من الأخطار، وفي سبيل ذلك اعتمدت الباحثة على تحميل عدد 50 ملفاً من 6 مواقع سحابية، ثم العمل على فحص مدى أمانها باستخدام برامج الحماية (Avira & AVG)، وخلصت النتائج إلى أن بوابات المستخدم تقدم هذه الحماية فعلياً، بينما لا تقدمها الحوسبة السحابية بشكل فعال، ورأت الباحثة ضرورة اهتمام المؤسسات بأن يكون لها حوسبة سحابية خاصة مستقلة عن الحوسبة السحابية العامة التي يستخدمها الأفراد.

الكلمات المفتاحيّة: بوابات المستخدم، بلوكشين، حوسبة سحابية

المقدّمة:

في ظل التطوير المستمر للمؤسسات الحكومية والخاصة، والاستغناء الدائم عن العنصر البشري، وغلبة العناصر الحاسوبية؛ ظهرت مشاكل الحماية والأمان اللذان يجب أن تتمتع بهما كل من بيانات المستخدمين، والحواسيب المتصلة بنفس الشبكة على حد سواء، وبدأ العمل من جانب المؤسسات المتخصصة بالتكنولوجيا، مدفوعة من المؤسسات التي تبحث عن أمن معلوماتها، وخصوصية بيانات مستخدميها، بالبحث عن وسائل تحقق هذه الحماية، فظهر ما يسمى ببوابات المستخدم، والتي استمر تحديثها بشكل مستمر إلى وقتنا الحالي لتظهر كل من (IBM Watson)، وبوابات المستخدم القائمة على (BlockChain)، كما ظهرت في مجال حماية الحواسيب من الأخطار الفيروسية، والبرامج الخبيثة ما يسمى بالمواقع السحابية، التي يفترض فيها خلوها من أي تقنيات مضرة بالحاسب وبالمعلومات، وكذلك استمرارية حفاظها على بيانات المستخدمين لها.

ونتيجة لذلك رأت الباحثة ضرورة أن ينصب بحثها على هذه التقنيات، ومعرفة مدى الحماية التي تقدمها واقعياً، بعيداً عن وجهة النظر النظرية، ووجهة نظر منشئ هذه الخدمات.

مشكلة البحث

نتيجة للتطور التكنولوجي، وإدخال النظم الحاسوبية لكافة المؤسسات التابعة للدول، ومنها المؤسسة التربوية – بديهياً –، وفي مقابل هذا التطور والانتشار، تطورت كذلك الأخطار على هذه النظم، سواءً كانت أخطار أمنية على خصوصية بيانات المستخدمين، أو أخطار فيروسية على الحواسيب المزودة بها المؤسسة التربوية، وكنتيجة لذلك أرتأت الباحثة أن تخطو خطوة لدراسة مدى نجاعة أساليب الحماية الموجودة حالياً، ومن أهم هذه الأساليب المواقع السحابية، وبوابات المستخدم القائمة على بلوكشين (BlockChain)، وذلك بغرض الإجابة على التساؤلات التالية :-

1- هل تحقق هذه الأساليب الحديثة الحماية اللازمة للمؤسسات ؟

2- هل تتطلب هذه الأساليب مزيداً من التطوير؟

3- هل هذه الأساليب غير ناجحة من الأساس ويجب البحث عن بدائل؟

أهمية البحث :-

تتوقع الباحثة أن يسهم بحثها – في المجال التربوي – في التأكد من مدى خصوصية بيانات العاملين بالمؤسسات التربوية المعتمدة على أساليب الحماية المعروفة حالياً، ومدى الحماية من الأخطار الفيروسية التي تعمل على إتلاف البيانات والملفات الهامة – في بعض الأحيان – .

أهداف البحث :-

تهدف الباحثة من خلال هذه الدراسة إلى تحقيق الأهداف التالية :-

1- التأكد من خصوصية بيانات العاملين بالمؤسسات التربوية.

2- بيان مدى نجاح أساليب الحماية المعروفة في الوقت الحاضر في حماية البيانات من التلف والتلصص.

3- وكنتيجة لذلك يتم الاستمرار في الاعتماد على تكنولوجيا الحماية الحالية، أو البحث عن بدائل لها.

فروض الدراسة :-

1- عدم وجود علاقة بين المواقع السحابية، وحماية البيانات من التلف أو التلصص.

2- وجود علاقة طردية بين استخدام بوابات المستخدم القائمة على بلوكشين وحماية بيانات المستخدمين.

