جامعة إفريقيا العالمية
عمادة الدراسات العليا والبحث العلمي والنشر
كلية إقرأ لدراسات الحاسوب
قسم تقانة معلومات

تحسين الأمنية بتطوير نموذج للتوثيق وفحص سلامة ملفات المستخدم لتطبيقات الويب السحابية العامة

بحث مقدم لنيل درجة الماجستير في تقانة المعلومات

إعداد الطالب: راجي اتويبي عبد المجيد
إشراف: د. مرتضى آدم مالك الحاج

خرطوم–السودان

1144هـ-2020م


بسم الله الرحمن الرحيم
١٤١٨

الاستهلال

قَال تعَالَىَ:

﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا قِيلَ لَكُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا يَفْسَحِ اللَّهُ لَكُمْ ۖ وَإِذَا قِيلَ انشُزُوا فَانشُزُوا يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ۚ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ﴾ ... سورة المجادلة الآية (11)

صدق الله العظيم.

الإهداء

أهدي هذا العمل المتواضع لكل الباحثين وطلاب العلم وكل من في الرحلة لاكتساب العلم

الشكر والتقدير

كل الشكر والحمد لله الذي منحني القوة والدعم والإرشاد وتخفيف الصعوبات التي واجهتها أثناء إعداد هذا البحث.

أود أن أعرب عن عميق امتناني لمشرفي العظيم، **الدكتور مرتضى مالك آدم الحاج**، أستاذ في تقانة المعلومات في الجامعة أفريقيا العالمية، الذي قام بتوجيهني وصححني، وقدم لي الكثير من التوصيات بلا كلل حتى تمكنت من تحقيق أهداف هذا البحث.

كما أود أن أشكر **الدكتور البراء أبو عبيدة**، عميد كلية اقرأ لدراسات الحاسوب في جامعة أفريقيا العالمية، على كلماته المستمرة في التشجيع والمساعدة. كما أود أن أشكر جميع أعضاء هيئة التدريس في الكلية لدعمهم لي بشكل مباشر وغير مباشر.

ولا انسى شكري لوالدي **المهندس عبد الرشيد راجي والسيدة مسلمة علي**، الذين يتفهمون ويدعمون دائمًا. لقد ضحوا بكل ما يلزم للتأكد من أنني لم اجد الصعوبة أكاديميا، فأعرب عن امتناني الدائم لهم. شكر خاص لأخي وأختي، **مبارك راجي وأمينة راجي** لدعمهما ولتشجيعهما.

وشكرى الخاص للدكتورة **هناء يوسف** التي ساعدتني كثيرًا في إكمال هذا البحث. لا يمكنني أن أنسى شكر لزميلي **على بكيل** ولزملائي في كلية اقرأ لدراسات الحاسوب الذين ساندوني حتى الانتهاء من هذا البحث.

قائمة المحتويات

فهرس الأشكال

فهرس الجداول

قائمة الاختصارات

الاختصار	معني بالغة العربية	معني بالغة الانجليزية
SaaS	البرمجيات كخدمة	Software as a service
IaaS	البنية التحتية كخدمة	Infrastructure as a service
PaaS	النظام الأساسي كخدمة	Plateform as a service
MAC		Message Authentication Code
CC	الحوسبة السحابية	Cloud Computing
CPU	وحدة المعالجة المركزية.	Central Processing Unit
CIA	السرية وتكامل البيانات والتوثق.	Confidentiality, Availability, Availability.
RSA	خوارزمية رافست شامير.	Ravist Shamir Algorithm
AES	نظام التشفير المتقدم.	Advanced Encryption System
SHA3	خوارزمية هاش الآمنة.	Secure Hashing Algorithm 3
CSA	التحالف الأمن سحابة.	Cloud Security Alliance
K-Gen	توليد المفتاح.	Key Generation
PK	المفتاح العام.	Public Key
SK	المفتاح السري	Secret Key
M	رسالة	Message
TPA	مدققو الطرف الثالث.	Third party Auditors

NIST	المعهد الوطني للمعايير والتكنولوجيا	National Institute of Standards and Technology
DoS	الحرمان من الخدمة.	Denial of Service
E-Data	البيانات المشفرة.	Encrypted Data
E-Skey	المفتاح السري المشفر.	Encrypted Secret key
MFA	توثق متعددة العوامل	Multi Factor Authentication
POR	إثبات الموثوقية	Proof of Reliability
HAIL	طبقة توفر ونزاهة عالية	High Availability and Integrity Layer
PKI	البنية التحتية للمفتاح العام	Public Key Infrastructure
SSO	تسجيل الدخول الأحادي	Single Sign On
DBMS	نظام إدارة قواعد البيانات	Database Management System
ACID	الاتساق , العزلة , المتانة	Atomicity, Consistency, Isolation, Durability
CSP	مزود خدمة السحابي	Cloud Service Provider
RBAC	التحكم في الوصول المسند الي الدور القائم	Role Based Access Control
KHMC	رسائل هاش ذات المفاتح	Key Hashed Message Code
PDP	اثبات ملكية البيانات	Proof of Data Possession

DAC	التحكم في الوصول المستقل	Discretionary Access Control
SDDB	النسخ الاحتياطي الآمن للبيانات الموزعة	Secure Distributed Data Backup
TTP	طرف ثالث موثوق به	Trusted Third Party
ABS	توقيع يستند إلى السمة	Attribute Based Signature

المستخلص

يتم اعتماد علي الحوسبة السحابية بشكل عام وقد أظهر تأثيرًا كبيرًا على تطوير الأعمال، وهو يتيح الوصول عند الطلب إلى مجموعة مشتركة من موارد الحوسبة السحابية. الحوسبة السحابية يواجه العديد من المشاكل الأمنية مثل أي نظام إلكتروني آخر، ومن بين هذه المشاكل هي الهجمات على التوثق من المستخدم وبالتالي تؤثر علي سلامة البيانات وسريتها وخاصة في بيئة الحوسبة السحابية العامة. تلعب التوثق دورًا كبيرًا في الحفاظ على أمان البيانات والمعلومات في بيئة السحابة. ويجب على مستخدمي السحابة التأكد من سلامة ملفاتهم المخزنة في السحابة.

في هذا البحث، الهدف الرئيسي هو إنشاء نموذج للتوثيق من المستخدم والتحقق من سلامة الملفات المخزنة في الحوسبة السحابة العامة وذلك من خلال دراسة النماذج الأمنية في الحوسبة السحابية العامة وتحليلها خاصة التي تحقق سلامة البيانات او الملفات وخاصة للتوثق من المستخدم.

واتبع البحث المنهجية التفصيلية والاستنتاجية والتطبيقية والنماذج الأولية وتم تطوير النموذج لنظام للتوثق المستخدم ونظام التحقق من سلامة الملفات، في نظام توثق المستخدم، استخدمنا التوثق الثنائية حيث التي تتكون من كلمة السر والتوقيع الرقمي. علما بان جميع البيانات تكون مشفرة من جانب العميل والخادم قبل الإرسال. بالنسبة لنظام التحقق من سلامة الملفات، استخدم النموذج خوارزمية هاش الآمنة حيث يتم احتساب قيمة تجزئة الملف وتشفيره قبل الإرسال الي السحابة، ويتم تشفير جميع عملية نقل الملفات بين مزود السحابة والمستخدم باستخدام نظام تشفير الاستخدام المتماثل وغير المتماثل. استخدمنا العديد من أدوات مثل لغات البرمجية لتنفيذ النموذج و ايضا أجريت العديد من التجارب و أثبتت أن النموذج فعال ومقبول.

واهم النتائج التي وجدنا هو ان النموذج يقدم نظام قوي للتوثق المستخدم ونظام للفحص الفشل للتكامل الملفات في حوسبة. يوفر النموذج أيضًا السرية وعدم التنصل. يزيد نموذجنا المقترح من ثقة المستخدم في التطبيقات السحابية، كما يقلل النموذج أيضًا من قوة الحساب على أجهزة المستخدم. ومن اهم التوصية هو ان يجرى دراسات مستقبلية لحل مشكلة هجمات التصيد الاحتيالي لصفحات الويب، ويمكن أيضًا تحسين النموذج للتحقق من سلامة الملفات التي تتم مشاركتها بواسطة عدة المستخدمين وتكييف النموذج مع خوارزميات الأمان الجديدة.

Abstract

Cloud computing is being adopted generally and it has shown a high impact on the development of businesses, it enables on-demand access to a shared pool of configurable computing resources. Cloud computing faces many security problems like any other electronic system, and among these problems is the attacks on user authentication and thus on the integrity and confidentiality of data especially in the public cloud computing environment. Authentication plays a major role in keeping information secure in the cloud environment. Cloud users must ensure the integrity of their files stored in the cloud.

In this study, the main objective is to develop a model for user authentication and checking the integrity of files stored in the public cloud, by studying the state of art of security models in public cloud computing and analyzing them, in particular the models for integrity of data or files and user authentication.

This study uses the descriptive, deductive, applied and prototype methodology. We developed a model for the user authentication and file integrity checking for files in the cloud, in the user authentication system, we used two-factor authentication that involves password and digital signature which uses the certificate-based authentication. For the file integrity checking system, the model used a secure hashing algorithm whereby the file hash value is calculated and encrypted before sending to the cloud. All file and data transfers between the cloud provider and the user are encrypted using the symmetric and asymmetric encryption system. We used several tools and programming languages to implement the model and experiments. Our experiments proved that the model is effective and acceptable.

Among the most important results is that the model provides strong user authentication and integrity checking system for cloud users and files. The model also provides confidentiality and non-repudiation. It also increases user confidence in cloud applications as we ensured secure connection between cloud users and cloud service providers, the model also uses less computation power on user devices. Future studies should be conducted to solve the problem of phishing attacks for web pages, and the model can be improved to verify the integrity of files shared by multiple users and adapt the model to new security algorithms.

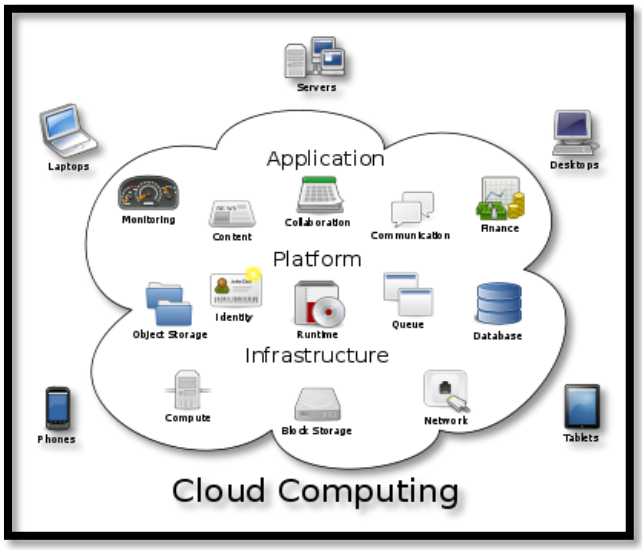
الفصل الأول

المقدمة

1. مقدمة.

البيانات في عصرنا والتي يشير إليها بعض الخبراء على أنها "ذهب" تعد موردا قيما، وإدارة البيانات التي تشمل ضمان سلامتها وسريتها وتوافرها وظيفة مهمة. بشكل عام، يتم تخزين البيانات في أجهزة التخزين مثل الأقراص الثابتة وأقراص DVD والأقراص المدمجة والأقراص المرنة. لقد أدى إدخال أنظمة قواعد البيانات إلى تعزيز إدارة المعلومات، ويمكن معالجة بيانات اليوم بكفاءة على منصات الحوسبة والتخزين الكبيرة التي يمكن الوصول إليها عبر الإنترنت، ويعود ذلك إلى التقدم الهائل في تقنيات الإنترنت وأنظمة قواعد البيانات وهذا جلب نماذج حوسبة جديدة، وتشمل هذه النماذج تطوير الحوسبة الشبكية في أوائل التسعينيات؛ بالإضافة إلى حوسبة المرافق والحوسبة السحابية، تم تطويرها في عام 2005 [12] وحوسبة الضباب"Fog computing" التي تم تقديمها في عام 2010.

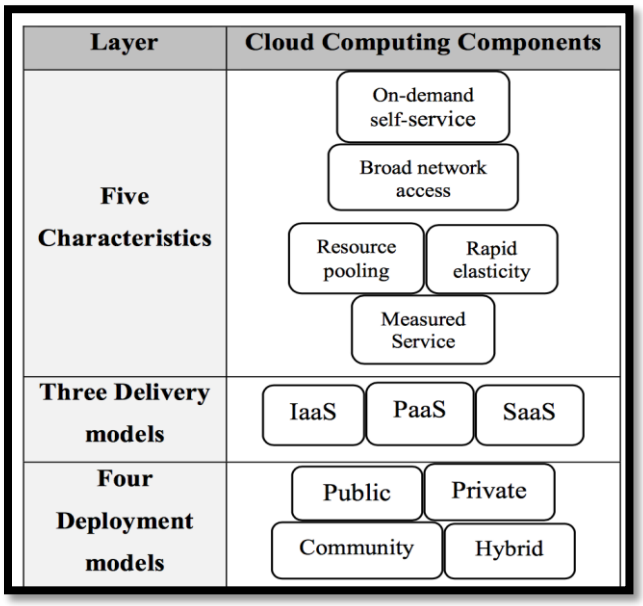
الحوسبة السحابية هي نموذج لتمكين الوصول في كل مكان وشبكة مريحة عند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم ووحدات التخزين والتطبيقات والخدمات) التي يمكن توفيرها وإصدارها بسرعة بأقل مجهود إداري أو تفاعل مزود الخدمة. يمكن الوصول إلى الخدمات السحابية من أجهزة الكمبيوتر المحمولة والهواتف وأجهزة الكمبيوتر المكتبية والطاولات وما إلى ذلك كما هو موضح في الشكل 1.1.



الشكل(1.1) نظرة عامة للحوسبة السحابية

كما هو مبين في الشكل 2.1 أدناه، يتكون نموذج السحابة من خمس خصائص أساسية وثلاثة نماذج للخدمة وأربعة نماذج للنشر. الخصائص الأساسية الخمسة هي الخدمة الذاتية عند الطلب، والوصول

إلى شبكة واسعة، وتجميع الموارد، والمرونة السريعة، والخدمة المقاسة. نماذج الخدمة الثلاثة هي البرامج كخدمة (SaaS) ومنصة كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) بينما نماذج النشر الأربعة هي سحابة خاصة وسحابة عامة وسحابة مختلطة وسحابة مجتمع. [1] ، [2].



الشكل(2.1) نموذج الحوسبة السحابية

تعد المحاكاة الافتراضية واحدة من التقنيات الرئيسية لخدمات الحوسبة السحابية، ومنشآتها، وتجميع أنظمة متعددة قائمة بذاتها في نظام أساسي فردي للأجهزة من خلال تصور موارد الحوسبة (مثل: الشبكة، ووحدة المعالجة المركزية، والذاكرة، والتخزين). يسمح لموفري الخدمة السحابية بمشاركة مثيل فعلي واحد لمورد أو تطبيق ما بين العديد من العملاء والمؤسسات. يتم ذلك عن طريق تعيين اسم منطقي للتخزين الفعلي وتوفير مؤشر لذلك المورد الفعلي عند الطلب [13]. من بين شركات الحوسبة السحابية الكبرى: Amazon و sales.com و Google وغيرها.

