The Contents of Electronic Archive Files and their Protection Measures: A Critical Review Study

Afraa Ali Al-Marri

Faculty of Arts and Humanities, King Abdulaziz University

Jeddah, Saudi Arabia

Abstract: In view of the large and increasing risks to information security, privacy and copyright, it was necessary to find and develop technical and legislative solutions that guarantee the security of documents and digital files, whether circulated, published or archived. In the past few years, several solutions have been developed to provide the maximum possible level of protection for data, files and digital repositories. Each of these solutions had qualitative, competitive and specialized advantages, but on the other hand some of them had some drawbacks, whether in terms of efficiency or the possibility of wide application or their impact on the quality and effectiveness of scientific participation, publishing transparency and property rights. We are well aware of the impact of fear of the dangers of privacy, theft, plagiarism, quotation and disruptive piracy on the level of scientific participation and the scientific research movement in general. This leads researchers around the world to try to develop solutions that combine cybersecurity with the effectiveness of publishing and sharing.

This research paper aims to study and analyze some of the currently used methods in the protection and security of digital files and documents, discuss the feasibility, effectiveness and flexibility of each of them, and come up with the best methods, tools and practices that guarantee the security of digital files. And this is through the critical scientific method of some studies that have dealt with these methods, especially recent studies, because progress in this field is very fast. Hardly a few months pass without us finding new systems and tools that have been developed in the field of information security and have canceled or modified what preceded them. We have reached some important results, which we will detail at the end of this paper, but it is worth noting here the most important of these results. Such as the seriousness of the threats facing stored and circulating documents, to the national security of each country, to the scientific research movement, as well as to the confidentiality and privacy of data. Several aspects as well as comprehensive solutions for securing digital documents.

محتويات ملفات الارشفه الالكترونيه وتدابير حمايتها: مراجعة نقدية

عفراء علي المري

كلية الاداب و العلوم الانسانيه– جامعة الملك عبد العزيز

جده– المملكة العربية السعوديه

المستخلص

نظرا للمخاطر الكبيرة والمتزايدة على أمن المعلومات والخصوصية وحقوق النشر، كان لابد من إيجاد وتطوير حلول تقنية وتشريعية تضمن أمن المستندات والملفات الرقمية، سواء المتداولة والمنشورة أو المؤرشفة. وفي السنوات القليلة الماضية تم تطوير العديد من الحلول لتوفير أقصى مستوى ممكن من الحماية للبيانات والملفات والمستودعات الرقمية. وكان لكل من تلك الحلول مميزات نوعية وتنافسية وتخصصية، ولكن على الجانب الآخر كان لبعضها بعض السلبيات سواء من ناحية الكفاءة أو إمكانية التطبيق واسع المجال أو تأثيرها على جودة وفاعلية المشاركة العلمية وشفافية النشر وحقوق الملكية.
ولا يخفى علينا تأثير الخوف من مخاطر الخصوصية والسرقة والانتحال والاقتباس والقرصنة التخريبية، على مستوى المشاركة العلمية وحركة البحث العلمي بشكل عام. مما يدفع الباحثين في جميع أنحاء العالم إلى محاولة تطوير حلول تجمع بين الأمن السيبراني وبين فاعلية حركة النشر والمشاركة.
وتهدف هذه الورقة البحثية إلى دراسة وتحليل بعض الأساليب المتبعة حاليا في حماية وأمن الملفات والمستندات الرقمية، ومناقشة جدوى وفاعلية ومرونة كل منها، والخروج بأفضل الطرق والأدوات والممارسات التي تضمن أمن الملفات الرقمية. وذلك من خلال المنهج العلمي النقدي لبعض الدراسات التي تناولت هذه الأساليب، وخاصة الدراسات الحديثة منها، وذلك لأن التقدم في هذا المجال سريع جدا. ولا يكاد تمر شهور قليلة إلا ونجد أنظمة وأدوات جديدة تم تطويرها في مجال أمن المعلومات، وقامت بإلغاء أو تعديل ما قبلها.وقد توصلنا إلى بعض النتائج الهامة، والتي سوف نفصلها في نهاية هذه الورقة، ولكن تجدر الإشارة هنا إلى أهم تلك النتائج. مثل خطورة التهديدات التي تواجه المستندات المخزنة والمتداولة، على الأمن الوطني لكل دولة، وعلى حركة البحث العلمي، وكذلك على سرية وخصوصية البيانات.ومما لاحظناه في معظم الدراسات التي مرت علينا، هو تركيز كل دراسة على جانب معين من جوانب الحماية، وقلما نجد حلا يشمل عدة جوانب فضلا عن حلولا شاملة لتأمين المستندات الرقمية.

الكلمات المفتاحية

الأرشفة الإلكترونية – المستودعات الرقمية – التخزين السحابي – الملفات الرقمية – أمن الملفات – أمن المعلومات والخصوصية – حماية الملفات الرقمية – الأمن السيبراني – التشفير – العلامة المائية – التوقيع الرقمي – هجمات الاختراق – التحكم في الوصول – البرمجيات الخبيثة – تزوير البيانات.

المقدمة

في العصر الحالي، يحتل أمن المعلومات أولوية قصوى لجميع المنظمات والهيئات. فنادرًا ما يمر أسبوع دون أن نسمع عن اختراق جديد للبيانات أو محاولة اختراق من مجموعات مختلفة حول العالم. فمع التطور السريع لتقنيات الإنترنت مثل إنترنت الأشياء والبيانات الضخمة والأرشفة الإلكترونية والحوسبة السحابية يواجه الأفراد والمسؤولون مشاكل كبيرة للحفاظ على أمان البيانات. وعلى الجانب الآخر، نظرًا للمعدل الهائل لنمو البيانات، فإنها مهمة صعبة بالنسبة للباحثين، تتمثل في كيفية إدارة الكمية الهائلة من البيانات بأمان وفعالية.

سنقوم في هذه الدراسة بمراجعة بعض الدراسات السابقة التي تقدم حلا تقنيا يستخدم إحدى طرق حماية الملفات الرقمية. ونفحص مدى نجاعة هذه الحلول ومرونتها، وما إذا كانت قابلة للتطبيق على نطاق شامل.

ولفهم تلك الدراسات والأساس الذي قامت عليه، لابد من معرفة واقع الأرشفة الإلكترونية والطرق المتبعة في ذلك حاليا والتقنيات الأكثر انتشارا في هذا المجال.

وفي جانب الأرشفة الإلكترونية، يعد تأمين المستندات أحد أهم جوانب الأمان في كل عمل أكاديمي أو حكومي أو تجاري. ولسوء الحظ، يمكن أن يكون بناء سياسة أمان المستندات عملية معقدة وتستغرق وقتًا طويلاً.

ومن المهم معرفة دورة حياة المستند، حتى يتسنى لنا فهم مدى وأهمية كل مرحلة منها عند إنشاء المستندات ومعالجتها لضمان إدارتها بفعالية: وهذه المراحل هي:

الإنشاء – التصنيف – المشاركة والحماية – الحفظ – الأرشفة وضمان الوصول – الإتلاف [9]

شكل رقم (1): دورة حياة المستند

مصدر الصورة (www.inforouter.com)

وجدير بالذكر أن تصنيف المستندات من حيث درجة سريتها وخصوصيتها من الأمور الهامة للغاية عند تخزين الملفات وتحديد صلاحيات الوصول إليها. فالتصنيف الصحيح والفعال يوفر الكثير من الجهد والوقت، بل وتكلفة التخزين والإدارة. لذلك تعطي بعض الجامعات، مثل جامعة بريستول أهمية بالغة لتصنيف ملفاتها، وتصدر تحديثا دوريا لهذا التصنيف، كما بالشكل التالي [9]:

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Open	Available to all authenticated members of University staff
Confidential	Available only to authorised and authenticated members of staff
Confidential & Sensitive	Access is controlled and restricted to a small number of named, authenticated members of staff
Secret	Known only to a very small number of authenticated members of staff

شكل رقم (2): تصنيف المستندات من حيث درجة سريتها وخصوصيتها في جامعة بريستول [9]

ومن أشهر طرق تخزين وحفظ وإدارة الملفات الرقمية هي المستودعات الرقمية. وهي أنظمة تكنولوجيا المعلومات التي تقدم أدوات لتخزين ونشر البيانات والمعلومات واسترجاعها ومشاركتها من خلال جمع سجلات البيانات جنبًا إلى جنب مع البيانات الوصفية ذات الصلة [1]. وتظهر للمستخدمين على شكل مواقع ويب. وهي عدة أنواع، منها العامة (المؤسسية) ومنها المتخصصة ومنها التجارية. وتتسابق المؤسسات العلمية والجامعات على إنشاء مستودعات رقمية. ويتم تصنيف المستودعات على أعداد ما تحتويه من مصادر رقمية من كتب ومجلات وأبحاث وأطروحات علمية ودراسات ومقالات[8].