حدود البحث :-

الحدود الموضوعية للبحث :-

تنحصر الحدود الموضوعية للبحث في بيان مفهوم الحماية من الفيروسات، وخصوصية بيانات المستخدمين، وبوابات البلوكشين، بالإضافة إلى المواقع السحابية، ومدى تحقيق هذه الأساليب للأهداف المطلوبة منها، وهي حماية البيانات من التلف والتلصص.

الحدود الزمانية للبحث :-

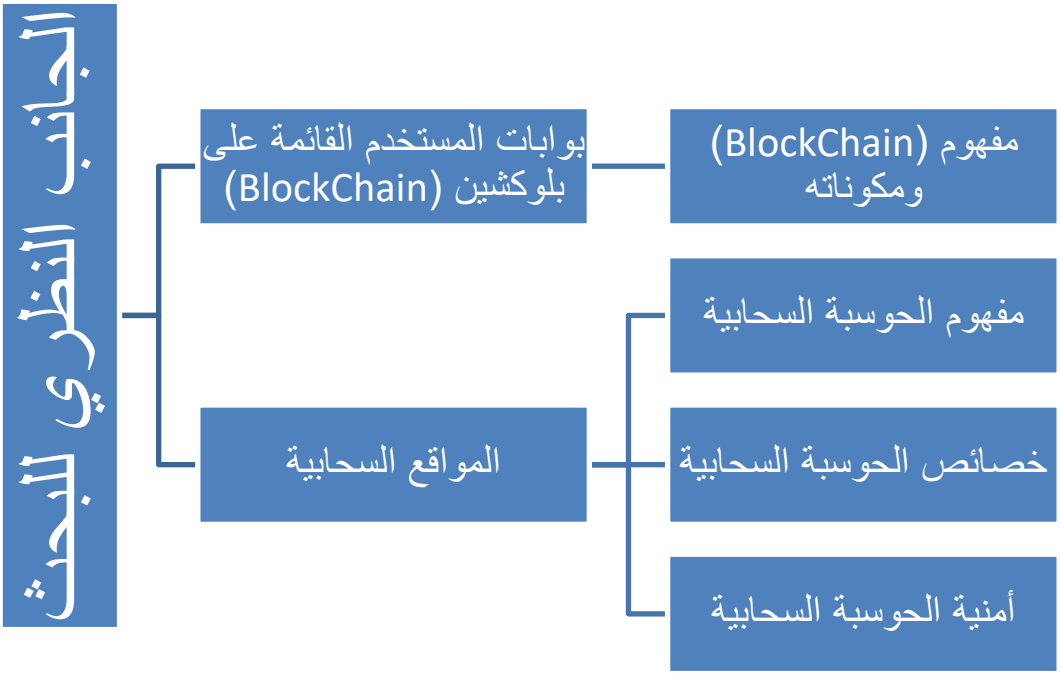
تنحصر حدود البحث زمانياً في الفترة التي أجريت فيها الدراسة، وهي النصف الأول من عام 2020م/1441هـ.

منهج الدراسة وأدواتها :-

أولاً- منهج البحث :-

1- الجانب النظري :-

تسير الباحثة للوصول إلى الأهداف النهائية للبحث وفقاً للمخطط التالي :-



2- الجانب العملي للدراسة :-

اعتمدت الباحثة في الجانب العملي على طريقة تحميل عدد 50 ملفاً من 6 مواقع سحابية مختلفة، ثم العمل على فحصها باستخدام برامج الفحص الفيروسي المدفوعة (Avira & AVG)، وكانت نتيجة الفحص أن عدد 46 ملفاً كانوا خاليين تماماً من الفيروسات، بينما كانت 4 ملفات مصابة وتعرض الحاسب للخطر.

مصطلحات الدراسة :-

1- الحوسبة السحابية :-

مصطلح يشير الي المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد» من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تُبَسِّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية(كلو, 2015).

2- بوابات بلوكشين :-

هي أكبر سجل رقمي موزع ومفتوح يسمح بنقل أصل الملكية من طرف إلى آخر في الوقت نفسه، دون الحاجة إلى وسيط، مع تحقيق درجة عالية من الأمان لعملية التحويل في مواجهة محاولات الغش أو التلاعب، ويشترك في هذا السجل جميع الأفراد حول العالم، ويمكن اعتبار البلوكشين حالياً أكبر قاعدة بيانات موزعة عالمياً بين الأفراد(خليفة, 2018).