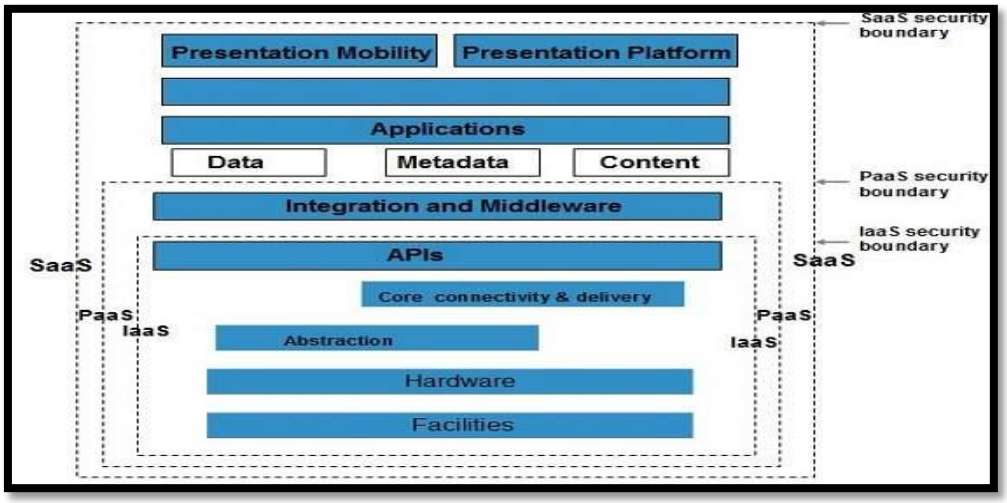
1.1 معلومات أساسية عن أمن الحوسبة السحابية

التخزين السحابية هو نموذج للحوسبة السحابية يخزن البيانات على الإنترنت من خلال مزود الحوسبة السحابية الذي يدير ويدير تخزين البيانات كخدمة. يتم توفيرها عند الطلب مع توفير السعة والتكاليف في الوقت المحدد، كما تعمل على التخلص من شراء البنية الأساسية لتخزين البيانات وإدارتها.

يمنحك هذا خفة الحركة"Agility"، النطاق العالمي"Global scale" والمتانة"Durability"، مع الوصول إلى البيانات في أي وقت وفي أي مكان. [3] ينقل الأشخاص بياناتهم إلى السحابة نظرًا لأن البيانات تصبح أكبر ويجب أن تكون متاحة من العديد من الأجهزة. لذلك، يصبح تخزين البيانات على السحابة فكرة مقبولة. في هذا البحث، سوف نقدم تحليلًا للتقنيات المختلفة المستخدمة لتكامل البيانات في السحابة. عند مقارنتها بالمزايا والعيوب، ثم اقترح نموذجنا المحتمل.

الأمن في الحوسبة السحابية هو مصدر قلق كبير. يجب أن يتم تخزين البيانات مشفرة في السحابة في شكل مشفر. لتقييد العميل من الوصول إلى البيانات المشتركة مباشرة، يجب استخدام خدمات البروكسي والوساطة.[13] في عام 2018، أفادت ممارسة أطباء الأطفال في كاليفورنيا التي تعرضت لها فدية بأن ملفات المرضى "قد تم تغييرها" أو "تالفة". [13] وفي عام 2006، واجه Gmail أيضًا حذفًا جماعيًا للبريد الإلكتروني مما أدى إلى فقدان البيانات [5]، على الرغم من أن معظم مزودي السحابة مثل amazon تحملوا مسؤولية إخفاقات الأمن، لكن هذا لا يكفي يجب أن تكون هناك تقنيات فعالة للحفاظ على سلامة البيانات في السحابة.[4]

يحدد نموذج مكدس Cloud Security Alliance (CSA) الحدود بين كل نموذج خدمة ويوضح مدى ارتباط الوحدات الوظيفية المختلفة ببعضها البعض [13] كما هو موضح في الشكل 3.1 أدناه.

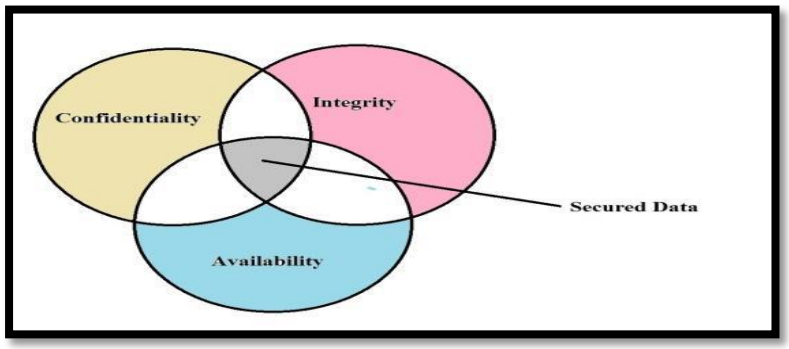


الشكل (3.1) التحالف الأمني

النموذج "CIA:Confidentiality, Integrity, Availability" يتكون من السرية وتكامل البيانات والتوافر يلعب دوراً مهماً في معالجة مختلف قضايا الأمن، حيث تم إنشاء ثالوث CIA لأمن المعلومات

لتوفير معيار أساسي لتقييم وتنفيذ أمن المعلومات بغض النظر عن النظام و / أو المؤسسة الأساسية. [6]

السرية: يقال إنه يتم الحفاظ على سرية بيانات المستخدم إذا لم يتم تسريب بيانات المستخدم إلى كيان غير مصرح به. تكامل البيانات: –يقال الحفاظ على سلامة بيانات المستخدم في حالة بقاء المحتويات كما هي بعد الاستعانة بمصادر خارجية لخدمة مزودي الخدمة السحابية. التوفر: يشير التوفر إلى ضمان وصول المستخدم المصرح له إلى المعلومات عند الاقتضاء. التوافر مضمون من خلال صيانة الأجهزة وكذلك الحفاظ على نظام التشغيل في أداء مناسب حيث لا يحدث أي نوع من تعارض البرامج [6]. كما هو مبين في الشكل 4.1 أدناه، إذا كان مزود الخدمة السحابية يحافظ على السرية والتوافر وتكامل البيانات من البيانات التي تعتبر آمنة.



الشكل (4.1) نموذج "CIA"

تكامل البيانات في النظام السحابية يعني الحفاظ على سلامة المعلومات المخزنة. يجب عدم فقدان البيانات أو تعديلها من قبل المستخدمين غير المصرح لهم. موفري الحوسبة السحابية موثوقون للحفاظ على سلامة البيانات ودقة البيانات. ذكرت [8] في عام 2016 أن من بين تهديدات سلامة البيانات هي بيانات المستخدمين التي يتم اختراقها أو تغيير معلوماتها أو تعديلها من قبل كيانات داخلية أو خارجية. قد يحدث خلل في تكامل البيانات أيضًا من خلال أخطاء برامج مايو، والإصدارات الخلفية في تطبيقات مختلفة، وإصدارات التطبيقات القديمة، والمكونات الإضافية، والقوالب، أو الخلل في النظام، أو المتسللين ذوي الدوافع الاقتصادية، والرمز الضار وأشكال التحميل المختلفة، على الرغم من أن معظم مزودي السحابة يبذلون قصارى جهدهم لمنع هذه الهجمات، من بين الآليات المستخدمة لحماية البيانات التحكم في الوصول والتوثق والتدقيق والترخيص [13]. تم أيضًا تطوير العديد من تقنيات

التحقق من تكامل البيانات من قِبل الباحثين، والتي تتضمن في الغالب استخدام مراجعي الطرف الثالث "TPA-Third Party Auditor" [9] ويستخدمون تقنيات مختلفة مثل "Secure Hashing Algorithm–SHA"، وبيانات التملك المحتملة "PDP:Provable Date Possession"، ونظام PDP الأساسي بناءً على PDP،MAC قابلة للتطوير: PDP الديناميكي، والدليل الأساسي على عدم قابلية الاسترجاع "POR:Proof of data Retrievability" استنادًا إلى دالة هاش ذات المفاتيح(F)hk.[10,11]

في هذا البحث سوف ندرس بداية فن تكامل البيانات في الحوسبة السحابية، والنماذج المتاحة للحفاظ على تكامل البيانات في الحوسبة السحابية ونقترح نموذجًا أكثر كفاءة للحفاظ على سلامة البيانات في السحابة.

2.1 مشكلة البحث

من خلال الاعتماد الأخير الواسع لخدمات الحوسبة السحابية، يفضل المستخدم استخدام السحابة لتخزين ومعالجة كمية كبيرة من البيانات والمعلومات التنظيمية، وهذا يفرض تحديات على نموذج CIA بسبب الحجم الهائل للمعلومات التي يجب حمايتها على الرغم من ان مزودي خدمات التخزين السحابية غالبًا ما تنص على أنها توفر بيئة آمنة للبيانات المخزنة، ويأتي تعدد مصادر البيانات والمعلومات من التنسيقات المتنوعة الموجودة، وهناك حاجة للتأكد من أن نموذج معالجته CIA مضمون لضمان ثقة العميل.قام بحث حديث [57] بتقييم أربعة أنظمة تخزين سحابية: Mozy وCarbonite وDropbox وCrashPlan. بعد التقييم، تبين أنه لا يمكن لأي من هذه الأنظمة توفير أي ضمانات لتكامل البيانات. من بين أسباب فشل سلامة البيانات تقنيات التوثق الضعيفة، وهذا يؤدي إلى الوصول غير المصرح به إلى البيانات التي تشكل تهديدات كبيرة لملف المستخدم حيث يمكن للمستخدم الضار الوصول إلى البيانات وبالتالي التأثير على سلامة الملفات. يجب التأكد من المستخدمين السحابين أن البيانات التي يتم الاستعانة بمصادر خارجية لها على السحابة لا تزال كاملة وصحيحة وعند تحميلها، هناك حاجة ملحة لنموذج ذو توثق قوية للمستخدم يضمن الحفاظ على سلامة الملفات في السحابة. في هذا البحث، سنقترح ونطور نموذج الأمان المحسن للتوثق المستخدم والتحقق من سلامة البيانات للملفات في السحابة.

1. الوصول الي الملفات من قبل مستخدميسن غير مصرح.
2. هذف البيانات والملفات سرية ولم يطلع عليها احد.
3. عدم وجود نموذج لتقق منسلامة الملفات.

3.1 الأهداف البحث

1.3.1 الأهداف العامة

الهدف العام لي هذا البحث هو بناء نموذج للتوثق المستخدم وفحص سلامة الملفات وذلك للحفاظ على سلامة البيانات في السحابة عامة. يعتمد نموذجنا المقترح على استخدام الشهادة الرقمية وهاش الآمنة للملفات وتوثق المستخدم.

1.3.2 أهداف محددة

1. دراسة طبيعة عمل ومشاكل الامنية التي تواجه الحوسبة السحابية.
2. تحليل نموذج أمان تكامل البيانات المعروف في الحوسبة السحابية.
3. اقتراح نموذج حماية تكامل البيانات في الحوسبة السحابية.
4. تصميم وتنفيذ النموذج المقترح.
5. تجربة وتقييم النموذج المقترح.

4.1 أسئلة البحث

1. ما هي نماذج الأمان الحالية في الحوسبة السحابية؟
2. هل تتوافق الحوسبة السحابية مع تكامل أمن المعلومات؟
3. ما هي نقاط الضعف في نماذج سلامة البيانات الحالية؟
4. ما هي حلول نقاط الضعف المحددة؟
5. كيفية بناء مخطط يمكن أن يفرض تكامل البيانات في البيئة السحابية؟

5.1 أهمية البحث

تقترح هذا البحث نموذجًا للتوثق المستخدم وفحص تكامل البيانات. المستخدمين الاستعانة بمصادر خارجية البيانات إلى السحابة. لذلك، يحتاج مقدمو الخدمات السحابية إلى ضمان الحفاظ على سلامة البيانات ويمكنهم القيام بذلك من خلال فرض تقنيات توثق قوية للمستخدم.في هذا البحث سنقترح تقنيات أو نماذج يمكن أن تساعد موفري الخدمات السحابية على تقليل التهديدات الناتجة عن هجمات التوثق مثل الرجل في الهجوم المتوسط ، وبالتالي ضمان سلامة البيانات الموجودة في وحدات التخزين الخاصة بهم.

6.1 منهجية البحث

منهجية البحث هي عملية لإدارة وحل المشكلات البحثية بشكل منهجي. لتحقيق أهداف البحث، يتم استخدام الأساليب والتقنيات المختلفة التي تشمل: نبدأ بدراسة أحدث حالة من الأمن السحابية، والنظريات والتقنيات القائمة المتعلقة بمجال مشكلة البحث، ومن ثم يتم استخدام المنهج الاستنتاجي وسنقترح نموذجًا لذلك المنهج ثم تطوير تطبيق النموذج الأولي بحيث سيتم اتباع منهجية النموذج الأولي.

1.6.1 ادوات البحث

يستخدم هذا البحث تحليل المستندات والكتب ذات الصلة والمراقبة والمقابلات. تمت كتابة هذا البحث استنادًا إلى الأوراق العلمية والمصادر على الإنترنت والمجلات. للعثور على الأوراق ذات الصلة، بحثنا في الغالب عن قواعد البيانات التالية: IEEEXplore وGoogle Scholar وIEEE وScience-direct. بحثنا عن الكلمات الرئيسية "الحوسبة السحابية" و "أمان الحوسبة السحابية" و "تكامل البيانات في الحوسبة السحابية" و "الحوسبة السحابية لـ CIA" في العناوين أو الملخصات أو الكلمات الرئيسية للمقالات. ونستخدم برنامج Microsoft word لكتابة هذا البحث وبرامج LibreOffice Drawer للرسومات وللرسومات UML نستخدم Star-UML التي هي مفتوحة المصدر.ومن اللغات البرمجة سوف نستخدم SQL, PHP, HTML, CSS, JavaScript, و

المكتبات الاخري المستخدمة OpenSSL, سيتم نشر النموذج المطبق على منصة سحابة مفتوحة المصدر (GearHost).

7.1 حدود البحث

تركز هذا البحث على تحليل التقنيات المستخدمة للحفاظ على سلامة البيانات في بيئة الحوسبة السحابية من خلال تقديم نظرة عامة واسعة لبعض المخططات / النماذج الأساسية التي تعزز تكامل بيانات المستخدم. سنؤسس الحالة الراهنة لأحدث التقنيات لضمان صحة بيانات المستخدم المخزنة في البيئة السحابية. ستقترح هذا البحث أيضًا مخطط / نموذج فعال لتكامل البيانات في البيئة السحابية. لذلك ستحدد هذا البحث التحديات التي تواجه مخططات تكامل البيانات الموجودة في خوادم التخزين السحابية وتقترح لموفري السحابة تقنيات فعالة لضمان صحة بيانات المستخدم المخزنة في السحابة.
النطاق الزمني: سيتم إجراء هذا البحث من سبتمبر 2019 إلى مارس 2020.