ومن طرق تخزين المستندات الرقمية هو التخزين السحابي. ففي مواجهة عبء تخزين البيانات بالأسلوب التقليدي، اختار عدد متزايد من الأفراد والمؤسسات تخزين بياناتهم في السحابة، مما أدى إلى التطور السريع للتخزين السحابي والحوسبة السحابية. على الجانب الإيجابي، يمكن للتخزين السحابي توفير المساحة المحلية ، وتحرير الكثير من قوة الحوسبة المحلية، وعلى الجانب السلبي، قد تواجه البيانات التي يتم رفعها إلى السحابة العديد من المخاطر، بما في ذلك على سبيل المثال لا الحصر فقدان البيانات وتسرب الخصوصية وهجمات الأمان، بالإضافة إلى خطر الفيروسات الضارة.

ومن عيوب التخزين السحابي، أنه لا يتم التحكم في البيانات الخارجية من قبل المستخدم. ولتوفير مساحة التخزين ، قد تقوم السحابة بإزالة البيانات النادرة الاستخدام أو المتكررة بشكل كبير ، مما يضعف سلامة بيانات المستخدم في السحابة. ويصبح من المستحيل بالنسبة لمعظم المستخدمين، الذين لا يتمتعون بقدرة تدقيق جيدة، معرفة ما إذا كانت بياناتهم في السحابة لا تزال كاملة. ولحل هذه المشكلة، يمكن للمستخدم أن يكلف طرفًا ثالثًا بمراجعة سلامة بياناته عن طريق التحقق من دقة البيانات وصلاحيتها واتساقها وتحديد الإدخالات غير الكاملة أو المفقودة في تخزين البيانات. يعتبر تدقيق النزاهة مهمًا بشكل خاص لمستخدمي مجموعة التخزين السحابي مع خدمات المشاركة، حيث إن أي مستخدم يسيء

التصرف في المجموعة قد يعرض أمن البيانات لأعضاء المجموعة الآخرين للخطر. وفي النهاية، يمكن للمستخدمين في نفس المجموعة مشاركة البيانات مع بعضهم البعض، والوصول إلى البيانات المشتركة وتعديلها [2].

ومن الطرق الرئيسية لحماية تأليف المستندات الإلكترونية هي استخدام التوقيع الرقمي (Digital Signature). وهو بديل للتوقيع بخط اليد ويستخدم عند تنظيم تدفق إلكتروني آمن للمستند. يسمح التوقيع الرقمي بتأكيد حقيقة تغيير المستند الإلكتروني بعد توقيعه.

ومن طرق الحماية أيضا، التشفير وهو فرع من الرياضيات التطبيقية يهتم بتطوير خوارزميات معقدة لتخليط المعلومات (نص عادي) في نسخة غير قابلة للفك تشفير من تلك المعلومات (نص مشفر) والعودة إلى نص عادي [10].

وإلى جانب استخدام طرق التشفير لحماية البيانات، ومن الطرق الفعالة تضمين بيانات إضافية في أغلفة رقمية، خاصة في محتوى الوسائط المتعددة. هناك اتجاهان لإخفاء البيانات في الكائنات الرقمية: إخفاء المعلومات والعلامة المائية.يهدف علم إخفاء المعلومات إلى حماية سرية المعلومات. ويتم تضمين البيانات المحمية في شكل غلاف وتصبح غير مرئية لأطراف ثالثة.

العلامات المائية الرقمية مصممة لحماية حق تأليف أو سلامة كائن الغلاف نفسه. ويسمح الغلاف باستخراج المعلومات المضمنة بالتأكيد. للقيام بذلك ، عادة ما تتم مقارنة العلامة المائية المستخرجة بالعلامة الأصلية. حيث يجب أن تتطابق العلامة المائية المستخرجة والعلامة المائية الأصلية مع بعضهما البعض. يعتمد ذلك على حالة الاستخدام المحددة للعلامات المائية الرقمية. العلامة المائية هي بديل للتوقيع الرقمي. وفي بعض الأحيان، يتم استخدام هاتين التقنيتين معًا.

المنهجية

في هذه الدراسة سوف نستخدم المنهج الاستطلاعي النقدي، حيث نسرد باختصار، بعض الأعمال التي تناولت موضوع حماية الملفات الإلكترونية خلال تخزينها وتداولها، والتي قدمت حلولا عملية لها، ونناقشها ونحاول تحديد مدى جدوى وفاعلية الحلول المقدمة. كما نستخلص بعض الاستنتاجات من هذه الدراسات التي تفيدنا في اقتراح حلول أخرى، أو الخروج بأفكار استرشادية وأسس قد نبني عليها استرتيجيات ناجحة للتعامل مع الملفات الإلكترونية.

ولتحقيق ذلك، تم اختيار الدراسات المتخصصة في مجال الأرشفة الإلكترونية وتحديدا حماية الملفات والمستندات الرقمية من عدة جوانب. مثل حماية الشبكة، وحماية المستودعات الرقمية، وحماية المخازن السحابية، وصد أنشطة القرصنة الهجومية والتخريبية.

النتائج والمناقشة

بعد الاطلاع على العديد من المراجع والدراسات في مجال البحث (محتويات الملفات وتدابير حمايتها)، اتضح أن الموضوع متشعب جدا، ويشمل طرق حماية وتأمين الملفات الرقمية من جوانب عديدة. فبمجرد أن تتواجد الملفات على شبكة

الإنترنت (سواء داخل الأجهزة الخاصة بالفرد أو المؤسسة أو داخل مستودع رقمي أو في مخزن سحابي)، أصبحت عرضة لأنواع عديدة من التهديدات.

لذلك تم اختيار سبع دراسات، يقدم كل منها حلا تقنيا يغطي جانبا محددا من جوانب تلك التهديدات. وتم ترتيب الدراسات في تسلسل زمني من الأحدث إلى الأقدم على النحو التالي:

دراسة (2021) Chen, et al بعنوان:

"A threshold hybrid encryption method for integrity audit without trusted center"

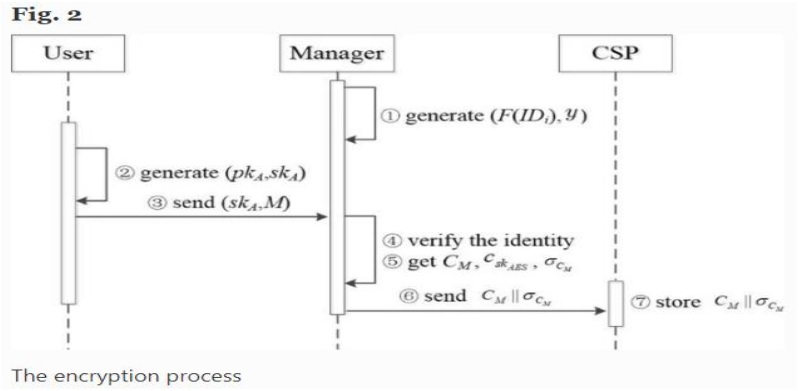
تقترح هذه الورقة طريقة تشفير جديدة (تشفير هجين) لطريقة تدقيق السلامة في أنظمة التخزين السحابي، دون الاعتماد على مركز موثوق. وذلك للتحقق من سلامة البيانات والحفاظ على البيانات والخصوصية الرئيسية. وإلى جانب ذلك، يقوم الباحث بتصميم وتنفيذ طريقة جديدة لتدقيق التكامل وإعادة التوقيع والتي تتحقق من سلامة البيانات وتحل مسألة التداخل بين السحابة والمستخدمين الذين تم إبطالهم. يوضح تحليل الأمان وتقييم الأداء أن المخطط المقترح يحقق الدقة والأمان والكفاءة بتكلفة منخفضة للاتصال والحساب.

حيث يؤكد الباحث أن الدراسات السابقة المتعلقة بالتخزين السحابي ركزت على أمن البيانات وتكاملها في السحابة، وفشلت في معالجة أمن البيانات في عملية التحميل أو التنزيل ، بينما تتم سرقة البيانات بسهولة عن طريق هجمات القرصنة. كذلك لتقليل المخاطر وحماية الخصوصية ، يجب تشفير البيانات والمفتاح. لذلك ، ومن المهم تطوير نظام تشفير فعال وآمن للحفاظ على البيانات والخصوصية الرئيسية ، مما يدعم تدقيق سلامة البيانات المشتركة بين أطراف متعددة، مثل مجموعة من المدراء والموظفين.