أولاً- المواقع السحابية :-

مفهوم الحوسبة السحابية

اختلفت التعريفات حول مفهوم الحوسبة السحابية، نذكر منها ما يلي :-

1- التزايد في استخدام وتوفير وإيصال الخدمات المعتمدة على الانترنت، كخدمات عبر شبكة الانترنت، ويتم تقديم هذه الخدمات عبر مراكز، ويطلق على برمجيات وأجهزة المراكز، مصطلح السحابة للدلالة على ضخامة الموارد(Shahbaz, 2013; Armbrust).

2- نموذج لتمكين الوصول الملائم للشبكة حسب الطلب، لمشاركة الموارد الحاسوبية " الشبكات – الخدمات – البرمجيات – نظم التخزين "، والتي يمكن الحصول عليها بأقل مجهود إداري(Garrison, 2010).

خصائص الحوسبة السحابية :-

وضع المعهد الوطني للمعايير والتكنولوجيا (NISNT) مجموعة من الخصائص المميزة للحوسبة السحابية، تذكرها الباحثة فيما يلي :-

1- توفير خدمات ذاتية حسب الطلب، حيث يمكن للمستفيد الحصول على الخدمات التي يحتاجها كالتخزين السحابي، وغيرها دون التواصل الشخصي مع موفر الخدمة.

2- توفر مجموعة متنوعة من الموارد الحاسوبية سواء المادية أو الافتراضية دون علم المستفيد بمكان وجودها الفعلي.

3- قياس الخدمة المقدمة، حيث يقوم موفر الخدمة بقياس معدلات استخدام الخدمة، وإعداد تقارير عنها وحساب التكلفة المستحقة على المستفيد.

4- إتاحة الوصول لجميع الموارد والخدمات عبر الإنترنت.

5- المرونة الشديدة بالخدمة، حيث يمكن للمستفيد في أي وقت الاشتراك بخدمات إضافية أو وقف الاشتراك بمرونة وسهولة شديدة.

6- تعتمد على مدى واسع من الخدمات الرخيصة وبفعالية عالية.

7- ذات طابع تجاري يدعم بشكل كبير انتشار خدماتها، ودعم استخدام مواردها.

8- تقدم خدمات متمثلة في: البنية التحتية، ومنصات العمل والبرمجيات.

أمنية الحوسبة السحابية :-

رصد تقرير منظمة أمنية السحب (CSA)، والذي جاء تحت عنوان (Top Threats to Cloud Computing)، والذي صدر في مارس 2010 كثير من التهديدات الأمنية في الحوسبة السحابية، وجاء هذا التقرير لمساعدة المنظمات المهتمة بالانتقال إلى خدمات الحوسبة السحابية في اتخاذ القرار مع إدراك حجم المخاطر والتهديدات التي قد تواجهها، ومن التهديدات التي رصدها هذا التقرير :-

1- اساءة الاستعمال والأعمال الخبيثة :-

إن اجراءات التسجيل البسيطة والسهلة نسبياً للوصول إلى خدمات السحابة سهلت على مرسلي الرسائل غير المرغوب فيها، والمتطفلين، وغيرهم من المتسللين الاستفادة منها لشن هجمات مختلفة، وأمثلة على هذه الهجمات، الهجوم على كلمة المرور الرئيسية (Password)، تسكين البيانات الخبيثة (Key Cracking)، إخفاء الخدمة عن المستفيدين (DDOS)، شن هجوم ديناميكي، بناء جداول قوس قزح (Rainbow Tables) والتي تستخدم لاستعادة أرقام المرور، التحكم عن بعد بالقيادة أو المراقبة (Botnet)، حل مشاكل ال (CAPTCHA) التي تكشف هوية المهاجم إذا كان نوع من أنواع البرمجيات الخبيثة، ويستهدف هذا التهديد مستوى البنية التحتية كخدمة (PaaS)، والمنصة الحاسوبية كخدمة (IaaS).

2- واجهات التطبيقات غير آمنة :-

تعتبر واجهات التطبيقات التي يتفاعلوا المستخدمين مع الخدمات من خلالها ثغرة، يمكن من خلالها توقع الهجوم، وعلى موفر الخدمة ضمان أمنية هذه الواجهات وبنفس الوقت على المستفيد التنبه للمخاطر الأمنية عن الاستخدام من خلال إدارة ومراقبة الخدمة. أمثلة على تلك التهديدات تبعية ال (API)، محدودية الرصد أو إمكانيات التسجيل، عدم مرونة التحكم بالوصول، وصول مجهول، يمكن إعادة استخدام المميزة أو كلمات مرور، مصادقة النصوص و/أو نقل المحتويات من التصاريح، ويستهدف هذا التهديد مستوى البنية التحتية كخدمة (IaaS)، والبرمجيات كخدمة (SaaS)، والمنصة الحاسوبية كخدمة (PaaS).