8.1 مصطلحات البحث

1. الأمن.
2. الخصوصية.
3. الحوسبة السحابية
4. سحابة مقارنة الأمن
5. تكامل البيانات.
6. التوفر.
7. السرية.
8. الموثوقية.
9. توثق.
10. شهادة الرقمية.
11. توقيع الرقمية.

9.1 الدراسات السابقة

الدراسة الأولى: دراسة صفاء طاهر لولو[51]

أجرت صفاء بحثًا في عام 2016 حيث تم تطوير نموذج للكشف عن انتهاك سلامة الملفات المشتركة في السحابة، وكان الهدف العام من هذا البحث هو البحث "لبناء نموذج جديد يكشف عن انتهاك سلامة ملفات بين مشترك مجموعة من المستخدمين في السحابة. التي تستند إلى طريقة هاش ودعم عمليات البيانات الديناميكية (إلحاق البيانات وتحديثها وحذفها). "حيث كانت الأهداف المحددة هي طريقة لتنظيم العملية على الملف ، لوضع التغيير على الملف في ملف السجل ، استخدام خوارزمية تجزئة مناسبة وفعالة (SHA256) لتجزئة الملف قبل إرساله إلى السحابة ، لتحميل بعض الملفات إلى السحابة كمجموعة بيانات ، لتصميم موقع على شبكة الإنترنت سحابي يمثل نموذجنا ويدعم عمليات البيانات الديناميكية على الملفات لتنفيذ النموذج وإجراء التجارب في السحابة الخاصة بنا ، لتقييم أداء وكفاءة النموذج من حيث الدقة والتزامن. حيث تم توضيح مشكلة البحث على أنها "مع تزايد الاتجاه في الاستعانة بمصادر خارجية للبيانات للخوادم السحابية البعيدة مع إمكانية مشاركة الملفات، فإن معظم هذه الخوادم السحابية المجانية تتظاهر بأنها قد تحتفظ بالملفات المحفوظة بشكل آمن. ومع ذلك، لا يمكن ضمان أي شيء محفوظ على الإنترنت تمامًا. لذلك، فإن هذه الملفات المشتركة معرضة لمخاطر أمنية، ولا يمكن لأي شيء اكتشاف كيفية انتهاك سلامة الملفات على الخوادم السحابية المجانية، كما يمكن تهديد سلامة الملفات من المستخدمين الداخليين الذين يشاركون هذا الملف. لذا، فإن اكتشاف انتهاك سلامة الملفات المشتركة يؤكد أن المستخدمين يثقون في أن ملفاتهم في وضع آمن ولا يوجد أي تعديل غير قانوني عليها. "استخدم البحث منهجية النماذج الأولية التالية (الحصول على البيانات ، إعداد الملف ، إعداد الملف ، دعم تشغيل البيانات الديناميكية ، التطوير ملف سجل ، كشف انتهاك تكامل البيانات ، تقييم التزامن). تم إجراء تقييم دقة واكتشف أن نظامهم المقترح قادر على ضمان دقة الملفات واكتشاف كل نوع من تعديلات الملفات. بالإضافة إلى ذلك، تم إجراء تقييم التزامن على الملفات حيث وجدوا أن نظامهم كان قادرًا على تنظيم عمليات التزامن على الملف المشترك وتمكين مستخدم واحد فقط من تعديل الملف في نفس النقطة. في بحثنا، سوف نستخدم SHA3 لتجزئة الملفات.

الدراسة الثاني: دراسة مي منصور دهشان [14]

أجرى منصور بحثًا في عام 2013 حول أمن البيانات في التخزين السحابية حيث تم تطوير نموذج؛ كان الهدف من ذلك هو تصميم خدمة موثوقة لجهة خارجية تمكن المستخدمين من مشاركة البيانات عبر أي منصة تخزين سحابية قائمة على الويب مع الحفاظ على أمان البيانات. تحمي هذه الخدمة سرية البيانات المرسلة ويمكن استخدامها محليًا أو عن بُعد، وأيضًا لإنشاء مخطط "CP–ABE" متعدد السلطات جديد يحقق تحكمًا دقيقًا في الوصول، لاقتراح نهج إبطال فعال لل "CP" متعدد السلطات المقترح مخطط –ABE. تم تحديد نتيجة هذا البحث "نظام تخزين آمن يستخدم خدمة موثوق بها لجهة خارجية تمكن المستخدمين من مشاركة البيانات عبر أي منصة تخزين سحابية قائمة على الويب مع الحفاظ على أمان البيانات. تحمي هذه الخدمة سرية البيانات المرسلة ويمكن استخدامها محليًا أو عن بُعد. "بالإضافة إلى ذلك ، فقد قاموا بإنشاء نظام "CP–ABE" متعدد السلطات جديد يحقق التحكم في الوصول الدقيق. استنادًا إلى السلطة المتعددة، يدعم النموذج العديد من القراءة والكتابة للمستخدمين (وهذا يعني أنه بعد قيام المالك بإنشاء ملف مشفر واحد على خادم التخزين، يمكن للمستخدمين الآخرين ذوي السمات المناسبة أيضًا تحديث الملف المشفر في وقت لاحق دون أي المساعدة من مالكي الملفات الأصلية) بدلاً من قراءة واحدة للكثير .من خلال استخدام"CP–ABE"متعدد السلطات، نأخذ خطوة على معظم الأعمال الحالية التي تعتمد على سلطة واحدة "CP–ABE" لإصدار مفاتيح الوصول الخاصة. علاوة على ذلك،لا تعتبر أنظمة التخزين السحابية القائمة على "CP–ABE" متعددة السلطات القائمة جميعها تأمين سلامة بيانات الاستعانة بمصادر خارجية، على عكس مخططنا الذي يدعم التحقق من سلامة البيانات. علاوة على ذلك، نحن ندعم العديد من عمليات القراءة والكتابة للمستخدمين التي تفتقر إليها جميع الأنظمة التي تدعم أنظمة"CP–ABE"متعددة السلطات. اقترحوا نهجًا فعالًا لإلغاء نظام "CP–ABE"متعدد السلطات المقترح، حيث أدركوا بشكل فعال الإلغاء الفوري لمستوى المستخدم / السمة مع تحقيق كل من السرية الخلفية. بالإضافة إلى ذلك، فوضوا حق إعادة التشفير إلى خوادم البروكسي السحابية للاستفادة من الموارد السحابية الوفيرة. نحن نستفيد من الأنظمة التي تدعم إما لا تدعم الإلغاء في "CP–ABE"متعدد الصلاحيات أو تدعم إما إبطال المستخدم أو السمة وليس كليهما. "في بحثنا ، سوف نستخدم التوثق المستندة إلى الشهادة للتوثق المستخدم لتحسين نموذجنا.

الدراسة الثالث: دراسة موروفات كاتانوش[52]

تم إجراء بحث في عام 2015 بواسطة كاتانوش حول التحقق من سلامة البيانات في السحابة، وكان الهدف من هذا البحث هو معالجة مشكلة التحقق من سلامة البيانات في الحوسبة السحابية وأيضًا تحديد عناصر البيانات التي من المحتمل أن تُسرق كبيانات حساسة ومحاولة للحفاظ عليها في مأمن من أي تحديثات غير مصرح بها. في الختام، قدموا نموذج أمان جديد للتحقق من سلامة البيانات لقاعدة بيانات الاستعانة بمصادر خارجية. تحدد هذه الطريقة بعض بيانات التحكم للتعرف على تحديثات البيانات في حالة قيام مستخدم غير مصرح له بتغيير البيانات. لتحقيق وقت استجابة أسرع للاستعلام، يقومون بتخزين البيانات الحقيقية في قاعدة بيانات علائقية كنص عادي على خادم بعيد. من أجل التحقق من تكامل البيانات الحقيقية المدمجة، فإنها تنشئ بيانات وصفية (يتم الاحتفاظ بها كنص مشفر) وجدول يخزّن معلومات حول جميع عناصر البيانات الحساسة كنص عادي. باستخدام المحاكاة، أثبتوا أن طريقة عملهم فعالة حيث أنه عند زيادة عدد الأقسام، يكون هناك انخفاض في وقت المعالجة. في بحثنا، نستفيد من استخدام خوارزمية هاش الآمنة وتشفير قيمة هاش لمنع الهجمات على قيمة هاش.

الدراسة الرابع: دراسة أنانتوار وآخرون[48]

تم إجراء بحث في عام 2015 بواسطة أنانتوار وآخرون اقترح حماية ثلاثية الطبقات للحفاظ على تكامل البيانات في السحابة، الطبقة 1: توثق المستخدم، الطبقة 2: تشفير بيانات المستخدم، الطبقة 3: استعادة بيانات المستخدم، أطلقوا هذا الدفاع الأول والثاني والثالث، واستخدموا خوارزمية "3DES" ل تشفير البيانات وخوارزمية SHA1 لتكامل البيانات والأمن متعدد المستويات لتأمين البيانات. مشكلة البحث، أولاً "المشكلة هي بناء الثقة في التنفيذ عن بُعد. بشكل أساسي، السحابة عبارة عن بنية حسابية موزعة يعمل فيها حساب العميل على مضيف بعيد في مركز بيانات. في النظام السحابية، يجب أن يحصل العميل على تأكيد بأن النظام الأساسي يقوم بتنفيذ مثيله السحابية مع حماية سلامته وسريته، وهو بمثابة التشغيل على جهاز العميل نفسه. "ثانياً ،" المشكلة الثانية هي حماية تنفيذ سحابة واحدة مثيل من مثيلات أخرى على نفس النظام الأساسي أو البنية الأساسية. مرة أخرى، يجب أن يقوم النظام الأساسي بتطبيق هذا المطلب. الأنظمة الأساسية والخدمات السحابية هي موارد مشتركة يمكن لأي عميل سحابة الاستفادة منها، لذلك يجب عليه ضمان العزلة أثناء التفاعلات مع العملاء.

"ثالثًا ،" المشكلة الثالثة هي حماية تنفيذ مثيل سحابة من الخصوم الخارجيين. غالبًا ما يحتاج المثيل السحابية إلى الوصول إلى الشبكة للتواصل مع العميل والتفاعل مع التخزين. في كلتا الحالتين، يمكن للهندسة السحابية تبسيط الإدارة لأن النظام الأساسي يعرف موقع كل من التخزين والعميل "

الدراسة الخامس: دراسة سلطان الدوسري وآخرون[2]

تم إجراء بحث في عام 2016 من قبل الدوسري وآخرون حول أمان البيانات والخصوصية والتوافر وتكامل البيانات في الحوسبة السحابية: المشكلات والحلول الحالية، حيث عرضنا المشكلات التي تمنع الناس من تبني السحابة وتعطي استبيانًا عن الحلول التي تم القيام بها لتقليل مخاطر السحابة قضايا الأمن. في الختام، وجدوا أن هناك العديد من مشكلات الأمان التي تؤثر على الحوسبة السحابية، وتشمل هذه المشكلات القضايا المتعلقة بالإصدارات السابقة للإنترنت، ومشكلات الشبكة، ومشكلات التطبيق، ومشكلات التخزين، وأيضًا أن تخزين البيانات على الخوادم البعيدة قد يؤدي إلى مشكلات تتعلق بالسرية، قضايا فشل تكامل البيانات والتوافر. وذُكرت أيضًا بعض التقنيات لحماية البيانات في السحابة مثل استخدام "Provable Data Possession"، ومراجع الطرف الثالث، وإثبات الاسترجاع، وإثبات الملكية. يرتبط هذا البحث بأبحاثنا، حيث أننا سنقوم بدراسة الحلول الأمنية السحابية الحالية مثل تلك التي قاموا بها. سوف نستخدم هذا البحث لفهم المزيد حول قضايا الأمن السحابية.

الدراسة السادس: دراسة جوزيني اتينيز وآخرون[43]

اقترحت دراسة أجراها جوزيني اتينيز وآخرون اقتراحًا لامتلاك البيانات في متاجر غير موثوق بها، وهو النموذج الذي يسمح للعميل الذي قام بتخزين البيانات في خادم غير موثوق به بالتحقق من أن الخادم لديه البيانات الأصلية دون استعادتها، ويولد النموذج أدلة إثباتية الحيازة عن طريق أخذ عينات عشوائية من الكتل من الخادم، مما يقلل بشكل كبير من تكاليف الإدخال / الإخراج. لقد استفدنا من هذا البحث من خلال البحث عن طرق لتحسين نموذجنا لتقليل قوة الحساب.

10.1 هيكل البحث

سنقسم هذا البحث إلى ستة فصول،

الفصل (1) مقدمة: والذي سيتضمن مقترح البحث.

الفصل (2) الاطار النظري: في هذا الفصل سنناقش نظرة عامة على الحوسبة السحابية، كما سنناقش نظرة عامة على الأمن في الحوسبة السحابية.

الفصل (3) التحليل : يعرض تحليل لنموذج المقرح وا.

الفصل (4) المنهجية: التحليل، التصميم سوف نقدم نموذجًا للحفاظ على سلامة البيانات في السحابة مع بنيتها المعمارية والوظائف الرئيسية وأساسيات النموذج. ثم التنفيذ.

الفصل (5) التجربة والتقييم: تجربة نظام ، وتقييم وتحليل النتائج التجريبية.

الفصل (6) النتائج,التوصية والخاتمة: نقدم النتائج و المناقشات النتائج والتوصيات والأعمال المستقبلية.

الفصل الثانـي

الإطار النظري

2. مقدمة.

سيتم تقسيم هذا الفصل إلى قسمين، أولاً سنقوم باستعراض الحوسبة السحابية التي تتضمن التعريف والخصائص ونماذج التسليم ونماذج النشر والفوائد والمخاطر والعقبات التي تحول دون اعتماد الحوسبة السحابية، العوامل التي تؤثر على الأداء، وبنية الحوسبة السحابية المرجعية. ثانياً، سوف نعرض نظرة عامة على الأمان في الحوسبة السحابية، ومشكلات التهديدات الأمنية السحابية، وأهداف ومتطلبات الأمان، تكامل البيانات في السحابة، والحل لمشاكل الامنية السحابية الحالي. مبادئ خدمات التخزين السحابية، والواجهات المستخدمة لخدمات التخزين السحابية والتحسين في خدمات التخزين السحابية.

1.2 نظرة عامة للحوسبة السحابية

1.1.2 الحوسبة السحابية.