وفكرة الطريقة الجديدة المقترحة من الباحثة، هي الجمع بين معيار التشفير المتقدم (AES) وتشفير المنحنى الإهليلجي (ECC)، وهي طريقة مناسبة لتدقيق النزاهة للحوسبة السحابية والتعلم التعاوني للتعلم الآلي. لا يسهل النهج المختلط توزيع المفاتيح وإدارتها فحسب، بل يعمل أيضًا على تحسين سرعة التشفير وكفاءة البيانات المشتركة. من خلال هذه الطريقة، يتم تشفير البيانات التي تم تحميلها لتجنب تسرب الخصوصية وهجمات الأمان، ويتم أيضا تدقيق البيانات التي تم تنزيلها للحفاظ على سلامة البيانات، وإعادة التوقيع ضد المستخدم الذي تم إلغاؤه من معرفة أي مفتاح خاص أو معلومات بيانات. بالإضافة إلى ذلك، حتى إذا فشل المدير في المشاركة في فك التشفير، يمكن للمديرين الآخرين العمل معًا لاستعادة البيانات عندما يتجاوز عدد المدراء المشاركين حدًا محددًا مسبقًا. تضمن هذه الميزة المتانة العالية للنظام. ويتم التحقق من صحة وأمن هذه الطريقة من خلال التحليل التفصيلي. علاوة على ذلك، نقوم بتقييم أداء وكفاءة هذا المخطط، وتظهر النتائج أنها خطة صحيحة وآمنة وفعالة.

تعتمد هذه الطريقة مشاركة ما يسمى (Shamir secret) بتوظيف العديد من المدراء في المجموعة لتوليد السر والاستغناء عنه بدون مركز موثوق به ، مما يسهل توزيع المفاتيح وإدارتها. بهذه الطريقة ، يتم تحويل سيناريو تعدد

المدراء إلى سيناريو متعدد الوكيل ، مما يقلل من احتمالية وجود مدراء غير نافعين ويجعل الآلية بأكملها موثوقة وآمنة.



شكل رقم (3): عملية التشفير [2]

كذلك تدعم هذه الطريقة التدقيق العام مع مدقق خارجي موثوق (TPA) وإعادة التوقيع مع بيانات المستخدمين الملغاة بواسطة السحابة بمساعدة أحد المدراء. يشير تحليل الأمان وتقييم الأداء إلى أن طريقتنا تحقق الصلاحية والأمان ، وتتحقق من فعالية التشفير ، وتقليل وقت إعادة التوقيع وتكلفة الاتصال والحساب. واستكمالا لشمول النظام الجديد، فإنه يقدم طريقة لتدقيق النزاهة، ومرحلة فك التشفير. وكل مرحلة تعتمد على طلبات كل مستخدم وكل مدير، تبعا لصلاحيات كل منهم.

من نقاط قوة هذه الدراسة أنها حققت تدقيق النزاهة والتحديث الديناميكي للبيانات بتكلفة منخفضة للتواصل والحساب.

ومن نقاط ضعف هذه الدراسة أن المخطط المقترح يتطلب مستخدمين على مستوى خاص من الخبرة في التعامل مع مثل هذه الأنظمة. أو ربما يحتاج المستخدمون إلى تدريب خاص للتعامل معه.

دراسة (2020) Ogiela, et al .بعنوان:

"Intelligent Data Management and Security in Cloud Computing"

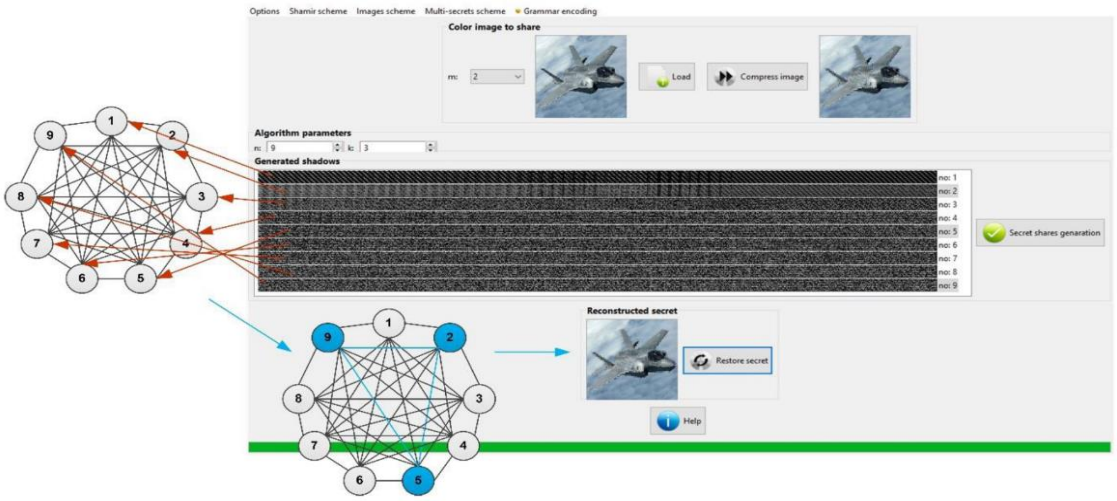
هدفت هذه الدراسة إلى تقديم حلولا لحماية وتأمين البيانات ضد الاستحواذ غير المصرح به. حيث يتم تقسيم مجال حماية البيانات لمستويات مختلفة ، ثم يتم من خلالها تنفيذ مهام إدارة البيانات وحمايتها. فالبيانات ذات الأهمية الكبيرة – الإستراتيجية أو السرية – تخضع لحماية خاصة.

وتعتمد هذه الحلول على استخدام تقنيات التشفير المستخدمة لتقسيم السر بين مجموعة محددة من الأمناء السريين ،عن طريق تطبيق الأساليب اللغوية لوصف السر المشترك، معززًا في نفس الوقت بفئة جديدة من البروتوكولات ، أي مخططات حدود الذكاء اللغوي (Intelligent Linguistic Threshold Scheme). ويتم تخصيص الحلول المقدمة في هذه الورقة لمستويات مختلفة من إدارة البيانات. يمكن التمييز بين هذه المستويات في كل من هيكل كيان معين وفي

بيئته. وخير مثال على ذلك عمليات إدارة السحابة. وستخضع هذه أيضًا لتقييم جدوى تطبيق البروتوكولات التي تمت مناقشتها في هذه المجالات.

يسمح هذا البروتوكول بتقسيم البيانات وإدارتها في وقت واحد في هياكل هرمية. عادةً ما تولد تقنيات التقسيم التقليدية أجزاء سرية لها نفس الأهمية والامتيازات. في الحلول المقترحة ، من الممكن إنشاء أجزاء سرية ذات أهمية أعلى من غيرها ، ويمكن أيضًا إنشاء صلاحيات وصول مختلفة للمستخدمين الموجودين على مستويات مختلفة في هيكل الإدارة. مثل هذا البروتوكول عالمي للغاية وفعال من الناحية الحسابية ويمكن تطبيقه على مهام إدارية مختلفة. كحل علمي ، لا يعتمد على متطلبات الأمان المحلية ويمكن تطبيقه في مجموعة واسعة من تطبيقات إدارة المعلومات الآمنة.

تتعلق التطبيقات المبتكرة للمخططات اللغوية المحددة في هذه الورقة بإمكانية استخدامها مع استخدام أنواع مختلفة من القواعد النحوية الرسمية وكذلك على مستويات مختلفة من إدارة خدمة البيانات.



شكل رقم (4): مثال على استخدام الحلول التي تمت مناقشتها [3]

في هذه المجموعة من البروتوكولات، تلعب بروتوكولات المشاركة السرية التي تثريها عملية الوصف اللغوي لمعنى البيانات المخفية دورًا مهمًا. يمكن تنفيذ عمليات وصف المعنى اللغوي للمعلومات الاستراتيجية المحمية مع مراعاة مستويات مختلفة من المعرفة الدلالية المتعلقة بالأسرار المخفية ؛ في الوقت نفسه ، تتضمن طريقة وصف المعنى اختيار بنية لغوية ونحوية مناسبة. تُظهر النتائج أن أعظم إمكانية لتطبيق هذه البرتوكولات هي في مجال الحوسبة السحابية.

سلطت هذه الدراسة الضوء على مميزات التخزين السحابي ، مثل توفير الأجهزة والخوادم والمساحة على الوسائط، بالإضافة إلى توفر الخدمة في كل مكان وكل وقت. ولكن لابد هنا من الإشارة إلى أنه مهما بلغت كفاءة أي نظام تشفير فإن الخادم السحابي غير الموثوق يهدد سلامة وأمن البيانات الخارجية. فلابد من اختيار شركة مرموقة معروفة بثقة خوادمها، وقدرتها على مقاومة الهجمات الضارة مثل هجمات إعادة التشغيل. كما أنه من الضروري للغاية تصميم مخططات أمان إضافية تسمح للمستخدمين بالتحقق من سلامة البيانات .

ومن أهم نتائج هذه الدراسة، أنها أثبتت امكانية تطبيق الإجراءات اللغوية في الهياكل الطبقية والتسلسلية في كلا النوعين من هياكل الإدارة التي يمكن تنفيذها في الأنظمة الموزعة على السحابة. كما أنها أثبتت فاعلية تطبيق نهج الرسم البياني في تقسيم البيانات السرية بطرق مختلفة لطبقات مختلفة في الهياكل الهرمية.