3- الخبيث الداخلي :-

الخبيث الداخلي يشكل خطراً كبيراً في بيئة الحوسبة السحابية؛ حيث يستغل المهاجمين أن المستخدمين لا يملكون رؤية واضحة حول سياسات وإجراءات موفر الخدمة، وعليها تعتبر هذه ثغرة للاستهداف والهجوم، على سبيل المثال دخول الموظفين والمستخدمين للخدمة والمراقبة والامتثال لمعايير الممارسات عادة لا تكون شفافة للمستفيدين (تحجب عليهم بهدف تسهيل العمل)، فيتمكن المهاجم من استغلال هذا والحصول على الدخول غير المصرح به إلى داخل المنظمات والممتلكات، بعض هذه التهديدات قد تشمل الإضرار تماماً بالجانب المالي، وتسبب فقدان الإنتاجية، ويستهدف هذا التهديد مستوى البنية التحتية كخدمة (IaaS)، والمنصة الحاسوبية كخدمة (PaaS)، والبرمجيات كخدمة (SaaS).

4- قضايا التكنولوجيا المشتركة :-

يقوم مستوى البنية التحتية كخدمة (IaaS) في الحوسبة السحابية على مفهوم التشاركية بالبنية الأساسية (مثل أقسام الفرص، وحدة المعالجة المركزية، وحدات معالجة الرسومات (GPU))، ولكن غالباً ما تكون هذه الموارد غير مصممة لاستيعاب بنية متعددة المستأجر (Multi-

Tenant)، ومثل هذا العيب سمح لأنظمة التشغيل المستضافة الحصول على مستويات غير مرخص بها من تحكم وتأثير على المنصة (Platform)، ويستهدف هذا التهديد مستوى البنية التحتية (IaaS).

5- فقدان أو تسرب البيانات :-

من التهديدات التي تتعرض لها الحوسبة السحابية أيضاً احتمالات حذف البيانات أو تعديلها بدون عمل نسخة احتياطية، وفك ربط السجل من السياق الأوسع، وفقدان مفتاح الترميز والوصول غير المصرح به للبيانات الحساسة والحرجة، واحتمالية زيادة حجم البيانات في الحوسبة السحابية بسبب البنية، ويستهدف هذا التهديد مستوى البنية التحتية كخدمة (IaaS)، والبرمجيات كخدمة (SaaS)، والمنصة الحاسوبية كخدمة (PaaS).

6- الاستيلاء على الحساب أو الخدمة :-

عادة ما يتم استغلال الثغرات الأمنية بالبرامج لسرقة وثائق التفويض من خلال هجمات تعتمد على الخداع والغش، ويستهدف هذا التهديد مستوى البنية التحتية كخدمة (IaaS)، والبرمجيات كخدمة (PaaS)، والمنصة الحاسوبية كخدمة (SaaS).

7- المخاطر غير المعروفة :-

خدمات الحوسبة السحابية تعني أن المنظمات المستفيدة أقل ملكية للأجهزة والبرامج وعمليات الصيانة، وعلى الرغم من أن هذا يوفر مزايا هامة من حيث الكلفة، إلا أنه ينبغي للمنظمات أن تكون على علم بقضايا كثيرة مثل إجراءات الأمن الداخلي، والاتفاقيات الأمنية، والولوج للسحابة، وغيرها، قد تتعرض لهجمات مختلفة تستهدف مستوى البنية التحتية كخدمة (IaaS)، والبرمجيات كخدمة (SaaS)، والمنصة الحاسوبية كخدمة (PaaS).

ورصد ذات التقرير التهديدات في الحوسبة السحابية على النحو التالي : فقدان قوة الحكم أو التحكم، ضبابية المسؤولية، والمصادقة والترخيص، وفشل العزل، والمخاطر القانونية، ومعالجة الحوادث الأمنية، وإدارة ضعف الواجهات، وحماية التطبيق، وحماية البيانات، والخبيث الداخلي، وفشل العمل من مقدم الخدمة، وعدم توفر الخدمات، والتقيد بالمورد، وفقدان أمنية واكتمال البيانات، والرؤية والمراجعة.