الحوسبة السحابية تحصل على اسمها كاستعارة للإنترنت. اسم الحوسبة السحابية يترجم بالحوسبة في السحابة ولكنه يعني الإنترنت أو مجموعة كبيرة من الخوادم المتصلة مع بعض. من بين العديد من التعريفات، تُعرّف "NIST–National Institute Of Science And Technology" الحوسبة السحابية بأنها "نموذج لتمكين الوصول في كل مكان وشبكة مريحة عند الطلب إلى مجموعة مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وصدر مع الحد الأدنى من جهد الإدارة أو تفاعل مزود الخدمة. [1]. تعريف أخرى على الحوسبة السحابية "على أنها استخدام تكنولوجيا الكمبيوتر التي تسخر قوة المعالجة للعديد من أجهزة الكمبيوتر المتشابكة مع إخفاء الهيكل الذي يقف وراءها". [15] من خلال جمع هذه التعريفات ، نعلم أن الحوسبة السحابية تعمل على تخفيف التنظيم من ضغوط القوى العاملة للأجهزة ، والمهندسين لإدارة مراكز البيانات وقضايا الصيانة الشاملة والأسعار لإدارة مراكز البيانات ، كما أنها توفر منصة سريعة للمطورين حيث لا يتعين عليهم القلق بشأن التحديثات وعناصر التحكم في الإصدار ، يمكن اعتبار الحوسبة السحابية حل للمشكلات التنظيمية التقنية والاقتصادية.

لفهم تعاريف الحوسبة السحابية بشكل أفضل، يتميز نموذج السحابة بخمس خصائص أساسية [1]، [14]. هذه الخصائص الخمس هي:

1) **الخدمة الذاتية عند الطلب:** يمتلك المستهلك إمكانيات الحوسبة من جانب واحد ، مثل وقت الخادم وتخزين الشبكة ، حسب الحاجة تلقائيًا دون الحاجة إلى تفاعل بشري مع كل مزود خدمة. تعد مصادر الخدمة الذاتية عند الطلب سمة أساسية في معظم العروض السحابية حيث يمكن للمستخدم توسيع نطاق البنية التحتية المطلوبة كما يحلو له دون إزعاج المضيف.

2) **الوصول إلى شبكة واسعة**: تتوفر الإمكانيات عبر الشبكة ويتم الوصول إليها من خلال الآليات القياسية التي تشجع على استخدام المنصات العميلة الرفيعة أو السميكة غير المتجانسة (مثل الهواتف المحمولة والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة ومحطات العمل). طرح نماذج جديدة مثل الحوسبة السحابية المتنقلة التي تعزز الحوسبة المتنقلة من خلال الاستفادة من الخدمات السحابية.

3) **تجميع الموارد:** يتم تجميع موارد الحوسبة الخاصة بالمزود لخدمة عدة مستهلكين باستخدام نموذج متعدد المستأجرين ، مع تخصيص الموارد المادية والافتراضية المختلفة ديناميكيًا وإعادة تعيينها وفقًا لطلب العميل. هناك حالة عامة لاستقلال الموقع لأن العملاء لا يعرفون الموقع الدقيق للمكان الذي ستأتي منه الخدمة.

4) **المرونة الزائدة:** يمكن توفير القدرات وإفراجها بشكل مرن ، في بعض الحالات تلقائيًا ، لتوسيع نطاقها بسرعة إلى الداخل وبما يتناسب مع الطلب. بالنسبة للمستهلك، غالبًا ما تبدو الإمكانيات المتاحة للتزويد غير محدودة ويمكن تخصيصها بأي كمية في أي وقت.

5) **الخدمة المقاسة:** تتحكم الأنظمة السحابية تلقائيًا في استخدام الموارد وتحسينها من خلال الاستفادة من قدرة القياس عند مستوى معين من التجريد المناسب لنوع الخدمة (مثل التخزين والمعالجة وعرض النطاق الترددي وحسابات المستخدمين النشطة). يمكن مراقبة استخدام الموارد والتحكم فيه والإبلاغ عنها، مما يوفر الشفافية لكل من مزود الخدمة المستهلكة والمستهلك [1]، [14].

2.1.2 نماذج التسليم السحابية

تقديم الخدمات السحابية للمستهلكين يعني ما هي الخدمات المتاحة للمستهلكين للتفاعل معها، وهناك العديد من النماذج المستخدمة في الحوسبة السحابية والمصطلحات الجديدة تستمر في الظهور بسبب التطورات في احتياجات العملاء البحثية المتزايدة، ومن بين هذه النماذج الثلاثة النموذج الرئيسي: البنية التحتية كخدمة، والنظام الأساسي كخدمة، والبرمجيات كخدمة [1]، [12]، [16]، [17]. هناك

نماذج تسليم أخرى مثل قاعدة البيانات كخدمة، التخزين كخدمة، تكنولوجيا المعلومات كخدمة، الأمن كخدمة، الشبكة كخدمة، الاختبار كخدمة، الروبوتات كخدمة، كل شيء كخدمة.

1. **البنية التحتية كخدمة:** "IaaS-Infrastructure as a Service"يتم تقديم أجهزة الكمبيوتر (الخوادم وتكنولوجيا الشبكات والتخزين ومساحة مركز البيانات) كخدمة. قد يشمل أيضًا تسليم أنظمة التشغيل وتقنية المحاكاة الافتراضية لإدارة الموارد [17]. من أمثلة خدمات "" Amazon" :"IaaS EC2 و Windows Azure"" و Rackspace و Google Compute Engine.تشمل خصائص ""IaaS

أ- عدة مستخدمين على قطعة واحدة من الأجهزة.

ب- الموارد المتاحة كخدمة.

ت- قدرات القياس الديناميكية -تختلف التكلفة بناءً على اختيار البنية التحتية.

يعد IaaS مناسبًا للمؤسسات التي تحتاج إلى تحكم كامل في برامجها، على سبيل المثال، للتطبيقات عالية الأداء. يعتبر IaaS مناسبًا أيضًا للشركات الصغيرة التي لا ترغب في إنفاق المال والوقت في شراء الأجهزة والبرامج والخدمات التي تواجه مطالب متقلبة مثل زيادة معدل الاتجار وانخفاضه [12].

2. **المنصة كخدمة:** "PaaS-Plateform as a service"تشمل تقديم أكثر من مجرد بنية تحتية. إنها توفر ما يمكن أن تسميه حزمة حلول -مجموعة متكاملة من البرامج التي توفر كل ما يحتاجه المطور لإنشاء تطبيق -لكلا من تطوير البرامج ووقت التشغيل [17]. أمثلة على "PaaS" هي "Beanstalk" "AWS Elastic" و"Windows Azure" و""Heroku،"Force.com" ، "Google App Engine"، "Apache Stratos". تشمل خصائص "[12] "PaaS،[14]

أ- تقنية افتراضية تمكن هذه المنصة.

ب- خدمات تطوير وتنفيذ التطبيقات المختلفة لتيسير تطوير تطبيقات البرمجيات واختبارها ونشرها واستضافتها في بيئة تطوير متكاملة.

ت- مشاركة نفس بيئة التطوير من قبل مستخدمين متعددين. خدمات الويب المتكاملة وقواعد البيانات.

ث- الفواتير والاشتراكات التي تديرها أدوات الحوسبة السحابية. يعد PaaS مناسبًا [12]، [14]: مطورين متعددين يعملون على تطوير نفس المنتج، يوقف PaaS الصعوبات المرتبطة بالتطور السريع وتكرار تطبيق ما بحيث يكون مناسبًا للمؤسسات التي تتبع منهجية Agile لتطوير البرامج، PaaS مناسب أيضًا للمؤسسات التي ترغب في خفض ميزانيتها على الإنفاق على البنية التحتية للحوسبة بالإضافة إلى تطوير التطبيقات وتنفيذها.

3. **البرمجيات كخدمة** : "SaaS-Software as a service"هي تقديم تطبيقات الأعمال المصممة لغرض محدد.[17] أمثلة على البرمجيات كخدمة هي ""Google Apps"،"box" ، "Microsoft Office 365"،"Amazon Web Services" "و "Dropbox". يوضح الشكل 1.2 نماذج التسليم السحابية أكثر.

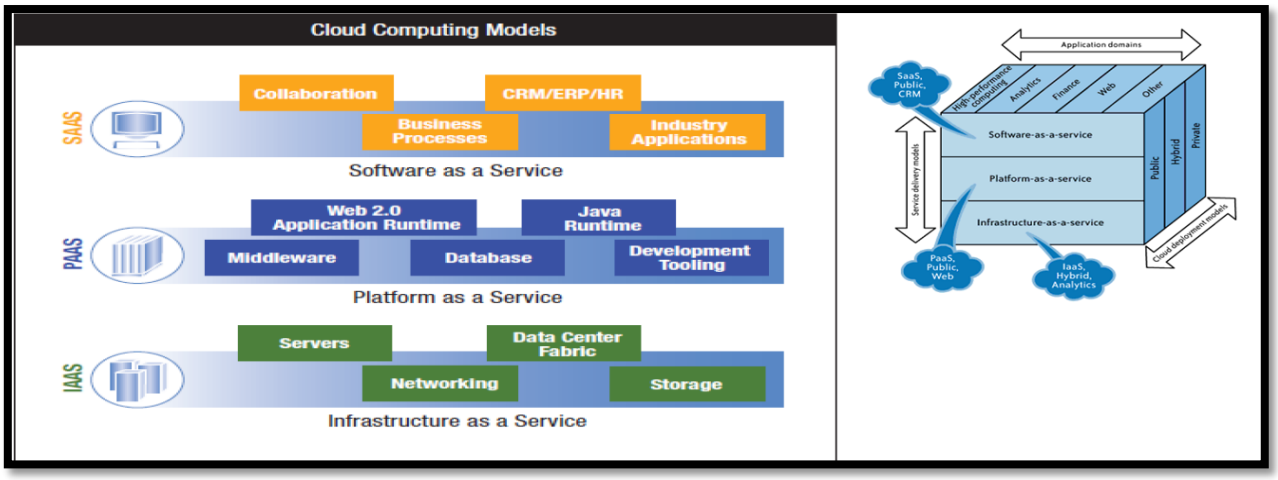
تشمل خصائصSaaS [14،12] :

أ- البرامج المستضعفة على خادم بعيد، ويمكن الوصول إليها دائمًا من خلال متصفح الويب أو تطبيق الهاتف المحمول عبر الإنترنت.

ب- التطبيق المدار من موقع مركزي.

ت- لا يحتاج مستخدمو التطبيق إلى القلق بشأن الأجهزة أو البرامج (التحديثات، والتصحيحات، وما إلى ذلك)

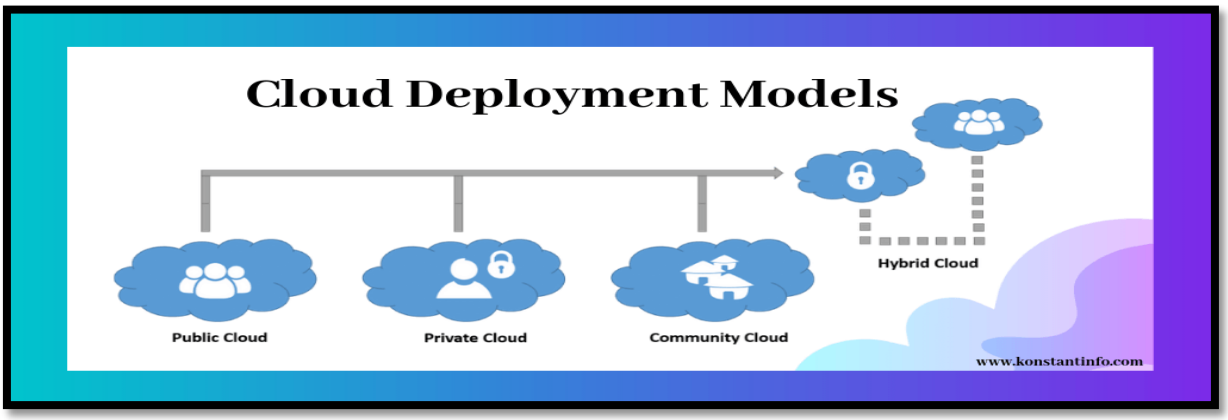
ث- يتم أي تكامل مع تطبيقات الطرف الثالث من خلال واجهات برمجة التطبيقات. [12]، [14] "SaaS" مناسبة لـ: التطبيقات التي ترتفع أو تنخفض فيها المطالب بشكل كبير. على سبيل المثال، حجز تذاكر الطيران مرتفع خلال العطلات الطويلة. "SaaS" مناسب أيضًا للتطبيقات التي تتطلب وصولاً متعددًا مثل الويب والجوال. [12] تعد "SaaS" مناسبة أيضًا للشركات الناشئة أو الشركات الجديدة التي ترغب في إطلاق خدماتها أثناء التنقل مثل التجارة الإلكترونية. تعد "SaaS" أيضًا مناسبة لشركات البرمجيات التي ترغب في زيادة التحكم في استخدام برامجها عن طريق الحد من النسخة أو المصدر. تعد "SaaS" مناسبة أيضًا للشركات الناشئة أو الشركات الصغيرة التي لا يمكنها تحمل تكلفة ترخيص البرامج وإدارة الأجهزة والموارد الأخرى اللازمة لاستضافة التطبيق محليًا [١٤.١٢]. يوضح الشكل 1.2 التسلسل الهرمي لنماذج التسليم السحابية وخدماتها.



الشكل (1.2) التسلسل الهرمي لنماذج التسليم سحابة وخدماتها

3.1.2 نماذج نشر السحابة

النشر في السحابة يعني مكان توفر الخدمة، وبمعنى آخر حيث يتم تشغيله، يتكون نموذج السحابة من أربعة نماذج للنشر تختلف اختلافًا كبيرًا: العامة والخاصة والهجينة والمجتمعية [1].



الشكل (2.2) نماذج نشر السحابة

كما هو مبين في الشكل 2.2 أعلاه. يعتمد اختيارك لنموذج النشر على مخاوفك المتعلقة بأمان البيانات واحتياجات مؤسستك.

1. **السحابة العامة:** كما يقال السحابة العامة، تكون السحابة متاحة لعامة الناس ويتم إنشاء البيانات وتخزينها في خادم الجزء الثالث. تنتمي البنية التحتية للخوادم إلى مزودي الخدمة الذين يديرونها ويديرون موارد التجمع [19]. يقوم الطرف الثالث بتأجيرها إلى مؤسسة أو شركات مدفوعة الأجر حسب رغبتك أو حتى مجانًا في بعض الأحيان. يُعرّف"NIST" [1] السحابة

العامة بأنها "البنية التحتية السحابية المتوفرة للاستخدام المفتوح من قبل الجمهور العام. قد تكون مملوكة أو مُدارة من قبل مؤسسة أعمال أو أكاديمية أو حكومية أو مزيج من هذه المؤسسات. إنه موجود في مقر المزود السحابية ". يوضح الجدول 2.1 إيجابيات وسلبيات السحابة العامة [14]، [18]، [19].