وعند النظر في نقاط قوة وضعف هذه التقنية، نجد أن العامل البشري في تشغيلها هو نقطة القوة ونقطة الضعف في نفس الوقت. فبالرغم من ميزة التقسيم الإداري للمهام والصلاحيات، فإن توزيع تلك الصلاحيات ومراقبتها قد يخضع لعوامل أخرى غير موضوعية.

كما أن هذه التقنية قائمة كليا على التخزين السحابي، والذي قد يكون أحيانا غير موثوق، ورغم أننا نؤيد حلول التخزين السحابي ونشجع عليه، إلا أننا نؤكد على ضرورة اختيار الشركات الكبرى الموثوقة في هذا المجال. خاصة وأنه لابد من اللجوء إلى هذه الحلول عاجلا أم آجلا.

دراسة (Kubik, and Kwiecień (2020 بعنوان:

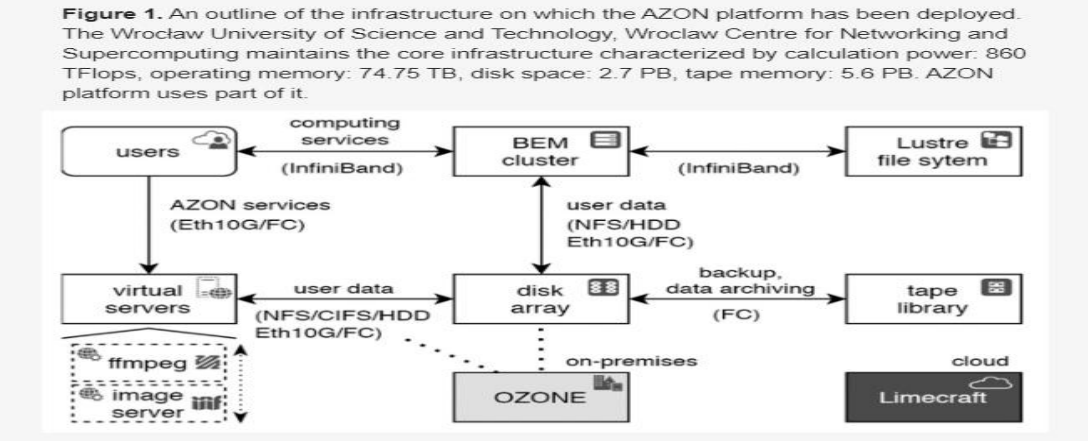
"Resolving Dilemmas Arising during Design and Implementation of Digital Repository of Heterogenic Scientific Resources"

تهدف هذه الدراسة إلى الإجابة عن الأسئلة التي قد تنشأ عند التعامل مع معضلات التصميم والتنفيذ المختلفة، مثل كيفية التعامل مع العمليات في مستودع رقمي، وكيفية استخدام الحلول السحابية في بنائه، وكيفية العمل مع واجهات المستخدم، وكيفية معالجة الوسائط المتعددة المجمعة. وتستكشف هذه الدراسة سياقها العملي بناءً على الخبرات المكتسبة أثناء تنفيذ منصة AZON. حيث تخزن هذه المنصة عشرات الآلاف من الموارد العلمية، التي تشمل الكتب والمقالات والمجلات والمواد التعليمية والعروض التقديمية والصور والمسح الضوئي ثلاثي الأبعاد وملفات الصوت والفيديو وقواعد البيانات وغيرها الكثير. وهو مثال ممتاز لتطبيق الاقتراحات المقدمة من الدراسة.

وتناقش هذه الدراسة التحديات التي تواجه إنشاء مستودعات رقمية لأرشفة ونشر المصادر العلمية. وتكشف الدراسة كيفية التغلب على تلك التحديات بشكل عملي، وذلك بما تم تطبيقه عند إنشاء مستودع رقمي ضخم، وهو مستودع AZON.

وتبين هذه الدراسة أن هذه التحديات لا تتعلق فقط بعمليات إعداد المصادر وإيداعها ومشاركتها وصيانتها وتنظيمها، ولكنها تواجه أيضًا جدوى الافتراضات المعتمدة والتنفيذ النهائي. حيث يصبح هذا النوع من القضايا مهمًا بشكل خاص في حالة معالجة الموارد التي تحتوي على وسائط متعددة. وبعد ذلك يصبح العامل الحاسم هو بنية مصممة بشكل صحيح تدعم المعالجة الفعالة للبيانات وطريقة عرضها عالميا.

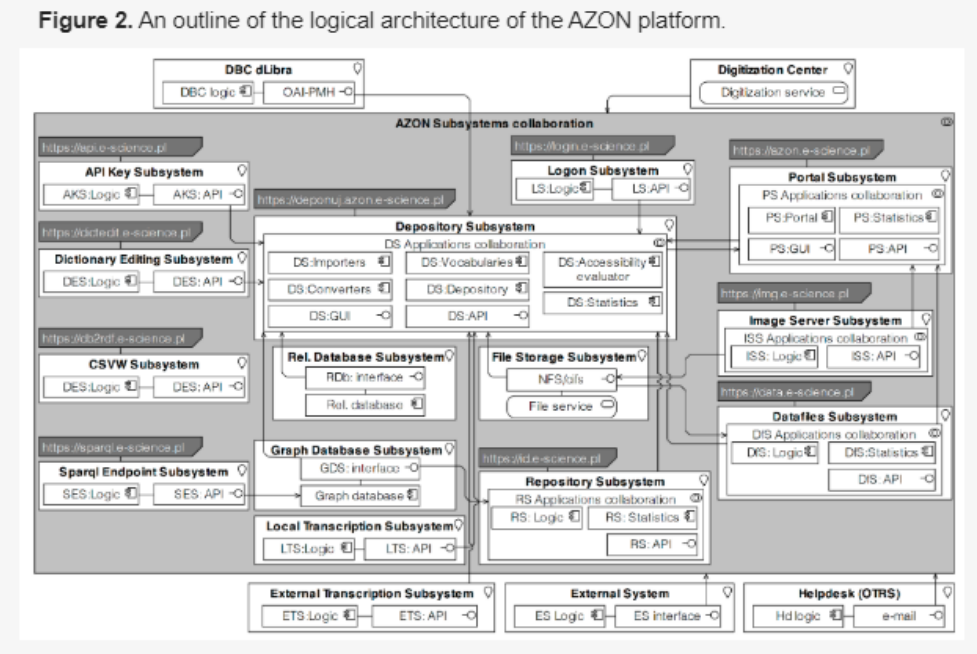
وتوضح الدراسة مخطط البنية التحتية والبنية المنطقية للمشروع، وأسباب نجاح هذه التصميمات.



شكل رقم (5): مخطط للبنية التحتية التي تم نشر منصة AZON عليها [1]

وقد قدم إنشاء منصة AZON للمؤسسات أداة وإجراءات لإتاحة الوصول إلى الوسائط المتعددة والموارد الأخرى عبر الإنترنت. توفر المنصة عدة طرق للوصول إلى سجلات البيانات واستكشافها، بما في ذلك المشاهدة عبر الإنترنت أو الاستماع أو قراءة المحتوى المشتق من شكله الأصلي. تقدم منصة AZON: الواجهة الأمامية للعرض التقديمي (حيث يمكن للمستخدمين عرض السجلات المختلفة والبحث فيها واستردادها)، الواجهة الأمامية للإدارة (حيث يمكن للمستخدمين إدارة السجلات وفقًا لامتيازاتهم ومشاركتهم في التنفيذ سير العمل)، واجهة الويب الدلالية (تتجلى من خلال الوصول المباشر إلى السجلات الدلالية، وأداة استعلام SPARQL، مع عرض محرر استعلام مدمج، ونقطة نهاية).

إذن فبفضل AZON والبيانات الوصفية والأدوات، من الممكن استكشاف المحتوى بشكل دلالي والبحث في سجلات البيانات المختلفة. تدعم البنية المصممة المعالجة الفعالة للبيانات والعرض التقديمي عبر الإنترنت وتجعل من السهل التكيف مع أدوات المعالجة والحلول البرمجية الجديدة أو المتطورة.