ثانياً- بوابات المستخدم القائمة على بلوكشين (BlockChain):-

إن إنترنت الأشياء عبارة عن شبكة من الكائنات المادية المضمنة مع الإلكترونيات والبرامج وأجهزة الاستشعار التي تمكن هذه الكائنات من جمع البيانات ومشاركتها ، كما يتيح إنترنت الأشياء الاستشعار عن بُعد والتحكم فيه عبر البنية التحتية للشبكة ، وتطبيقات إنترنت الأشياء قادرة على التفاعل مع بعضها البعض والبيئة دون أي تدخل بشري ، مما يحسن كفاءة ودقة العمل عبر القطاعات(Gokhale, Bhat, & Bhat, 2018).

ينصب التركيز على إنترنت الأشياء في تكوين الأجهزة أو "الأشياء" التي لا ترتبط تقليديًا بالإنترنت أو التحكم فيها أو ربطها بالإنترنت (TECNICO LISBOA, 2018).

لتعزيز ثقة المستخدم في إنترنت الأشياء ، يجب أن تكون آمنة لضمان سرية بياناتها والحفاظ على خصوصيتها ، وتحقيقًا لهذه الغاية ، تم إنشاء العديد من الأطر لضمان خصوصية بيانات المستخدم ، مما يعزز ثقته في استخدام إنترنت الأشياء ، وأهم هذه الأطر ، والتي تم تناولها في هذه الدراسة ، هو نظام (BlockChain).

يقوم BlockChain بتخزين جميع البيانات التي تم إدخالها في النظام ، بحيث لا يمكن مسحه لاحقًا بأي طريقة ، المثال الأكثر شيوعًا لاستخدام BlockChain للحماية هو BitCoin ، هذا النظام يفتح الباب لتحويل الاقتصاد من نظام مركزي إلى مفتوح (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, n.d.).

*** مفهوم (BlockChain) ومكوناته :-**

إنه إطار آمن يستخدم لتشفير العملات الإلكترونية(Zhang et al., 2019)، وفي(Groopman & Owyang, 2018) يقترحون استخدام Blockchain لتمثيل حقوق الوصول إلى الموارد ونقلها من مستخدم إلى آخر ، عن طريق تحديد الشرط الذي يحدد الشخص الذي مُنحت السياسة حق الوصول إليه ، وكذلك الشروط التي تحدد القيم المسموح بها للسمات: الموضوع والموارد والبيئة الممنوحة للوصول.

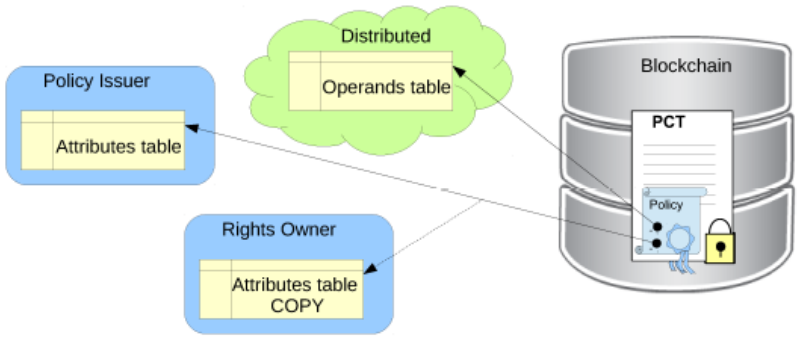


Fig.7 (Zhang et al., 2019)

1- FairAccess :-

تم استخدام Fairaccess كوسيلة جديدة لمنح حق الوصول والحصول عليه والإذن به وإبطاله استنادًا إلى (Ouaddah, Elkalam, & Ouahman, 2018) ، ويؤكد البعض(Zhang et al., 2019) أن له عددًا من العيوب مثل: دعم التراخيص المستندة إلى الرمز فقط والحاجة إلى الاتصال بمالك المورد لكل وصول جديد أو انتهاء صلاحية الرمز المميز.

2- ControlChain :-

ControlChain هو نظام مرن لامركزي يسمح بالعمل دون اتصال، وله ملف تعريف، ويستخدم معالجًا منخفضًا في عملية الترخيص (Julio & Pinno, 2017) (Adhav, Bhosale, Javanjal, & Kadam, 2018).