الجدول (1.2) –إيجابيات وسلبيات سحابة العامة

سلبيات	إيجابيات
1.أمن البيانات والخصوصية	1. سهلة الإعداد والاستخدام
2.الموثوقية للخطر	2. سهولة الوصول إلى البيانات
3.عدم التوفير	3. المرونة لإضافة وتقليل القدرات
	4. الفعالية من حيث التكلفة وقابلية الدفع حسب الاستخدام وقابلية التوسع العالية.
	5. القضاء على الحاجة للبرنامج

2. **السحابة الخاصة:** من الناحية الفنية، لا يوجد فرق كبير بين السحابة العامة والخاصة باستثناء أن السحابة العامة تدار من قبل طرف ثالث بينما في السحابة الخاصة، تكون البنية التحتية السحابية مخصصة لمؤسسة واحدة فقط. يتم الاحتفاظ بالموارد داخل المؤسسة من قِبل منظمة ما، أو يتم تخصيصها حصريًا للمؤسسة من قِبل موفر سحابة في مقرها [19]. بالإضافة إلى ذلك، تُعرّف [1] "NIST–National Institutu of Standards and Technology" السحابة الخاصة بأنها "البنية التحتية السحابية متوفرة للاستخدام الحصري من قبل مؤسسة واحدة تضم عدة مستهلكين (على سبيل المثال، وحدات الأعمال). قد تملكها وتديرها المنظمة ". يوضح الجدول 2–2 إيجابيات وسلبيات السحابة الخاصة [14]، [18]، [19].

الجدول (2.2) –مزايا وسلبيات سحابة العامة

سلبيات	إيجابيات
1. غالية	1. موثوقية عالية لأن جميع المعدات في أماكن العمل

2. صيانة إضافية	2. مستوى عال من الخصوصية والأمن للبيانات.
3. أكثر صعوبة للوصول إلى البيانات من المواقع النائية بسبب زيادة التدابير الأمنية.	3. المرونة لإضافة وتقليل القدرات.
	4. الأداء مرتفع جدا
	5. المرونة والكثير من السيطرة

3. **السحابة المجتمع:** سحابة المجتمع تشبه السحابة الخاصة باستثناء أن البنية التحتية السحابية مخصصة للاستخدام الحصري من قبل مجتمع معين من المستخدمين من منظمتين أو أكثر تشترك في المصالح المشتركة [19]. بالإضافة إلى ذلك، تُعرّف"NIST" سحابة المجتمع بأنها "يتم توفير البنية التحتية السحابية للاستخدام الحصري من قبل مجتمع محدد من المستهلكين من المنظمات التي لها اهتمامات مشتركة (مثل المهمة ومتطلبات الأمان والسياسات واعتبارات الامتثال). قد تكون مملوكة أو تديرها واحدة أو أكثر من المنظمات في المجتمع أو طرف ثالث أو مزيج منها، وقد تكون موجودة في أماكن العمل أو خارجها ". يوضح الجدول 2.3 إيجابيات وسلبيات السحابة الخاصة [14,1، 18,19].

الجدول (3.2) –إيجابيات وسلبيات سحابة المجتمع

سلبيات	إيجابيات
1. تكلفة أعلى من السحابة العامة	1. خفض التكلفة
2. تقاسم سعة التخزين الثابتة وعرض النطاق الترددي.	2. تحسين الأمن والخصوصية والموثوقية
3. ليست واسعة الانتشار حتى الآن	3. سهولة تبادل البيانات والتعاون
	4. الأداء مرتفع جدا

4. **السحابة الهجينة:** السحابة المختلطة هي مزيج من السحابة العامة والخاصة والسحابة المجتمعية الموجودة في شكلها ولكنها مرتبطة ببعضها البعض بمعيار يتيح إمكانية نقل البيانات والتطبيق (على سبيل المثال، انفجار السحب من أجل موازنة التحميل بين السحب) [18]. بالإضافة إلى ذلك، تُعرّف"NIST" السحابة المختلطة بأنها "البنية التحتية السحابية عبارة عن تركيبة من اثنين أو أكثر من البنى التحتية السحابية المميزة (الخاصة أو المجتمعية أو العامة) التي لا تزال كيانات فريدة من نوعها، ولكنها مرتبطة ببعضها البعض بواسطة تقنية قياسية أو خاصة تمكن البيانات وقابلية التطبيق (على سبيل المثال، انفجار السحاب من أجل موازنة التحميل بين السحب) ". يوضح الجدول 2.4 إيجابيات وسلبيات السحابة الخاصة [14]، [18]، [19].

الجدول (4.2) –إيجابيات وسلبيات السحابة الهجينة

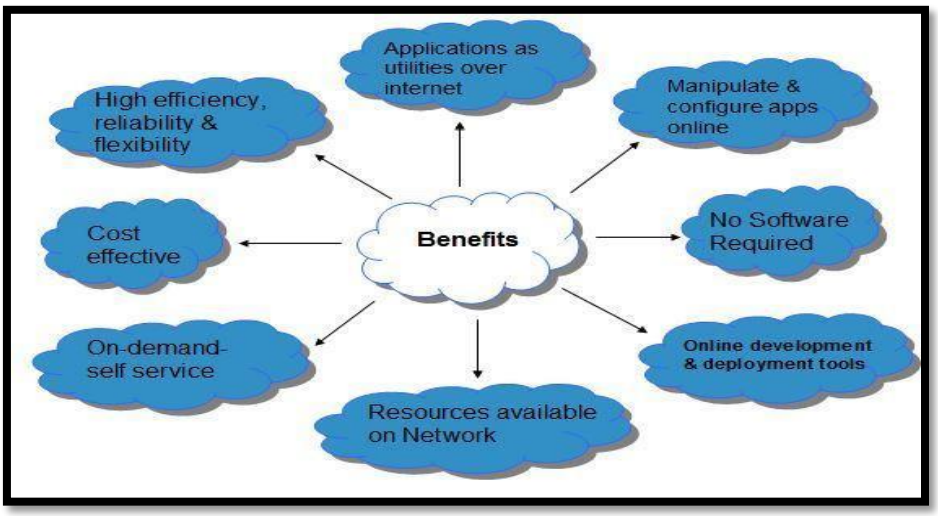
سلبيات	إيجابيات
1. يتطلب خبرة تكنولوجيا المعلومات	1. تحسين الأمن والخصوصية
2. البيانات تحتاج إلى تقسيم	2. تعزيز التدرجية والمرونة
	3. سعر معقول

4.1.2 فوائد الحوسبة السحابية

تمتلك الحوسبة السحابية العديد من المزايا [20]، [21] من بين هذه الفوائد:

1. يمكن الوصول إلى التطبيقات كأدوات مساعدة، عبر الإنترنت.
2. معالجة وتكوين التطبيق عبر الإنترنت في أي وقت.
3. توفر الحوسبة السحابية أدوات تطوير ونشر عبر الإنترنت، وبرمجة بيئة وقت التشغيل من خلال النظام الأساسي كنموذج خدمة.
4. تتوفر الموارد السحابية عبر الشبكة بطريقة توفر وصولاً مستقلاً للنظام الأساسي إلى أي نوع من العملاء.
5. الحوسبة السحابية تقدم الخدمة الذاتية عند الطلب. يمكن استخدام الموارد دون تفاعل مع مزود الخدمة السحابية.

6. الحوسبة السحابية فعالة من حيث التكلفة للغاية لأنها تعمل بكفاءات أعلى مع استخدام أكبر.
7. توفر الحوسبة السحابية موازنة تحميل تجعلها أكثر موثوقية كما هو موضح في الشكل 3.2.



الشكل (3.2) فوائد الحوسبة السحابية

5.1.2 مخاطر وتحديات الحوسبة السحابية.

1. **الأمان والخصوصية:** يعد أمان البيانات والخصوصية عنصرا حاسما يستدعي التدقيق. الشركات مترددة في شراء ضمان لأمان بيانات العمل من البائعين. انهم يخشون فقدان البيانات للمنافسة وأمن البيانات. الأمن والخصوصية هو أكبر قلق بشأن الحوسبة السحابية. نظرًا لأن إدارة البيانات وإدارة البنية التحتية في السحابة مقدمة من طرف ثالث، فمن المخاطرة دائمًا تسليم المعلومات الحساسة لمقدمي الخدمات هؤلاء. على الرغم من أن بائعي الحوسبة السحابية يضمنون حسابات أكثر أمانًا محمية بكلمة مرور، فإن أي علامة على خرق الأمان قد تؤدي إلى فقدان العملاء والشركات.
2. **عمليات التأمين:** من الصعب للغاية على العملاء التبديل من مزود خدمة Cloud (CSP) إلى آخر. ينتج عنه اعتماد على CSP معين للخدمة. قد يكون توفر بيانات العميل في خطر إذا تعطل أحد موفري الخدمات السحابية أو حصلت عليه مؤسسة أخرى. يجب أن يوضح مقدمو خدمة العملاء الإجراءات للعملاء لاسترداد بياناتهم عند الحاجة، ويوصى باستخدام المعايير المفتوحة من قبل مقدمي الخدمة لمنع قفل البيانات.

3. **فشل العزل:** ينطوي هذا الخطر على فشل آلية العزل التي تفصل التخزين والذاكرة والتوجيه بين المستأجرين المختلفين.
4. **الحذف غير آمن وغير مكتملة:** من الممكن ألا يتم حذف البيانات عند طلب للحذف. يحدث ذلك إما بسبب تخزين نسخ إضافية من البيانات ولكنها غير متوفرة أو إتلاف القرص أيضًا بتخزين البيانات من مستأجرين آخرين.
5. **القيود التنظيمية والامتثال:** في بعض البلدان، لا تسمح اللوائح الحكومية بتحديد معلومات العميل الشخصية والمعلومات الحساسة الأخرى فعليًا خارج الدولة أو البلد. من أجل تلبية هذه المتطلبات، يحتاج مقدمو الخدمات السحابية إلى إعداد مركز بيانات أو موقع تخزين خاص داخل الدولة للامتثال للوائح. قد لا يكون وجود بنية تحتية كهذه أمرًا ممكنًا دائمًا ويشكل تحديًا كبيرًا لموفري الخدمات السحابية.

6.1.2 العوامل المؤثرة في أداء السحابة

هناك العديد من العوامل التي تؤثر على أداء الحوسبة السحابية من بين هذه العوامل[12]:

1. عرض النطاق الترددي للشبكة: نظرًا لأن السحابة عبارة عن خدمة يتم توفيرها عبر الإنترنت، فعندما يكون عرض النطاق الترددي منخفضًا لتوفير خدمة مطلوبة في الوقت المطلوب، فسيؤدي ذلك إلى انخفاض في أدائها.
2. عدد المستخدمين: عندما يتجاوز عدد المستخدمين السعة السحابية، فقد يؤثر ذلك على أداء الخدمة المقدمة.
3. استعادة البيانات: تؤثر القدرة والوقت اللازمان لاسترداد الملفات على الأداء حيث يمكن فقد البيانات أو تعرضها للفشل وهذا يؤثر على الأداء.
4. خطأ التسامح: نظام التسامح عالي سيؤدي إلى أداء عالي.
5. عوامل أخرى: تشمل العوامل الأخرى التي يمكن أن تؤثر على أداء السحابة مشاكل قابلية التوسع والكمون والتكرار وعبء العمل وطاقة المعالج. [12]

7.1.2 هندسة الحوسبة السحابية المرجعية

وفقًا للتقرير الخاص بخريطة طريق الحوسبة السحابية من"NIST" [22]: "تعد البنية المرجعية للحوسبة السحابية "NIST" نموذجًا عامًا مفاهيمي عالي المستوى يمثل أداة قوية لمناقشة متطلبات وهياكل وعمليات الحوسبة السحابية. لا يرتبط النموذج بأي من منتجات أو خدمات أو موردي خدمات البائعين المعينة، كما أنه لا يحدد الحلول الإرشادية التي تمنع الابتكار. وهي تحدد مجموعة من العناصر الفاعلة والأنشطة والوظائف التي يمكن استخدامها في عملية تطوير أبنية الحوسبة السحابية، وتتعلق بتصنيف الحوسبة السحابية المصاحبة. يحتوي على مجموعة من المشاهدات والأوصاف التي تشكل أساسًا لمناقشة خصائص واستخدامات ومعايير الحوسبة السحابية ". إنها أداة لوصف ومناقشة وتطوير البنية الخاصة بالنظام باستخدام إطار مرجعي مشترك.

تحدد بنية مرجع الحوسبة السحابية "NIST" خمسة ممثلين رئيسيين [22] والذين لديهم أدوار رئيسية في بنية الحوسبة السحابية، يشارك كل منهم في معاملة أو عملية و / أو يؤدي مهام في الحوسبة السحابية:

1. **المستهلك السحابية:** هو فرد يستخدم خدمات الحوسبة السحابية، ويمكنه التعامل في أشكال كثيرة مع نماذج تسليم الحوسبة السحابية مثل SaaS وPaaS وIaaS للاستمتاع بعروض سحابة مختلفة مثل المبيعات والفوترة والتخزين ونشر التطبيق قاعدة البيانات بين الكثير.
2. **الموفر السحابية:** الموفر السحابية هو كيان أو شخص مسؤول عن إتاحة الخدمة للمستهلكين السحابيين. يقوم مزودو الخدمات السحابية بإدارة كل الجوانب الفنية للنظام وتأجيره للعميل بناءً على اتفاقية معينة. المسؤوليات إذا كان الموفر السحابية يعتمد على نوع نموذج التسليم.
3. **المدقق السحابية:** هي هيئة مستقلة تقوم بتقييم الخدمات السحابية وعمليات نظام المعلومات والأداء والأمن والخصوصية لتنفيذ الحوسبة السحابية والالتزام باتفاقية الخدمة. هناك حاجة لهذه الهيئة المستقلة لأن المستهلك السحابية لا يمكنه الوثوق الكامل بموفر السحابة والعكس صحيح.
4. **الوسيط السحابين:** تُعرّف NIST Reference Architecture،SP 500-292 وسيط Cloud على أنه كيان يدير استخدام الخدمات السحابية وأدائها وتسليمها، ويتفاوض على العلاقات بين موفري السحابية والمستهلكين. مع نمو الحوسبة السحابية، قد يصبح الأمر معقدًا

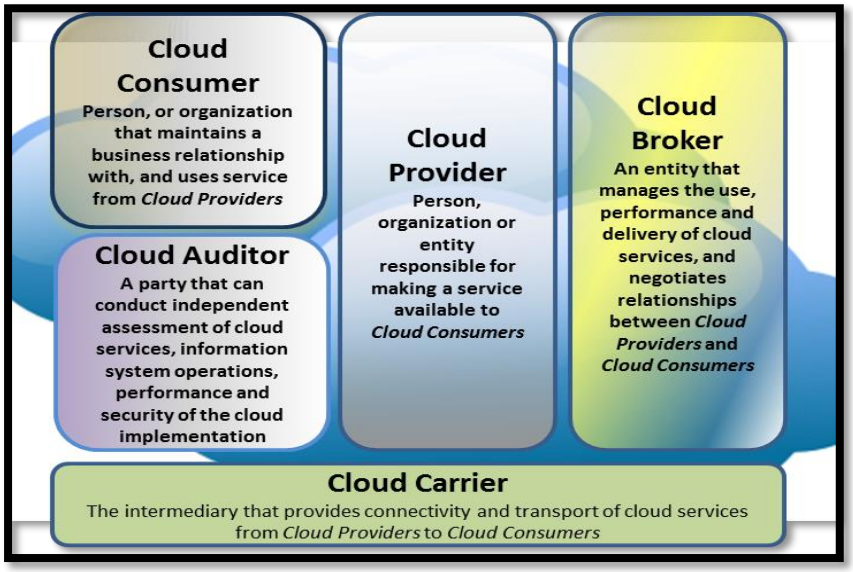
للغاية بحيث يتعذر على المستهلكين إدارته، لذلك هناك حاجة إلى وسيط لإدارة هذه الخدمات. يوفر الوسيط السحابين الخدمات في ثلاث فئات وهي:

أ- تعني الوساطة أن الوسيط يعزز أو يحسن خدمات معينة مثل إدارة الوصول إلى الخدمات السحابية، وإدارة الهوية، وإعداد تقارير الأداء، والأمن المحسن، إلخ.