شكل رقم (6): مخطط للتصميم المنطقي لمنصة AMAZON [1]

تم اختيار هذه الدراسة لأنها تناقش عملية إنشاء مستودع رقمي بشكل عام، وتوضح المخطط العام للمستودع وطريقة عمله. خاصة أنها توضح ذلك بمثال واقعي لمستودع قوي وناجح. وتتمثل نقاط قوه تلك الدراسة في تسليط الضوء على العوامل التي يجب على مصممي المستودعات الرقمية مراعاتها عند تقدير الموارد المطلوبة والاستثمار في البنية التحتية. مثل: الأسعار، ونوع الترخيص للمستودع، وتراخيص الخدمات السحابية، وحجم وموثوقية المجتمع، ونموذج البيانات والبيانات الوصفية المقدم، ومسارات التكامل المقدمة والمحتملة مع البرامج الأخرى، والمصادقة المعتمدة والأداء (بما في ذلك التعامل مع الملفات الكبيرة وعدد كبير من الملفات)، ووظائف البحث المحسنة، وإمكانية وطريقة عرض أنواع مختلفة من البيانات، ووظائف الويب الدلالية المقدمة ودعم قاعدة بيانات الرسم البياني، ودعم التنسيقات المفتوحة، والمتطلبات القانونية والتوصيات الخاصة بمستودعات البيانات المفتوحة، وكذلك الجوانب الأخرى المتعلقة بإمكانية الوصول (الأمن والخصوصية).

دراسة (2020) Yenlik, et al بعنوان:

"Development of an automated system model of information protection in the cross-border exchange"

تقدم هذه الدراسة نموذجا لنظام آلي لتبادل المعلومات الآمن عبر الحدود. وكان الدافع لهذه الدراسة هو الحاجة إلى نظام لتبادل المعلومات بين دولة كازاخستان – حيث يقيم الباحثون – ودول العالم، وخاصة دول الاتحاد الأوروبي. فالمشكلة الأساسية هنا هي تباين المواقف بين إدارات الدول المختلفة في التفاعل عبر الحدود، والذي أصبح أكثر تعقيدًا. ولحل هذه المشكلة فإن الباحثين أخذوا في الاعتبار قوانين ومتطلبات التعاون في (28)دولة في الاتحاد الأوروبي.

وتؤكد الدراسة أنه من المهم في ضمان أمن المعلومات في نظام الإدارة الآلي ضمان توافر وسلامة معلومات إدارة التكوين ومعلومات البيانات الشخصية. وأبدت اهتماما متزايدا لمنع الوصول غير المصرح به إلى النظام للحفاظ على أدائه المستقر. ومع ذلك ، نظرًا للعدد المتزايد باستمرار من الخدمات والهجمات المختلفة على حسابات المستخدمين ، هناك حاجة لاستخدام أساليب المصادقة الثنائية لضمان أمن المعلومات. في العقد الماضي ، تم استخدام هذه الأساليب على نطاق واسع في مختلف مجالات تكنولوجيا المعلومات والاتصالات. وهي تتعلق بقضايا تحديد والوصول إلى موضوع المعلومات السرية. يثق بها عدد كبير من الشركات، بما في ذلك مؤسسات التكنولوجيا ، والقطاعات المالية والتأمينية في السوق ، والمؤسسات المصرفية الكبيرة وشركات القطاع العام ، ومنظمات الخبراء المستقلة ، فضلاً عن شركات الأبحاث. وذلك باعتبار خوارزمية المصادقة ذات العاملين بناءً على برنامج المصادقة وتطبيق الهاتف المحمول لتحديد هوية المستخدم بشكل آمن.

وهذا النموذج قائم على تشفير البيانات ، والتوقيع الرقمي الإلكتروني (EDS) ، والتحكم في الوصول إلى المعلومات المخزنة على أساس المصادقة الثنائية، وحل حالات الصراع المحتملة.

وفي هذه الدراسة نجد وصفا تفصيليا للنموذج الرياضي لتشكيل التوقيع الرقمي والتحقق منه. كما نجد وصفا لتنفيذ البرنامج التدريجي لهذا النموذج مع تحليل النتائج.

ويمكن تلخيص هذه النموذج في خمسة مراحل:

- المرحلة الأولى: تشكيل ترميزات متعددة الحدود غير موضعية (NPNs).
- المرحلة الثانية: تشكيل مفاتيح (EDS). لكل من أرقام قاعدة العمل ، عناصر التوليد المقابلة (متعددة الحدود).
- المرحلة الثالثة: تجزئة الرسالة. تستخدم خوارزمية (EDS) لحساب قيمة التجزئة في (NPNs)
- المرحلة الرابعة: تشكيل (EDS). تم تحديد عدد صحيح عشوائي (K).
- المرحلة الخامسة: التحقق من التوقيع الرقمي.

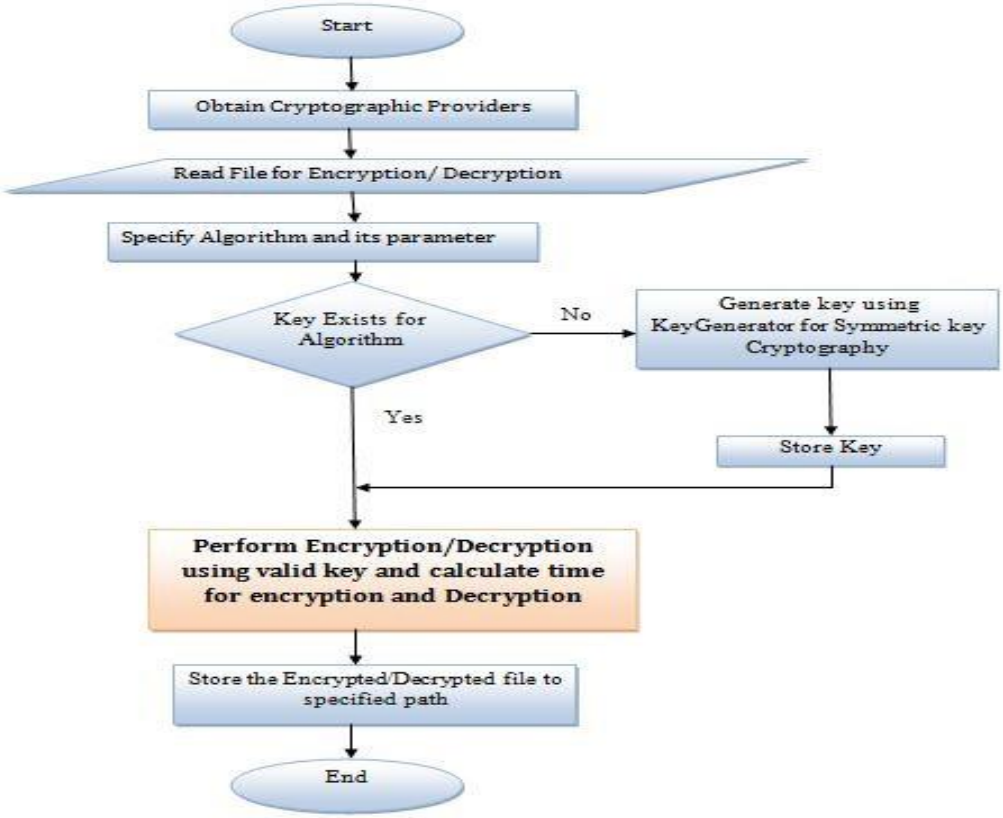
والنموذج يأخذ في الاعتبار خوارزمية المصادقة الثنائية القائمة على برنامج المصادقة والهاتف المحمول. وقد تم إجراء مولد سلسلة سري على أساس طريقة البحث الشامل. وتم وصف مولد الدوال المثلثية ، والذي يستخدم لحساب كلمة مرور لمرة واحدة. ونجد شرحا لتنفيذ البرنامج التدريجي لهذا النموذج. ثم يعرض النتائج التي تم تحليلها للخوارزمية.

تتميز هذه الدراسة بتطبيق عدة طرق لتحقيق الأمن للملفات في وقت واحد. فالنموذج المقدم قائم على التشفير والتوقيع الرقمي والمصادقة الثنائية. وبذلك يضمن سرية البيانات وتحديد الوصول إليها بالمستخدمين المخولين بذلك فقط.ومن نقاط ضعف الدراسة أنها لم تأخذ في الحسبان بعض أنواع الهجمات المحتملة الأخرى، مثل هجمات القناة الجانبية، والهجمات التي تستغل ذاكرة التخزين المؤقت .

دراسة (2020) Aloev and Nurullaev بعنوان:

"Software, Algorithms and Methods of Data Encryption Based on National Standards"

هدف هذه الدراسة هو تقديم حل لحماية الملفات الإلكترونية باستخدام تقنيتي التشفير والتوقيع الإلكتروني. حيث تقدم المقالة وصفًا لبرنامج مزود خدمة التشفير (Cryptography Service Provider) الذي طوره مؤلفو هذه المقالة ، والذي تم تصميمه لإنشاء مفاتيح تشفير (Encryption Keys)، وإنشاء مفاتيح خاصة وعامة للتوقيع الرقمي الإلكتروني (EDS)، وإنشاء وتأكيد صحة التوقيعات الرقمية ، والتجزئة ، والتشفير ، ومحاكاة البيانات باستخدام الخوارزميات المنسجمة مع معايير الدولة في أوزبكستان.