*** الطريقة والإجراءات :-**

لمعرفة مدى الأمان الذي تتمتع به بيانات المستخدم والحاسب، عند استخدامه للمواقع السحابية، وبوابات المستخدم القائمة على بلوكشين، تم الاعتماد على طريقة تحميل عدد 50 ملفاً من 6 مواقع سحابية مختلفة، ثم العمل على فحصها باستخدام برامج الفحص الفيروسي المدفوعة (Avira & AVG)، وكانت نتيجة الفحص أن عدد 46 ملفاً كانوا خاليين تماماً من الفيروسات، بينما كانت 4 ملفات مصابة وتعرض الحاسب للخطر.

كما وجد أن المواقع السحابية لا تقدم أي ضمان لخلو الملفات من الفيروسات، فيقتصر دور رافع الملف على رفعه، ودور المحمل على تحميله، دون أي ضمان لخلوه أو عدم خلوه من الفيروسات.

النتائج :-

خلصت الباحثة مما سبق إلى النتائج التالية :-

1- بوابات المستخدم تقدم حماية جيدة للحاسب من الأخطار سواء الفيروسية أو غيرها.

2- لا تقدم المواقع السحابية الحماية المتوقعة، حيث انتهت التجربة العملية إلى وجود ملفات تحتوي على الفيروسات موجودة ضمن المواقع السحابية.

3- بمجرد ضغط الملف بإحدى البرامج المعدة لذلك مثل (Winrar, zip)، يكون من الصعب على البرامج الفاحصة لأمن الملفات معرفة مدى خلو الملف من الأخطار الفيروسية من عدمه.

4- المؤسسات الحكومية وغير الحكومية بالمملكة العربية السعودية لا تعتمد حوسبة سحابية خاصة ومستقلة عن المواقع الموجودة على الشبكة مما يعرض بياناتها، وأمان الحواسب المستخدمة لها لكثير من الأخطار.

التوصيات :-

1- ضرورة اعتماد المؤسسات خصوصاً الحكومية منها على حوسبة سحابية خاصة ومستقلة.

2- لا يجب الاعتماد على الحوسبة السحابية، والاعتقاد بأن الملفات المحملة إليها خالية من الأخطار الأمنية على الحاسب.

3- حرص المستخدم عند تحميل الملفات المضغوطة.

قائمة المراجع :-

Adhav, V., Bhosale, S., Javanjal, P., & Kadam, N. (2018). A Review on – ControlChain : Access Control using BlockChain, 859–861.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (n.d.). *BlockChain Technology .. Beyond Bitcoin*.

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT, (January 2019), 0–4. https://doi.org/10.17148/IARJSET.2018.517

Groopman, J., & Owyang, J. (2018). *The Internet of Trusted Things Table of Contents .. BlockChain as the Foundation for Autonomous Products & Ecosystem Services*.

Julio, O., & Pinno, A. (2017). ControlChain : Blockchain as a Central Enabler for Access Control Authorizations in the IoT, (December). https://doi.org/10.1109/GLOCOM.2017.8254521

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2018). FairAccess : a new Blockchain-based access control framework for the Internet of Things, (February 2017). https://doi.org/10.1002/sec.1748

TECNICO LISBOA. (2018). *Internet of Things: An Introduction*.

Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., & Tao, F. (2019). Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System. *IEEE Transactions on Computational Social Systems*, *PP*(August), 1–9.

https://doi.org/10.1109/TCSS.2019.2918467

خليفة, إ. (2018). البلوك تشين: الثورة التكنولوجية القادمة في عالم المال والإدارة. *المستقبل للأبحاث والدراسات المتقدمة*, (3), 1–7.

كلو, ص. م. (2015). الحوسبة السحابية: مفهومها وتطبيقاتها في مجال المكتبات ومراكز المعلومات . In *The SLA-AGC 21st Annual Conference* (pp. 1–11). Abu Dhabi: قسم دراسات المعلومات–جامعة السلطان قابوس .

https://doi.org/http://dx.doi.org/10.5339/qproc.2015.gsla.8

Abstract

This study aimed to know the extent of protection provided by cloud sites and blockchain-based user portals to the computer from dangers, and for this reason the researcher relied on downloading 50 files from 6 cloud sites, then working on examining the extent of their security using the protection programs (Avira & AVG), The results concluded that the user portals do not provide this protection effectively, while cloud computing does not provide it effectively, and the researcher saw the need for institutions to have a special cloud computing independent of the general cloud computing that individuals use.

Keywords: User Portals, Blockchain, Cloud Computing