ب- التجميع يعني الجمع بين خدمات متعددة ودمجها في خدمة جديدة أو أكثر.

ت- التحكيم يعني هذا أن لدى الوسيط المرونة في اختيار الخدمات من مزودي خدمة متعددين. يمكن للوسيط السحابية أيضًا تقديم خدمة الدعم الفني [22].

5. **ناقلون سحابة:** يعمل كوسيط يوفر الاتصال ونقل الخدمات السحابية بين مستهلكي السحابة وموفري الخدمات السحابية. توفر شركات الاتصالات السحابية الوصول إلى المستهلكين من خلال الشبكات والاتصالات والكهرباء وأجهزة الوصول الأخرى. سحابة يحمل معظمها شركات الاتصالات السلكية واللاسلكية. يوضح الشكل 4.2 الجهات السحابية ومعناها



الشكل (4.2) الجهات الفاعلة في السحابة

2.2 الأمن في الحوسبة السحابية

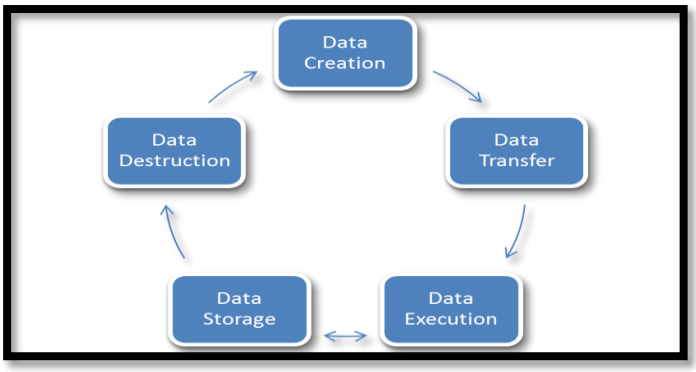
الأمن عنصر حاسم يستدعي التدقيق. الشركات مترددة في شراء ضمان لأمان بيانات العمل من البائعين. انهم يخشون فقدان البيانات للمنافسة وأمن البيانات. الأمن هو أكبر قلق بشأن الحوسبة السحابية. نظرًا لأن إدارة البيانات وإدارة البنية التحتية في السحابة مقدمة من طرف ثالث، فمن المخاطرة

دائمًا تسليم المعلومات الحساسة لمقدمي الخدمات هؤلاء. على الرغم من أن بائعي الحوسبة السحابية يضمنون حسابات أكثر أمانًا محمية بكلمة مرور، فإن أي علامة على خرق الأمان قد تؤدي إلى فقدان العملاء والشركات. يعد تأمين بيانات المستخدمين في السحابة أحد أكثر المهام صعوبة، حيث تكون موارد السحابة (مثل البرامج والأنظمة الأساسية والبنية التحتية) عرضة لسوء المعاملة أو السرقة أو التوزيع غير القانوني أو الضرر أو التضحية بالبيانات.

1.2.2 قضايا الأمن والتهديدات في الحوسبة السحابية

استقصاء حول التهديدات الأمنية العليا في الحوسبة السحابية، [23] قسم التهديدات السحابية إلى: i) تهديدات البيانات، ii) تهديدات الشبكة iii) تهديدات البيئة السحابية المحددة.

1) **تهديدات البيانات:** تعتبر البيانات واحدة من أهم الموارد القيمة لأي مؤسسة ويتزايد عدد العملاء الذين يقومون بتحويل بياناتهم إلى السحابة كل يوم. تشتمل دورة حياة البيانات في السحابة على إنشاء البيانات والعبور والتنفيذ والتخزين والتدمير كما هو مبين في الشكل 5.2 قد يتم إنشاء البيانات في العميل أو الخادم في السحابة، ويتم نقلها في السحابة عبر الشبكة وتخزينها في التخزين السحابية. عندما يتم نقل البيانات المطلوبة إلى بيئة التنفيذ حيث يمكن معالجتها. يمكن حذف البيانات من قبل مالكها لإكمال تدميرها.التحدي الأكبر في تحقيق أمان الحوسبة السحابية هو الحفاظ على أمان البيانات. تتمثل المشكلات الرئيسية التي تنشأ عند نقل البيانات إلى مجموعة النظراء في أن العملاء لا يتمتعون برؤية بياناتهم ولا يعرفون موقعها. إنهم بحاجة إلى الاعتماد على مزود الخدمة للتأكد من أن النظام الأساسي آمن، وأنه ينفذ خصائص الأمان الضرورية للحفاظ على بياناتهم آمنة. خصائص أمان البيانات التي يجب الحفاظ عليها في السحابة هي السرية تكامل البيانات والتفويض والتوافر والخصوصية. ومع ذلك، تنشأ العديد من مشكلات البيانات بسبب المعالجة غير الصحيحة للبيانات من قِبل الموفر السحابية. تتضمن تهديدات أمان البيانات الرئيسية خرق البيانات وفقدان البيانات والوصول غير المصرح به وانتهاكات تكامل البيانات. كل هذه المشكلات تحدث بشكل متكرر على البيانات السحابية. في هذه الورقة، نركز على انتهاكات البيانات وفقدان البيانات الموصوفة على أنها أخطر تهديدين للحوسبة السحابية. [23] ، [24] ، [25].



الشكل (5.2) دورة حياة البيانات في الحوسبة السحابية

أ- **فقد البيانات:** يعد فقدان البيانات مسألة حساسة لأي مؤسسة ويمكن أن يكون لها تأثير مدمر على أعماله. يحدث فقدان البيانات غالبًا بسبب المهاجمين الضارين أو حذف البيانات أو تلف البيانات أو فقدان مفتاح تشفير البيانات أو الأعطال في نظام التخزين أو الكوارث الطبيعية. واجه مقدمو الخدمات السحابية هجمات قاسية في 2013 أدت إلى فقد البيانات وتسرب البيانات. يؤدي انقطاع التيار الذي حدث مؤخرًا في عام 2019 في مرفق بيانات Amazon AWS إلى فقد البيانات لبعض العملاء كما. [30]

ب- **خروقات البيانات:** يُعرّف Cloud Security Alliance (2016) خرق البيانات بأنه حدث يتم فيه إطلاق المعلومات الحيوية والخاصة أو ملاحظتها أو سرقتها أو استخدامها من قبل شخص غير مصرح له. زادت خروقات البيانات بنسبة 54٪ في عام 2019 وفقًا للأمن القائم على المخاطر [27] أكثر من 3800 خرق بيانات قد ضربت المؤسسات في عام 2019 و89٪ من الانتهاكات ناتجة عن هجمات خارجية. يستشهد تقرير Deep Dive [26] باختراق كلمة مرور LinkedIn لعام 2012 كمثال رئيسي على الاختراق. تمكن المهاجم من سرقة 167 مليون كلمة مرور لأن LinkedIn لم يملح قاعدة بيانات كلمة المرور. وفقًا لوكالة CSA في عام 2018 [28]، تأثرت العديد من الشركات السحابية مثل Mongo DB و Dirty cow و Zynga و Yahoo و Net Traveler و Zepto و DynDNS بخروقات البيانات. لحماية أو منع فقدان البيانات وخروقاتها، يمكن استخدام الطرق التالية [25]، [29].

1. تنفيذ APIقوي لمراقبة الدخول.

2. تشفير وحماية سلامة البيانات في العبور.
3. يحلل حماية البيانات في كل من التصميم ووقت التشغيل.
4. تنفيذ ممارسات قوية لتوليد المفاتيح والتخزين والإدارة والتدمير.
5. يمسح مقدمو الطلب بشكل تعاقدي الوسائط المستمرة قبل طرحها في المجمع.
6. تحديد تعاقدية مزود النسخ الاحتياطي واستراتيجيات الاحتفاظ.

2) **تهديدات الشبكة:** تلعب الشبكة دورًا مهمًا في تحديد مدى كفاءة تشغيل الخدمات السحابية والتواصل مع المستخدمين. في تطوير معظم الحلول السحابية، لا يعتبر أمان الشبكة عاملاً مهمًا من قبل بعض المؤسسات. عدم وجود ما يكفي من أمان الشبكة يخلق هجمات متجهة للمستخدمين الضارين والأجانب مما يؤدي إلى تهديدات مختلفة للشبكة. معظم تهديدات الشبكة المهمة في السحابة هي اختطاف الحساب أو الخدمة، وهجمات الحرمان من الخدمة. [23]

أ- **سرق الحساب أو الخدمة:** يستخدم المستخدمون كلمات المرور للوصول إلى موارد الخدمة السحابية، لذلك عندما يتم سرق حساباتهم ، يتم إساءة استخدام كلمات المرور وتغييرها بشكل غير مفاجئ. يمكن للمستخدم غير المصرح به الذي لديه كلمة مرور الوصول إلى بيانات العملاء عن طريق سرقتها أو تغييرها أو حذفها أو لصالح بيعها للآخرين [25]، يمكنهم أيضًا التنصت على الأنشطة والمعاملات، ومعالجة البيانات، وإرجاع البيانات تزوير المعلومات وإعادة توجيه العملاء إلى مواقع غير شرعية [26]. يمكن أن يكون سبب هجمات الشبكة، بما في ذلك الخداع والاحتيال و " Scripting Scripting (XSS)" وشبكات الروبوتات والثغرات الأمنية مثل تجاوز سعة المخزن المؤقت، هو سرقة الحساب أو الخدمة [23]. تعرض موقع نيويورك تايمز للهجوم من قبل الجيش السوري الإلكتروني (SEA)، وهي مجموعة من المتسللين من سوريا في 27 أغسطس 2013 [31]، [32]. هاجم SEA موقع الويب الخاص بشركة NYT من خلال اختراق معلومات DNS الحساسة الخاصة بـ Melbourne IT، وهي منظمة مسجِّلة للمجال مقرها أستراليا، والتي تدير خدمات تسجيل النطاق لموقع الويب الخاص بشركة NYT إلى جانب مواقع الويب الخاصة بالمنظمات العالمية الأخرى مثل Twitter

وYahoo وغيرها. تقرير 2019، حدد تحالف الأمان السحابية [28] اختطاف حركة الخدمات باعتباره خامس أكبر خطر على الحوسبة السحابية. للحماية من اختلاس الحساب أو الخدمة، يُقترح سياسة وصول المستخدم، تقييد وصول المستخدم / ترخيصه، إلغاء وصول المستخدم، مراجعات وصول المستخدم، إدارة الحوادث، بيانات اعتماد هوية المستخدم، توثق المستخدم عن بُعد متعدد العوامل، تدقيق تسجيل / كشف التسلل [33].

ب- **هجوم رفض الخدمة:** يتم تنفيذ هجمات رفض الخدمة "DoS-Denial of service" لمنع المستخدمين الشرعيين من الوصول إلى الشبكة السحابية والتخزين والبيانات والخدمات الأخرى. يتم إجراؤها عادةً عن طريق تسوية خدمة يمكن استخدامها لاستهلاك معظم الموارد السحابية مثل طاقة الحساب والذاكرة وعرض النطاق الترددي للشبكة. يؤدي هذا إلى تأخير في العمليات السحابية، وأحيانًا لا تتمكن السحابة من الاستجابة للمستخدمين والخدمات الأخرى. يعد موفر DNS Dyn مثالًا رئيسيًا على هجوم DoS في تقرير CSA Deep Dive [28]، حيث قامت مجموعة خارجية بقيادة أجهزة IoT لإطلاق خدمة موزعة لرفض الخدمة (DDoS) على Dyn باستخدام البرامج الضارة Mirai. لقد نجحت نظرًا لأن أجهزة إنترنت الأشياء المعرضة للإصابة تستخدم بيانات الاعتماد الافتراضية. يوصي التقرير بتحليل حركة مرور الشبكة من أجل الحالات الشاذة ومراجعة واختبار خطط استمرارية العمل. لمنع هجمات DOS يجب على موفري السحابة تنفيذ جميع متطلبات الأمان الأساسية للشبكة السحابية وقواعد البيانات والخدمات الأخرى، يجب اختبار التطبيقات بعد التصميم، ويمكن أيضًا استخدام نظام الكشف عند الاختراق. [23]

ت- **هجمات التوثق:** وفقًا لتعريف من IBM، فإن هجوم التوثق هو هجوم "يسمح للمهاجم بتخمين اسم مستخدم أو كلمة مرور أو بطاقة ائتمان أو مفتاح تشفير للشخص باستخدام عملية تلقائية للتجربة والخطأ". يهدف إلى الوصول إلى الموارد دون بيانات الاعتماد الصحيحة. وفقًا لـ Techopedia "التوثق هي عملية تضمن وتؤكد هوية المستخدم وهي واحدة من الركائز الخمس لضمان المعلومات بما في ذلك تكامل البيانات والتوفر والسرية وعدم التنصل". وفقًا لقاموس أوكسفورد: "عملية إثبات أو إظهار شيء ما حقيقي. في

مستخدمي الحوسبة السحابية الذين يقومون بتسجيل الدخول إلى خدماتهم السحابية من مختلف الأجهزة والمواقع، تزيد هذه من مخاطر هجمات التوثق، ندرج هجمات التوثق المتنوعة على مركز عملائي وكيفية منعها:

1. **هجمات القوة الغاشمة:** في هذا النوع من الهجوم، تنطبق جميع مجموعات كلمة المرور الممكنة على كسر كلمة المرور. يتم تطبيق هجوم القوة الغاشمة عمومًا على كسر كلمات المرور المشفرة حيث يتم حفظ كلمات المرور في شكل نص مشفر.
2. **هجمات التنصت**: يكتسب المهاجم معلومات من تبادل التوثق واستعادة البيانات، مثل قيم مفتاح التوثق يمكن استخدامها للتوثق.
3. **هجمات رجل في منتصف الهجوم:** –حيث يقوم المهاجم بإدخال نفسه بين العميل والمدقق في عملية التوثق. يحاول المهاجم التوثق من خلال التظاهر كعميل للمدقق والتحقق إلى العميل.
4. **هجمات الإعادة:** –حيث يتتبع المهاجم بيانات التوثق الناجحة ويعيد هذه المعلومات للحصول على توثق غير صحيحة إلى المدقق.
5. **هجمات انتحال المدقق:** عندما يتظاهر المهاجم بأنه المدقق للعميل للحصول على مفاتيح التوثق أو البيانات التي يمكن استخدامها للتوثق بشكل خاطئ على المدقق.
6. **هجمات اختطاف الجلسة:** حيث يختطف المهاجم جلسة بعد التوثق الناجحة عن طريق سرقة مفتاح الجلسة أو ملف تعريف ارتباط الجلسة.
7. **هجوم القاموس:** هذا النوع من الهجوم هو أسرع نسبيا من هجوم القوة الغاشمة. بخلاف التحقق من جميع الاحتمالات باستخدام هجوم القوة الغاشمة، يحاول هجوم القاموس مطابقة كلمة المرور مع معظم الكلمات أو الكلمات التي تحدث في الحياة اليومية.
8. **هجمات ركوب الأمواج الكتف:** هو اسم بديل "للتجسس" يتجسس فيه المهاجم على حركات المستخدم للحصول على كلمة المرور الخاصة به. في هذا

النوع من الهجوم يلاحظ المهاجم المستخدم؛ كيف يدخل كلمة المرور، أي مفاتيح لوحة المفاتيح التي ضغط عليها المستخدم.