شكل رقم (7): مخطط لخوارزميات التشفير المفتاحي المتماثل [11]

لغات البرمجة الأصلية لهذا النظام هي C و C ++. يتضمن هذا النظام (CSP) المكونات الوظيفية التالية: مكتبة قابلة للتحميل ديناميكيًا تنفذ مستشعرًا للأرقام العشوائية ؛ مكتبة ديناميكية تنفذ خوارزميات التشفير وفقًا لمعايير الدولة

في أوزبكستان ؛ وحدة دعم العمل مع الأجهزة الخارجية ؛ وحدة التثبيت التي توفر تركيب CSP في بيئة التشغيل المناسبة (البيئة). يوفر CSP إنشاء مفاتيح EDS الخاصة والعامة ومفاتيح التشفير ؛ إنشاء وتأكيد صحة EDS وفقًا لخوارزميات محددة؛ تشكيل مفاتيح التشفير المشتقة المستخدمة بواسطة خوارزميات تشفير البيانات المرفقة؛ العمل مع المعلومات الأساسية المخزنة على الوسائط الخارجية ؛ تجزئة مناطق الذاكرة والبيانات الأخرى وفقًا للخوارزميات المرفقة ؛ تشفير مناطق الذاكرة والبيانات الأخرى وفقًا لخوارزميات تشفير البيانات المرفقة. يوفر CSP دعمًا لمعرفات الخوارزميات والمعلمات لتنفيذ التوافق مع موفري التشفير الخارجيين من حيث القدرة على العمل مع شهادات المفتاح العام الصادرة عن مراكز تسجيل تابعة لجهات خارجية ، بشرط استخدام خوارزميات التشفير المرفقة. يوفر موفر خدمة التشفير القدرة على العمل مع الشهادات الرقمية للمفاتيح العامة.

أحد أنظمة التشغيل التالية ضروري لأداء CSP:

Microsoft Windows XP (32 bit) Professional SP3; Microsoft Windows Vista Ultimate SP2; Microsoft Windows 7 (32 bit) Ultimate; Microsoft (32 bit) bit) Enterprise Edition R2 SP2; Microsoft Windows Server 2003 (32 SP2. Windows Server 2008 (32 bit) Enterprise Edition

ويوفر CSP العمل مع ناقلات المفاتيح الخارجية مثل USB-flash و eToken Aladdin (eToken ((JAVA) PRO 72K. كجزء من CSP ، يتم توفير الوحدات النمطية التي توفر استدعاء وظائف التشفير من خلال واجهة Microsoft CryptoAPI 2.0 عند التشغيل ضمن أنظمة تشغيل Microsoft.

ويدعم هذا البرنامج خوارزميات التشفير لجمهورية أوزبكستان وروسيا بالإضافة إلى بعض خوارزميات التشفير الشائعة المستخدمة في نظام التشغيل Windows ، مثل RSA و DES3 و SHA-1 وما إلى ذلك.

وأيضا يحتوي (CSP) على مكون يسمح لك بالتحقق من قابلية تشغيل خوارزميات التشفير المطبقة فيه أو أي خوارزميات متوافقة معها. حيث يوفر دعمًا لمعرفات الخوارزميات والمعلمات للتوافق مع موفري التشفير التابعين لجهات خارجية.

كما يوفر CSP العمل مع حاويات المفاتيح التي تحتوي على: مفاتيح التوقيع ومفاتيح التشفير والمعلومات الإضافية اللازمة لضمان الحماية المشفرة للمفاتيح وضمان التحكم في سلامتها. لحماية المعلومات الأساسية من الاستبدال أو التشويه أثناء تخزينها على محرك الأقراص الثابتة وشركات نقل المفاتيح الخارجية ، وكذلك أثناء التوزيع ، يتم توفير المعلومات الأساسية مع المجموع الاختباري.

ومن أجل ضمان الاستخدام الآمن لـ CSP المثبت على جهاز الكمبيوتر ، يتم توفير التدابير التنظيمية ، وكذلك يتم استخدام طرق البرامج والأجهزة ووسائل حماية المعلومات لضمان أن المفاتيح السرية المخزنة في ذاكرة الكمبيوتر أثناء

تشغيل CSP تظل سرية ، بالإضافة إلى معلمات خدمة CSP المخزنة على القرص الصلب. يحتوي CSP على مكون يسمح لك بالتحقق من تشغيل خوارزميات التشفير المطبقة فيه. يتم تنفيذ العمل على أساس أمثلة الاختبار.

ولضمان الاستخدام الآمن لتطبيق ما مع CSP مدمج، يتم توفير آليات للتحكم في تكامل مكتبات CSP. في CSP ، يتم استخدام مستشعر الأرقام العشوائية البيوفيزيقي لإنشاء تسلسلات ثنائية عشوائية تنفذ آلية إنشاء مفاتيح التوقيع الرقمي السرية ، ومفاتيح التشفير ، ونواقل التهيئة باستخدام خوارزميات مختلفة.

وكانت نتيجة هذه الدراسة هي الخروج بهذا البرنامج الذي يستخدم في حماية المستندات والملفات الإلكترونية. حيث يمكن استخدام هذا البرنامج في شبكات الاتصالات وأنظمة المعلومات العامة وأنظمة معلومات الشركات الحكومية من خلال تضمين التطبيقات التي تخزن وتعالج وتنقل المعلومات التي لا تحتوي على معلومات تتعلق بأسرار الدولة ، وكذلك في تبادل المعلومات وضمان الأهمية القانونية للوثائق الإلكترونية.

توصلت الباحثة الى أن فكرة هذا النظام تعتمد على الخوارزميات المطبقة في أوزبكستان وروسيا بالإضافة إلى بعض خوارزميات التشفير الشائعة المستخدمة في نظام التشغيل Windows، وهذا ما يجعل النظام محدود الاستخدام بعض الشيء، خصوصا من ناحية أنظمة التشغيل. ولكن مطوروا النظام جعلوه قابلا للتوافق مع خوارزميات أخرى، وقابل لتحميل مكتبات خارجية. كما أنه غير آمن على البيانات السرية مثل بيانات الدولة.

كما أن المعهد الوطني للمعايير والتقنية في الولايات المتحدة (NIST) أقر بأن معيار تشفير البيانات (DES) قد أصبح ضعيفًا في مواجهة التطورات في تحليل الشفرات والنمو الهائل في قوة الحوسبة، وحل محله المعيار AES.

دراسة (2020) Melman , et al بعنوان:

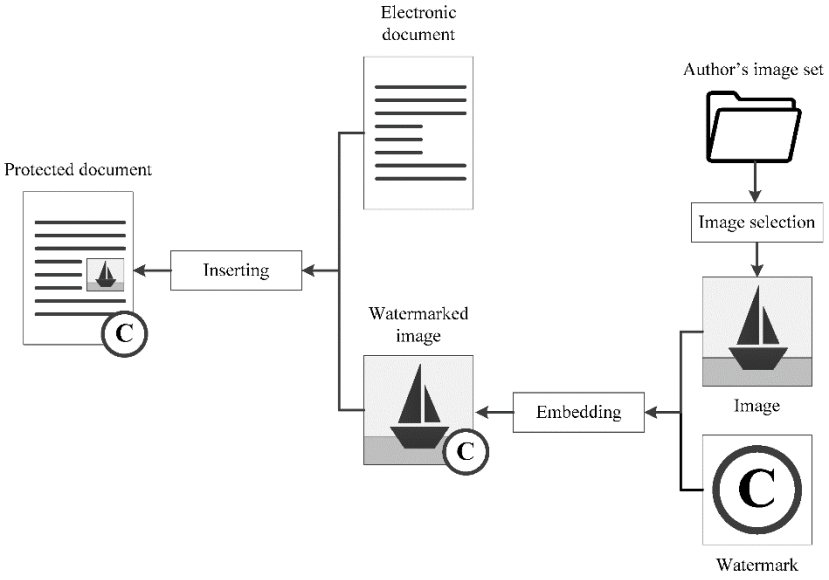
"An Authorship Protection Technology for Electronic Documents Based on Image Watermarking"

الهدف الرئيسي لهذه الدراسة هو حماية حقوق التأليف للمستندات الإلكترونية، وبشكل خاص تلك التي تحتوي على صور. والفكرة التي تقوم عليها هذه الدراسة هي أنه يمكن تحقيق ذلك عن طريق تضمين علامات مائية رقمية في الصور الموجودة في هذا المستند. وعلى عكس النص، الذي غالبًا ما تتم معالجته عند نسخه ، عادةً ما يتم نسخ الصور دون تغيير ، نظرًا لأن إعادة إنتاج مثل هذه الصورة قد يستغرق وقتًا طويلاً أو حتى يكون مستحيلاً. لا تؤدي المعالجة البسيطة للصورة المنسوخة إلى إتلاف العلامة المائية المضمنة. هذا يسمح بإثبات حق التأليف بنجاح، إذا لزم الأمر. يمكن أن توفر هذه التقنية حماية حقوق التأليف للنسخ المطبوعة من المستندات عندما يتم مسحها ضوئيًا باستخدام تطبيقات الهواتف الذكية الخاصة.