9. **هجمات التصيد الاحتيالي:** إنه هجوم قائم على الويب يقوم فيه المهاجم بإعادة توجيه المستخدم إلى موقع الويب المزيف للحصول على كلمات مرور / رموز سري للمستخدم.
10. **أدوات تسجيل المفاتيح:** أدوات تسجيل الدخول الرئيسية هي البرامج التي تراقب أنشطة المستخدم من خلال تسجيل كل مفتاح يضغط عليه المستخدم.

ث- تشمل تهديدات الشبكة الأخرى ما يلي: تزوير الطلبات عبر المواقع، هجمات تجاوز سعة المخزن المؤقت، البرمجة النصية للمواقع المشتركة، عيوب حقن SQL، معالجة رأس HTTP، معالجة الحقول المخفية، معالجة ملفات تعريف الارتباط، Botnets [35]، اختطاف الحساب وجلسة الجلسة، إلخ.

3) **تهديدات البيئة السحابية المحددة:** يتحمل مقدمو الخدمات السحابية مسؤولية كبيرة عن التحكم في البيئة السحابية. يتضمن ذلك بعض التهديدات الخاصة بالحوسبة السحابية مثل توفير واجهات وواجهات برمجة التطبيقات"APIs" غير آمنة للمستخدمين، والمهام الضارة، ونقاط الضعف في التكنولوجيا المشتركة، وسوء استخدام الخدمات السحابية، وعدم كفاية العناية الواجبة من قبل الشركات قبل الانتقال إلى السحابة. [23]

أ- **واجهات التطبيقات وواجهات البرمجة غير الآمنة:** يعرض مقدمو الحوسبة السحابية مجموعة من واجهات البرامج أو واجهات برمجة التطبيقات التي يستخدمها العملاء لإدارة الخدمات السحابية والتفاعل معها. يتم إجراء التوفير والإدارة والمراقبة باستخدام هذه الواجهات. يعتمد أمن وتوافر الخدمات السحابية العامة على أمان واجهات برمجة التطبيقات الأساسية هذه. من التوثق والتحكم في الوصول إلى التشفير ومراقبة النشاط، يجب تصميم هذه الواجهات للحماية من كل محاولات عرضية وخبيثة لتجاوز السياسة. لمنع هجمات Insecure API، يجب على المصممين تصميم واجهات برمجة التطبيقات هذه باتباع مبادئ الحوسبة الموثوقة، يجب تصميم واجهة برمجة التطبيقات وتنفيذها

بشكل آمن مع آليات التوثق القوية وتدابير التحكم في الوصول واختبارها قبل النشر بحثًا عن نقاط الضعف المحتملة. [24]

ب- **المستخدمين داخلية الخبيثين:** "Malicious insider" هذا معروف لمعظم المنظمات. يتم تضخيم هذا التهديد للمستهلكين للخدمات السحابية من خلال التقارب بين خدمات تكنولوجيا المعلومات والعملاء ضمن نطاق إدارة واحد، إلى جانب الافتقار العام للشفافية في عملية مزود الخدمة وإجراءاتها. على سبيل المثال، قد لا يكشف مقدم الخدمة عن الطريقة التي يمنح بها الموظفين إمكانية الوصول إلى الأصول المادية والافتراضية، أو كيف يراقب هؤلاء الموظفين، أو كيف يقوم بتحليل التقارير حول الامتثال للسياسات والإبلاغ عنها. لتعقيد الأمور، غالبًا ما يكون هناك قدر ضئيل أو لا يوجد أي رؤية لمعايير وممارسات التوظيف للموظفين السحابيين. من الواضح أن هذا النوع من المواقف يخلق فرصة جذابة لخصم ما –بدءًا من الهاكر الهاوي، أو الجريمة المنظمة، أو التجسس على الشركات، أو حتى الاقتحام الذي ترعاه الدولة القومية. يمكن لمستوى الوصول الممنوح أن يمكّن هؤلاء المطلعين الخبيثين من الحصول على بيانات سرية أو السيطرة الكاملة على الخدمات السحابية مع وجود خطر ضئيل أو معدوم للكشف. وفقًا لتقرير CSA [28]، عانت Zynga من الداخل الخبيث حيث قام موظف الساخط الذي قام بتنزيل بيانات العمل السرية من الشركة والتخلص منها. Mongo DB ، لينكداين لديها أيضا حالات من هذه الهجمات. لمنع الهجمات الداخلية الخبيثة، يمكن استخدام ما يلي: تشفير البيانات، والوصول إلى البنية التحتية للموظفين المصرح لهم فقط، وفصل الواجبات وما إلى ذلك.

ت- **إساءة استخدام الخدمات السحابية:** إن عمليات النشر السحابية المضمونة بشكل سيئ والتجربة المجانية للخدمة السحابية والاشتراكات الاحتيالية في الحسابات عن طريق الاحتيال في أداة الدفع تعرض نماذج الحوسبة السحابية لهجمات ضارة، وفقًا لوكالة CSA. قد تؤدي الجهات الفاعلة السيئة إلى الاستفادة من موارد الحوسبة السحابية لاستهداف المستخدمين أو المؤسسات أو موفري الخدمات السحابية الآخرين. تتضمن

أمثلة سوء استخدام الموارد المستندة إلى مجموعة النظراء إطلاق رسائل البريد الإلكتروني العشوائي لـ DDOS وحملات التصيد الاحتيالي. [28] ، [35]

ث- **عدم كفاية الهوية وبيانات الاعتماد والوصول وإدارة:** يعرض مقدمو الخدمات السحابية مجموعة من واجهات مستخدم البرنامج أو واجهات برمجة التطبيقات التي يستخدمها العملاء لإدارة الخدمات السحابية والتفاعل معها. يتم تنفيذ كل من التزويد والإدارة والمراقبة باستخدام هذه الواجهات، ويعتمد أمان وتوافر الخدمات السحابية العامة على أمان واجهات برمجة التطبيقات، حسبما تقول "CSA-Cloud Security Alliance" يجب أن تكون مصممة للحماية من المحاولات العرضية والخبيثة للتحايل على السياسة.

ج- **مشاكل التقنيات المشتركة:** يقدم مقدمو الخدمات السحابية خدمات قابلة للتطوير من خلال مشاركة البنية التحتية أو الأنظمة الأساسية أو التطبيقات، وملاحظات "CSA". تقسم تقنية الحوسبة خدمة "كخدمة" دون تغيير كبير في الأجهزة / البرامج الجاهزة -في بعض الأحيان على حساب الأمان. ربما لم يتم تصميم المكونات الأساسية التي تتضمن البنية التحتية التي تدعم نشر الخدمات السحابية لتوفير خصائص عزل قوية لبنية متعددة المستأجرين أو تطبيقات متعددة العملاء. يمكن أن يؤدي ذلك إلى ثغرات أمنية مشتركة يمكن استغلالها في جميع نماذج التسليم. مثال على تقرير "Deep Dive" هو مشكلة عدم حصانة سحابة السحابة، حيث تمكن ممثل ضار خارجي من سرقة مفاتيح واجهة برمجة التطبيقات وكلمات المرور وبيانات الاعتماد الأخرى من موفر خدمات الأمان "Cloud-flare"من خلال الاستفادة من ثغرة أمنية في برنامجه. يوصي التقرير بتشفير جميع البيانات الحساسة وتقسيم البيانات وفقًا لمستويات الحساسية [23]، [35].

ح- **عدم بذل العناية الواجبة الكافية:** عندما ينشئ المسؤولون التنفيذيون استراتيجيات أعمال، يجب مراعاة التقنيات السحابية ومقدمي الخدمات، وفقًا لوكالة "CSA". يعد وضع خريطة طريق وقائمة مرجعية جيدة للعناية الواجبة عند تقييم التقنيات ومقدمي الخدمات أمرًا ضروريًا لتحقيق أكبر فرصة للنجاح. المؤسسات التي تسارع إلى تبني التقنيات السحابية واختيار مقدمي الخدمة دون بذل العناية الواجبة تعرض نفسها لعدد من المخاطر.

خ- **تشمل التهديدات الأخرى للبيئة السحابية ما يلي:** نقاط ضعف التحكم في الوصول، قفل البائع [35].

2.2.2 الأهداف الأمنية

مصطلح "CIA" هو معنى معترف به على نطاق واسع للأمن يمثل الأهداف الأمنية المشتركة المتمثلة في السرية تكامل البيانات والتوافر. [6] فيما يلي تعريف [6] ، [8] أهداف الأمان في السحابة:

1. **السرية:** لا يتم توفير أو الكشف عن البيانات للأفراد أو الكيانات أو العمليات غير المصرح لهم.
2. **السلامة:** البيانات دقيقة وكاملة.
3. **التوفر:** البيانات التي يمكن الوصول إليها وقابلة للاستخدام عند الطلب من قبل كيان معتمد.

يمتد هذا التعريف في الأدبيات من خلال عدم التنصل، والأصالة والموثوقية، والترخيص، والإلغاء، والموقع، والمراجعة، قابلية النقل، وضمان الحذف [14]، [34].

1. **عدم التنصل:** القدرة على إثبات وقوع حدث أو إجراء مزعوم والكيانات الناشئة الخاصة به.
2. **الأصالة:** "Authenticity" البيانات تكن نسخة الأصلية.
3. **الموثوقية:** القدرة على توفير السلوك والنتائج المقصودة متسقة.
4. **التخويل:** يجب ألا تكون الكيانات المصادق عليها قادرة على الوصول إلى البيانات التي لا يحق لها الوصول إليها.
5. **الإلغاء:** أحد المتطلبات الهامة هو الإلغاء. يجب أن يكون إلغاء الوصول إلى البيانات الفردية والخدمة نفسها مسموحًا به.
6. **الموقع:** لا يتمكن المستخدمون عادة من الوصول إلى بياناتهم وخدمات "CSP-Cloud Service Provider" من موقع ثابت واحد. يمكنهم الوصول إليها من المنزل أو العمل. لذلك، يجب أن تتم توثق المستخدم دائمًا ويجب ألا تكون مرتبطة بالجهاز الذي يصل منه إلى الخدمة.
7. **القابلية للتدقيق:** يمكن تعريف القابلية للتدقيق على أنها مهمة تدقيق النظام أو البيئة في النموذج السحابية، ويجب تحديد من قام بإنشاء البيانات وعرضها وتعديلها لأن ذلك سيمكن من تتبع كل ما تم إنجازه عبر الملف. طوال دورة حياته بأكملها. يمكن تعريف تدقيق الأمان على أنه تقييم منهجي لأمان "CSP" من خلال قياس مدى توافق "CSP" مع مجموعة المعايير المحددة.

8. **قابلية النقل:** في الوقت الحالي، لا تتبع معظم "CSP,s–Cloud Service Providers" أي معايير لتنسيقات البيانات وواجهات الخدمة التي تسهل التشغيل البيني وسهولة النقل بين بعضها البعض.
9. **حذف البيانات:** يجب حذف البيانات عند عدم الحاجة إليها أو بعد فترة زمنية محددة. بعد حذف البيانات، يتعين على موفري السحابة أن يشهدوا أن البيانات التي تم تدميرها لن يتم إعادة بنائها أبدًا.

3.2.2 تكامل البيانات في الحوسبة السحابية.

تعد سلامة البيانات أحد العناصر الأكثر أهمية في أي نظام معلومات. بشكل عام، تعني سلامة البيانات حماية البيانات من الحذف أو التعديل غير المصرح به. تضمن إدارة قبول الكيان وحقوقه في موارد المؤسسة المحددة عدم إساءة استخدام البيانات والخدمات القيمة أو اختلاسها أو سرقتها. تتضمن ثلاثة جوانب لحماية تكامل البيانات في بيئة الحوسبة السحابية صحة (تحقق من أن كافة الصفوف في نتيجة استعلام تم إنشاؤها من البيانات الحقيقية الأصلية دون العبث)، اكتمال (تحقق من أن جميع الصفوف في نتيجة الاستعلام تم إنشاؤها من الحقيقي الأصلي تتضمن البيانات جميع المعلومات التي نتوقعها) ونضارة البيانات (تتحقق من تنفيذ الاستعلامات على البيانات الحقيقية المحدثة.) [52]. يتم تحقيق تكامل البيانات بسهولة في نظام مستقل مع قاعدة بيانات واحدة. يتم الحفاظ على تكامل البيانات في النظام المستقل عبر قيود ومعاملات قاعدة البيانات، والتي عادة ما يتم الانتهاء منها بواسطة نظام إدارة قواعد البيانات "DBMS–Database Management Sytems". يجب أن تتبع المعاملات خصائص "ACID–Atomicity,Consistency,Isolation,Durability" (الذرية، والاتساق، والعزلة، والمتانة) لضمان سلامة البيانات. تدعم معظم قواعد البيانات معاملات "ACID" ويمكنها الحفاظ على تكامل البيانات [54].