من الواضح أن المستندات الإلكترونية المحمية يجب أن تحتوي على نوع من الكائنات الرسومية لتنفيذ هذا النهج. ومع ذلك ، في الوقت الحالي ، هذه ليست مشكلة ، حيث أن العديد من المستندات الإلكترونية مصحوبة بالعديد من الرسوم التوضيحية والمخططات والصور والشعارات وعناصر الرسوم الأخرى.

وبالتالي ، تقترح الورقة تقنية جديدة باستخدام العلامات المائية الرقمية. كما تقترح تقنية لحماية تأليف المستندات الإلكترونية عن طريق تضمين العلامة المائية الرقمية في الصور الموجودة في المستندات الإلكترونية. من المزايا المهمة لهذه التقنية استخدام مجموعة من خوارزميات العلامات المائية عند التعامل مع صور من أنواع مختلفة.ويتم وصف وتحليل جميع السيناريوهات الممكنة لتنفيذ تقنية حماية حقوق التأليف هذه اعتمادًا على أي جزء من المستند (مستند كامل ، نص فقط أو صور فقط) يتم نسخه بواسطة الانتحال.

كما يتم التحقق من حدود قابلية تطبيق التكنولوجيا المقترحة باستخدام عدة خوارزميات للعلامات المائية من فئات مختلفة. يتم إجراء التجارب باستخدام كل من الصور التفصيلية الكلاسيكية والصور المركبة ذات التفاصيل الضعيفة.



شكل رقم (8): مخطط للتصميم المقترح

من نقاط قوة الدراسة أعلاه أنها تطرقت الى التقنية أعلاه وهي هامة للغاية في حماية المستندات التي تحتوي على صور، فيمكن تطبيقها على معظم الملفات الرقمية. وهذه الميزة تجعلها قابلة للتطبيق على المستند بغض النظر عن اللغة المكتوب بها. وهذا يوفر الكثير من الجهد، حيث أن خوارزميات التشفير مثلا تعتمد على لغة النص.

وأهم نقاط ضعف هذه التقنية المقترحة هي أنها قاصرة على المستندات التي تحتوي على صور فقط.

دراسة (2019) Elena, et al بعنوان:

"A Model of Achieving Safe Interoperability of Medical Data in the Private Sector of Health Care in Romania"

تهدف هذه المقالة الى تقديم رؤية لنظام قابل للتشغيل البيني في القطاع الخاص للخدمات الطبية في رومانيا الذي يعاني فجوة كبيرة في استكمال الملف الطبي للمريض الذي يستخدم الخدمات الطبية الخاصة والعامة. وهناك نقص تام في قابلية التشغيل البيني للبيانات الطبية على الرغم من نمو القطاع الطبي الخاص بشكل كبير في السنوات الأخيرة.

ومع توسع النظام الطبي الخاص، من المهم جدًا تحقيق قابلية التشغيل البيني للبيانات الطبية من النظام الصحي الخاص.

وفي هذه الرؤية يتم حماية البيانات الشخصية والبيانات الطبية من البداية من خلال تصميم هذا النظام. يتم استخدام معايير الأمان والسرية في هذا النظام من أجل إنشاء نقل آمن للبيانات الطبية.

يحتوي هذا النظام على مستندات طبية موحدة (في المفاهيم) ووثائق طبية قابلة للتشغيل المتبادل (باستخدام معايير التشغيل البيني للوثائق). هذان عنصران مختلفان ، الأول يشير إلى جمع السجلات الطبية لجميع المرضى لكل مجال طبي (على سبيل المثال: أمراض القلب والأمراض الجلدية وما إلى ذلك) والثاني يشير إلى معايير النقل مثل HL7 / CDA (المستوى الصحي السابع) / التصوير الرقمي والاتصالات في الطب).

يركز هذا النظام الجديد بشكل كبير على حماية البيانات الشخصية للمرضى.

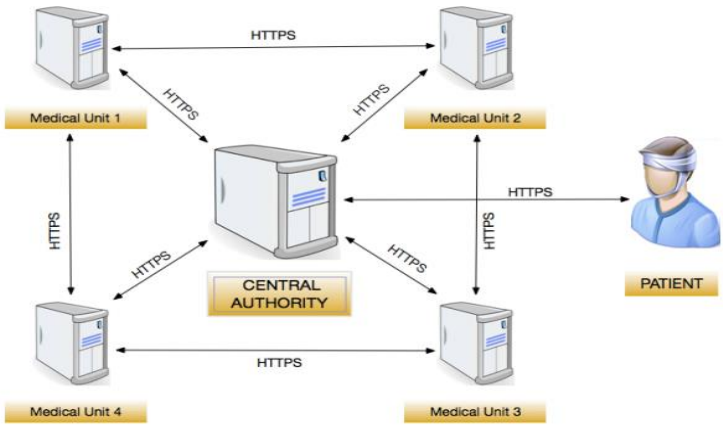


Fig. 1. Architecture of the proposed medical system

شكل رقم (9): تصميم النظام الطبي المقترح [4]

وتجيب الدراسة على السؤال الأكثر أهمية الذي يجب الإجابة عليه، وهو كيفية الحصول على البيانات الطبية التي يمكن أن تكون قابلة للتشغيل المتبادل لجميع الأنظمة الطبية ، وهو التوحيد القياسي (Standardization) لتحقيق قابلية التشغيل البيني الصحيحة.

ولتحقيق التوحيد القياسي لابد من توافر شرطين:

توحيد طريقة جمع البيانات السريرية – معيار البيانات السريرية – CDS. في جميع المجالات الطبية. فمن الضروري أن يكون لديك نفس هيكل الطريقة التي يتم بها جمع البيانات. لقد أدركت جميع المؤسسات الطبية هذا الامتياز ، ويتم الآن تطوير جهد عام في الحصول على أسئلة شائعة يجب استخدامها من قبل جميع الأطباء الذين يعملون في نفس المجال الطبي بهدف نهائي للحصول على بيانات سريرية موحدة.

قابلية التشغيل البيني بين أنظمة المعلومات الصحية. وهي ممكنة فقط من خلال تعريف الرسائل المعيارية ، والتي يجب أن تتبناها جميع الشركات المصنعة لهذا النوع من التكنولوجيا من أجل جعل تشغيل هذه الأنظمة فعالاً.

وتقدم هذه الدراسة الحلول التقنية للمراحل المختلفة لهذا النظام. مثل بنية المستندات السريرية وكيف تكون متوافقة مع متصفحات الويب. وكذلك فإن معيار DICOM هو المعيار للاتصال وإدارة معلومات التصوير الطبي والبيانات ذات الصلة. يغطي معيار DICOM مجال المعلوماتية الطبية. ضمن هذا المجال ، يتناول تبادل المعلومات الرقمية بين معدات التصوير الطبي والأنظمة الأخرى. نظرًا لأن مثل هذه المعدات يمكن أن تتفاعل مع الأجهزة الطبية الأخرى ، يجب أن يتداخل الغرض من هذه المواصفة القياسية مع المجالات الأخرى للمعلوماتية الطبية. وتؤكد الدراسة إن أهم مشكلة يجب إدارتها بشكل صحيح وجيد هي ضمان سرية وخصوصية السجلات الطبية للمريض.

يؤكد الباحثان أن هذا النظام يتمتع بالعديد من المزايا مثل:

– يستخدم البيانات الطبية التي تم جمعها ، مما يعني أن الطبيب الذي يعاين المريض لديه استبيان موحد لتشخيص المريض وهذه الحقيقة تقلل من فرصة نسيان المعلومات الضرورية من أجل وضع التشخيص الصحيح.

– يتم تخزين البيانات الطبية في الوحدة الطبية حيث يتم جمعها. هذا له ميزة عدم تكرار البيانات الطبية.

يمكن تصور جميع البيانات الطبية (Visualization) من قبل جميع المشاركين للنظام (الأطباء) ، ثم تختفي المعلومات، وبعد استخدامها ، تظل في قاعدة البيانات الأولية حيث يمكن استخدامها مرة أخرى في المستقبل.

– يسمح هذا النظام بسهولة إجراء ذكاء الأعمال (BI-Business Intelligence) من أجل إجراء بحث مكثف حول الحالة الصحية للسكان ، أو التنبؤ بأي مجال مرضي يثير الاهتمام في فترة زمنية.

– لديه القدرة على تقليل تكاليف خدمات الرعاية الصحية ، باستخدام المعلومات الطبية الموجودة ، دون الحاجة إلى التحقيق مرة أخرى مع المريض إذا تم التحقيق في ذلك بالفعل في مكان آخر.

من نقاط ضعف هذه الدراسة أنها ركزت على تحقيق التشغيل البيني والتكامل بين الأنظمة الطبية. وبطبيعة الحال يعتمد ذلك على البنية التحتية الرقمية الموزعة، والذي يجعلها عرضة لمخاطر أمنية عديدة. فيجب اتخاذ إجراءات لتقليل المخاطر الأمنية ومعالجة الحوادث الأمنية عندما تحدث. اضافة لذلك لم تشر الدراسة إلى أهمية وجود سياسة فعالة للنسخ الاحتياطي للبيانات في جميع المراكز الطبية المترابطة، وفي قاعدة البيانات الرئيسية.

مناقشة النتائج

وبعد فحص هذه الدراسات، تبين أنه لابد من اتخاذ جميع أشكال التهديدات على محمل الجد، وسد كل ثغرة يمكن أن تمثل فرصة للمخربين والمتطفلين وحتى مفتقدي الأمانة العلمية.

فبداية من بنية المستودعات الرقمية ومختلف أشكال التخزين الرقمي والسحابي، لابد أن تكون بنية مصممة بشكل صحيح تدعم المعالجة الفعالة للبيانات والملفات الرقمية بجميع أنواعها، وطريقة عرضها عالميا، وطرق للوصول إلى سجلات البيانات واستكشافها، ووظائف البحث المحسنة. بل واتباع طرق تأمين البيانات حتى في عملية الرفع أو التنزيل، بالإضافة إلى المتطلبات القانونية.

وكذلك تحديد كيفية التعامل مع العمليات في مستودع رقمي، وكيفية استخدام الحلول السحابية في بنائه، وكيفية العمل مع واجهات المستخدم، وكيفية معالجة الوسائط المتعددة المجمعة.

وعند اختيار طريقة من طرق تشفير البيانات، من المهم تطوير نظام تشفير فعال وآمن للحفاظ على البيانات والخصوصية الرئيسية، واختيار خوارزميات التشفير المناسبة لنوع البيانات وفي نفس الوقت تكون متوافقة مع الأنظمة العالمية.

وهناك طريقة ادخال العلامة المائية في الملفات التي تحتوي على صور من أجل حمايتها.

ايضا يجب دراسة وتقدير أنواع الملفات المستخدمة في المشروع من ملفات نصية أو صور أو فيديو، وكل منها له أنواع وامتدات عديدة.

الاستنتاج

من الواضح أن المخاطر الأمنية على الملفات الرقمية في ازدياد مستمر، ولابد لكل مؤسسة تمتلك مثل هذه الملفات أن تواكب مستجدات السياسات والتطبيقات الأمنية التي تحمي أصولها الرقمية بشكل فعال.استنتجت الباحثة أنه يتوجب على كل مؤسسة مراعاة إجراءات الأمان المختلفة بما فيها، إجراءات الأمان لعمليات تنفيذ التخزين – أمان التخزين المادي – حماية البيانات — تطبيق سياسات النسخ الاحتياطي واستعادة البيانات والأرشفة – النسخ المجدول – الحماية المستمرة للبيانات — تطبيق سياسات المصادقة والتحكم في الوصول إلى البيانات – مراعاة سياسات مواصفات كلمات المرور — تطبيق سياسة واضحة للامتيازات والصلاحيات — تحديد صلاحيات الوصول إلى الملفات.

التوصيات

ينبغي على المؤسسات تقديرالقيمة الاقتصادية للتحول الرقمي في جميع المعاملات، وخاصة من ناحية البرامج والبروتوكولات المستخدمة في تطوير وتنفيذ أدوات التشفير والإخفاء وغيرها.

بالرغم من أن وجود لوائح دولية لتنظيم تبادل وتداول المعلومات وحماية البيانات، إلا أن هناك حاجة لتنسيق دولي حول قوانين تنظم تبادل المعلومات عبر الحدود.

هناك حاجة إلى التعاون الدولي لتطوير خوارزميات التشفير والإخفاء والعلامة المائية والمصادقة المتعددة، بحيث تكون صالحة للتطبيق في جميع دول العالم.

مهمة صيانة البنية التحتية لا تعتمد فقط على القضايا المتعلقة بالأجهزة. فمشكلات البرامج، خاصة المتعلقة بالتبعية الناشئة عن آليات الأمان المطبقة، مهمة أيضًا. فهي تفرض الحاجة إلى الحصول على الشهادات وتحديثها أو الاحتفاظ بأسماء النطاق.

في حالة ما إذا كان مستودع البيانات موجود داخل المؤسسة، فلابد من وجود برامج قوية لمواجهة خطر الفيروسات الضارة.

الاتفاق مع مقدمي خدمات التخزين السحابي يجب أن يكون واضحا ومحددا من ناحية سياسة النسخ الاحتياطي، وطرق ومعدلات إزالة البيانات النادرة الاستخدام أو المتكررة.

تدريب الكوادر البشرية من المتعاملين مع البيانات تدريبا كافيا يمنحهم المعرفة الكافية بأهمية الملفات والبيانات التي يتعاملون معها. وكذلك الإلمام بالمخاطر المختلفة التي قد تتعرض لها تلك البيانات، وطرق الوقاية من تلك المخاطر والتعامل معها في حال وقوعها.

عند البحث عن أفضل الطرق لحفظ وتأمين وإدارة المستندات الرقمية، يفضل اللجوء إلى الشركات الكبرى المتخصصة في هذا المجال. وعلى سبيل المثال:

شركة أوراكل العالمية التي تقدم نظام (Oracle Content Management). وهو نظام إدارة محتوى مؤسسي، يجمع بين إدارة المستندات وإدارة محتوى الويب وإدارة الأصول الرقمية ووظيفة الاحتفاظ بالسجلات لمساعدة الشركات على تقليل التكاليف ومشاركة المحتوى وأتمتة العمليات التي تستغرق وقتًا طويلاً.

تقدم شركة أمازون نظام (Amazon DocumentDB). وهو عبارة عن خدمة قاعدة بيانات مستندات سريعة وقابلة للتطوير ومتاحة للغاية ومدارة بالكامل. ويمكن استخدامها دون القلق بشأن إدارة البنية التحتية الأساسية. وكقاعدة بيانات للمستندات، فإنها تجعل من السهل تخزين البيانات والاستعلام عنها وفهرستها.

المراجع

Tomasz Kubik, and Agnieszka Kwiecień. (2021), “Resolving Dilemmas Arising during Design of Digital Repository of Heterogenic Scientific Resources”. Available online at: https://doaj.org/article/b3c23ad70c424edabddeeaea1e4d6366

Yange Chen, Hequn Liu et al. (2021). "A threshold hybrid encryption method for integrity audit without trusted center". Available online at: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-020-00222-6

Lidia Ogiela, Marek R. Ogiela, and Hoon Ko. (2020). "Intelligent Data Management and Security in Cloud Computing". Available online at: https://www.mdpi.com/1424-8220/20/12/3458

Madalina-Elena RAC-ALBU and Marius RAC-ALBU. (2019). "A Model of Achieving Safe Interoperability of Medical Data in the Private Sector of Health Care in Romania". Available online at: https://doaj.org/article/21a288ec73db497b8bacae44f20028c2

Begimbayeva Yenlik, Ussatova Olga et al. (2020). "Development of an automated system model of information protection in the cross-border exchange". Available online at: https://www.tandfonline.com/doi/full/10.1080/23311916.2020.1724597

Rakhmatillo Djuraevich Aloev and Mirkhon Mukhammadovich Nurullaev. (2020). "Software, Algorithms and Methods of Data Encryption Based on National Standards"
Available online at: https://journals.iium.edu.my/ejournal/index.php/iiumej/article/view/1179

Anna Melman, Oleg Evsutin, and Alexander Shelupanov. (2020). "An Authorship Protection Technology for Electronic Documents Based on Image Watermarking" Available online at: https://www.mdpi.com/2227-7080/8/4/79

John Faundeen. (2017). "Developing Criteria to Establish Trusted Digital Repositories"
Available online at: https://doaj.org/article/4b7a7e90bce6480daacf8a80ee551e92

University of BRISTOL. (2018). "Document Management Policy" Available online at: https://www.bristol.ac.uk/media-library/sites/secretary/documents/information-governance/document-management-policy.pdf

National Institutes of Standards and Technology (NIST). (2018). "The Economic Impacts of the Advanced Encryption Standard, 1996-2017" Available online at: https://csrc.nist.gov/publications/detail/white-paper/2018/09/07/economic-impacts-of-the-advanced-encryption-standard-1996-2017/final

Ranjeet Masram, Vivek Shahare et al. (2014). "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features". Available online at: https://www.researchgate.net/publication/284459595_Analysis_and_Comparison_of_Symmetric_Key_Cryptographic_Algorithms_Based_on_Various_File_Features