تكامل البيانات في النظام السحابية يعني الحفاظ على سلامة المعلومات. يجب عدم فقدان البيانات أو تعديلها من قبل المستخدمين غير المصرح لهم. تكامل البيانات هو الأساس لتوفير خدمة الحوسبة السحابية مثل SaaS وPaaS وIaaS. إلى جانب تخزين البيانات للبيانات الكبيرة، عادة ما توفر بيئة الحوسبة السحابية خدمة معالجة البيانات. يمكن الحصول على تكامل البيانات عن طريق

تقنيات مثل استراتيجيات تشبه "RAID–Redundant Array of Inexpensive Disks" والتوقيع الرقمي. قد يفقد مقدمو الخدمات السحابية البيانات بسبب عدة عوامل مثل الأخطاء البشرية وتعطل الأقراص والكوارث الطبيعية، نظرًا للكمية الكبيرة من الكيانات ونقاط الوصول في البيئة السحابية، يعتبر الترخيص حاسمًا في ضمان أن الكيانات المصرح لها فقط يمكنها التفاعل مع البيانات. من خلال تجنب الوصول غير المصرح به، يمكن للمؤسسات تحقيق ثقة أكبر في تكامل البيانات. توفر آليات المراقبة رؤية أكبر في تحديد من أو ما قد يكون قد قام بتغيير بيانات أو معلومات النظام، مما قد يؤثر على سلامتها. موثوق موفري الحوسبة السحابية للحفاظ على سلامة البيانات ودقتها. ومع ذلك، من الضروري إنشاء آلية إشراف طرف ثالث إلى جانب المستخدمين ومقدمي الخدمات السحابية. [54]

هناك طريقتان تقليديتان لإثبات تكامل البيانات في الاستعانة بمصادر خارجية في خادم بعيد. يمكن التحقق من سلامة البيانات عن طريق عميل أو من قبل طرف ثالث. يمكن للعميل تنزيل الملف ثم التحقق من قيمة هاش. بهذه الطريقة، يتم استخدام خوارزمية كود توثق الرسالة. تأخذ خوارزميات "MAC–Message Authentication Code" اثنين من المدخلات، وهما مفتاح سري وطول متغير للبيانات، والتي تنتج مخرجات واحدة وهي "MAC" (علامة)، بعد الحصول على "MAC"، يقوم مالك البيانات بتخصيص هذه البيانات إلى الشبكة. للتحقق من سلامتها، يقوم مالك البيانات بتنزيل البيانات الخارجية ثم يقوم بحساب "MAC" عليها ومقارنتها بالبيانات المحسوبة قبل الاستعانة بمصادر خارجية لتلك البيانات. باستخدام هذه الطريقة يمكن للعميل اكتشاف وتغيير بياناته. عيب هذه الطريقة هو أنه بالنسبة للملف الكبير، يستغرق تنزيل وحساب "MAC" للملف الكثير من الوقت ويستهلك المزيد من النطاق الترددي. لذلك، هناك حاجة لاستخدام تقنية أخف، والتي تحسب قيمة هاش. ثانياً، يمكن للطرف الثالث حساب قيمة هاش في السحابة باستخدام شجرة تجزئة. في هذه التقنية، يتم بناء شجرة هاش من أسفل إلى أعلى حيث تكون الأوراق هي البيانات، ويتم تجميع الآباء أيضًا إلى أن يتم الوصول إلى الجذر. يقوم مالك البيانات بتخزين الجذر فقط. عندما يحتاج المالك إلى التحقق من بياناته، يسأل عن قيمة الجذر فقط ويقارنها بالقيمة التي لديه. هذا أيضًا غير فعال للغاية لأن حساب قيمة هاش لعدد كبير من القيم يستهلك المزيد من العمليات الحسابية [2]. لذلك، هناك حاجة لإيجاد طريقة للتحقق من تكامل البيانات مع توفير النطاق الترددي وقوة الحساب

[44] اقترح إطارًا نظريًا "بروفات الاسترجاع" لتحقيق التحقق من تكامل البيانات عن بُعد من خلال الجمع بين رمز تصحيح الأخطاء والتحقق من البقعة [9]. يستخدم نظام "HAIL" Availability and Integrity Layer" آلية "POR" للتحقق من تخزين البيانات في السحب المختلفة، ويمكن أن يضمن التكرار في نسخ مختلفة وتحقيق توافر وفحص التدقيق [10]، [11]. تم تطوير مخططات أخرى مثل إثبات الملكية وإثبات الامتلاك [9]، [10]، [11]، [43]، [44].

1.3.2.2 عوامل لتعزيز تكامل البيانات في الحوسبة السحابية

1. **التخويل:** للحفاظ على سلامة البيانات في السحابة، يجب أن توفر النظم آلية ترخيص قوية وفعالة بحيث لا ينبغي للكيانات التوثق الوصول إلى البيانات غير المصرح لها بالوصول إليها.
2. **التوثق:** التوثق هي عملية تضمن وتؤكد هوية المستخدم في السحابة، للحفاظ على سلامة البيانات هناك يجب أن يكون هناك التنفيذ السليم لآلية التوثق التي قد تشمل التوثق عبر اسم المستخدم وكلمة المرور، التوثق متعددة العوامل "MFA–Multifactor Authentication"، البنية التحتية للمفتاح العام "PKI–Primary Key Infrastructure"، الدخول الموحد "Single Sign On–SSO"، التوثق البيو مترية [46]. للأنظمة للحفاظ على سلامة البيانات، يجب اعتبار آلية التوثق عالية لأنه إذا تمكنت من وصول البيانات إلى المهاجم يمكنه احداث التغييرات في البيانات.
3. **التحكم في الوصول:** التحكم في الوصول هو عادة سياسة أو إجراء يسمح أو يمنع أو يقيد الوصول إلى النظام. قد تقوم أيضًا برصد وتسجيل جميع المحاولات التي بذلت للوصول إلى النظام. قد يحدد التحكم في الوصول أيضًا المستخدمين الذين يحاولون الوصول إلى نظام غير مصرح به. إنها آلية مهمة جدًا للحماية في أمان الكمبيوتر. يساعد التحكم في الوصول في الحفاظ على تكامل البيانات حيث يتم تسجيل كل وصول ويمكن للمراجعين مراجعة ذلك لجعل التخطيط الأمني في المستقبل.
4. **فقدان البيانات –آلية الاسترجاع:** قد يتم فقد البيانات بسبب عدة أسباب في المخازن السحابية مثل الكوارث الطبيعية أو فشل التطبيق أو فشل الشبكة أو التسلل أو القرصنة أو الأكواد الخبيثة

وفشل النظام. يتم استخدام العديد من آليات وحلول الاسترجاع [41]، [42] في حالات مثل هذه الكارثة:

أ- **النسخ الاحتياطي المحلي التكرار الجغرافي والنسخ الاحتياطي:** في[39]، يوجد في منطقتين سحابة نسخ متماثل لبعضهما البعض. إذا تعطلت إحدى المناطق، فسيتم تشغيل منطقة أخرى وتقديم الخدمات. هناك وحدة تراقب المناطق لاكتشاف الكوارث. التخزين السحابية بين القطاعات (IPCS): تم اقتراح هذا المنهج لتخزين البيانات السحابية (جيان هوا ونان، 2011). وفقًا لجمعية صناعة شبكات التخزين (SNIA)، فإن ثلاثة مواقع نسخ احتياطي على الأقل ضرورية لتخزين بيانات الأعمال. يجب تخزين بيانات المستخدمين في ثلاثة مواقع جغرافية مختلفة: الخوادم، خادم النسخ الاحتياطي المحلي وخادم النسخ الاحتياطي عن بُعد. يمنح هذا النموذج قدرة الاتصال على النسخ الاحتياطي للمواقع من أجل زيادة تكامل البيانات. النسخ الاحتياطي الآمن للبيانات الموزعة : توزيع النسخ الاحتياطية بين عدة وحدات تخزين. يجب على موفري خدمة الصوت عبر الإنترنت التأكد من أن هذه الحلول المستخدمة لاسترداد البيانات [41]، [42] في حالة فقدان البيانات تعمل بكفاءة وبشكل كامل لأنه إذا لم يتم استرداد البيانات تمامًا، فسيؤثر ذلك على سلامتها.

ب- **إدارة الموارد:** تتكون السحب غير المتجانسة من العديد من الأجهزة والبرامج المختلفة مثل التخزين المختلط والأقراص المتنوعة. في المؤسسات المستندة إلى مجموعة النظراء، يتم تخزين بيانات العمل بالكامل في وحدة التخزين السحابية. لذلك، تعد حماية البيانات وأمانها واستعادتها أمرًا بالغ الأهمية في هذه البيئات. البيانات المعرضة للخطر هي البيانات التي تمت معالجتها في المضيف الأساسي ولكنها لم تحدث في مضيف النسخ الاحتياطي حتى الآن. لذلك، في حالة الكوارث، من الضروري استخدام تقنية محسنة لاستعادة البيانات في السحب التخزينية. هناك ثلاثة حلول لاستعادة البيانات المقترحة في. [40]

i. استخدام أسرع تكنولوجيا للقرص في حالة وقوع كارثة لتكرار البيانات في خطر.

ii. تغيير عتبة الصفحة القذرة: "Dirty page threshold" قد يتم تخفيض النسبة المئوية للصفحات القذرة الموجودة في ذاكرة الوصول العشوائي والتي يجب انتظارها للتنظيف على القرص.

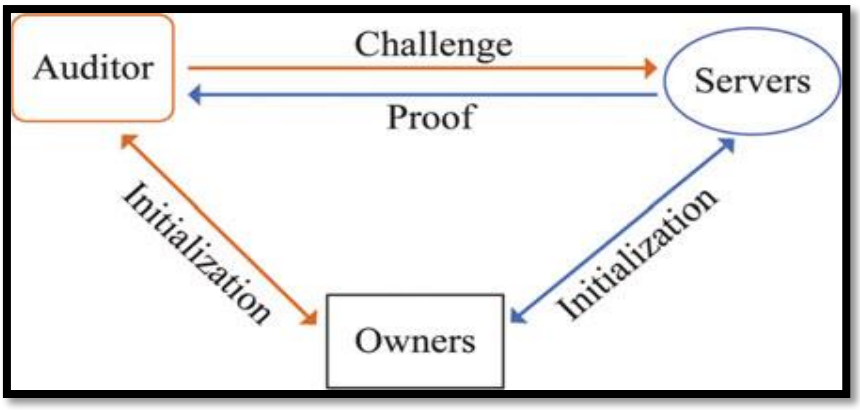
iii. التنبؤ واستبدال الأجهزة الخطرة: يمكن حساب بعض العوامل المهمة مثل استهلاك الطاقة وتبديد الحرارة واستخدام ائتمان الكربون وأهمية البيانات (المخزنة على كل قرص) في فترة زمنية محددة. [40]

ت- **توسيع نطاق الرفع / لأسفل:** في بعض الأحيان، يمكن أن يؤدي أداء الوظائف ذات الأولوية العالية إلى تقليل خسارة المال أو حتى زيادة الإيرادات في حالة وقوع كارثة. بعد حدوث كارثة طبيعية في منطقة ما، يواجه مقدمو الخدمات السحابية طلبات خدمة للفيضانات. في هذه الحالة، يتعين على مقدمي الخدمة إدارة خدمات المستخدمين الحاليين وأيضًا التعامل مع طلبات المستخدمين الجديدة. يجب أن يرضي مقدمو الخدمة المستخدمين الحاليين وأن يخدموا عملاء جدد قدر الإمكان.

5. **التدقيق:** يتم تقديم تدقيق البيانات في الحوسبة السحابية للتعامل مع تخزين آمن للبيانات. المراجعة هي عملية تحقق من بيانات المستخدم والتي يمكن إجراؤها إما من قبل المستخدم نفسه (مالك البيانات) أو بواسطة مدقق خارجي (TPA :Third Party Auditor). يلعب التدقيق دورًا كبيرًا للغاية في الحفاظ على سلامة البيانات المخزنة على السحابة [43]. يمكن إجراء التدقيق بطريقتين

أ- تدقيق خاص لا يُسمح فيه إلا لمستخدم أو مالك البيانات بالتحقق من سلامة البيانات المخزنة.

ب- المراجعة العامة التي تسمح لأي شخص، وليس فقط العميل، بالتحدي على الخادم وإجراء فحص التحقق من البيانات بمساعدة مدققي الطرف الثالث "TPA". "TPA"هو كيان يعمل نيابة عن العميل. يتمتع "TPA"بجميع الخبرات والقدرات والمعرفة والمهارات اللازمة للتعامل مع أعمال التحقق من تكامل البيانات. يوضح الشكل 6.2 تدفق تكامل البيانات باستخدام "TPA".



الشكل (6.2) تدفق تكامل البيانات باستخدام TPA.

تم اقتراح العديد من خطط التدقيق، وقد اقترح Ateniese وزملاؤه Juel وKalisk إثبات إمكانية الاسترداد "POR-Proof of Retrieavavility" وخطط تدقيق حسابات امتلاك البيانات "PDP-Proof of Data Posession" التي يمكن إثباتها. [43] ، [44]. ذكر راجو وآخرون [45] أن الإجراء الأساسي لتناسق المعلومات في السحابة هو إثبات إمكانية الاسترداد "POR" وحيازة ملكية البيانات المتوافقة "PDP" التي تستخدم عادةً لضمان موثوقية البيانات.

6. **قابلية التشغيل وقابلية التشغيل البيني:** تعد قابلية النقل مشكلة كبيرة في الحوسبة السحابية في الوقت الحالي، حيث لا تتبع معظم "CSP's" أي معايير لتنسيقات البيانات وواجهات الخدمة، وتشير قابلية التشغيل البيني إلى سهولة ترحيل التطبيقات / البيانات وتكاملها بين مختلف مقدمي الخدمات. أثناء الترحيل من مزود سحابة إلى آخر إذا لم يتم نقل البيانات بالكامل أو أي خطأ في العملية، يمكن أن يؤثر ذلك على سلامة البيانات.

4.2.2 الحلول الأمنية السحابية والآلية القائمة

كما ناقشنا سابقًا أن إحدى المشكلات التي تؤثر على بيئة الحوسبة السحابية هي مسألة الأمان، حيث يقوم مزودو السحابة بتطبيق آليات وتقنيات مختلفة للحفاظ على الأمان، وقد اقترح الباحثون حلولًا مختلفة أيضًا، في هذه الأطروحة نحن مهتمون بالآلية التالية: التحكم في الوصول، التشفير، سلامة البيانات، رمز توثق الرسالة، التوقيع الرقمي.

1.4.2.2 آليات التحكم في الوصول: هي تقنية أمنية تنظم من أو من يستطيع عرض أو استخدام الموارد في بيئة الحوسبة. إنه مفهوم أساسي في مجال الأمن يقلل من مخاطر العمل أو المؤسسة. [18] ، [36] هناك نوعان من التحكم في الوصول: المادية والمنطقية. التحكم الفعلي في الوصول هو التحكم في كيفية وصول الأشخاص أو المستخدمين إلى الخوادم أو المباني أو الغرف أو غيرها من البنى التحتية لتكنولوجيا المعلومات. بينما تحد عناصر التحكم في الوصول المنطقي من الاتصالات بشبكات الكمبيوتر وملفات النظام والبيانات [36].

المكونات الرئيسية للتحكم في الوصول هي: حق الوصول، الموضوع والكائن [18].

أ- يمكن أن يكون الموضوع إما مستخدم أو عملية أو سلسلة رسائل أو برنامج سيتخذ إجراءات معينة في النظام.

ب- الكائن عبارة عن عنصر كائن في النظام يمكن للمستخدم من خلاله اتخاذ إجراءات. ومن الأمثلة على ذلك الخوادم والمباني والأجهزة الأخرى.

ت- تحدد حقوق الوصول لكل كائن الإجراءات التي قد يقوم بها الشخص، وهذه هي القواعد المحددة لكل موضوع.

هناك عدة أنواع من نماذج التحكم في الوصول [18]، [36] من بين هذه النماذج:

أ- **التحكم الإلزامي في الوصول:** نموذج أمان تنظم فيه حقوق الوصول بواسطة سلطة مركزية تستند إلى مستويات متعددة من الأمن. يتم تعيين التصنيفات إلى موارد النظام ونظام التشغيل أو نواة الأمان، وتمنح أو تمنع الوصول إلى كائنات الموارد هذه بناءً على تصريح أمان المعلومات للمستخدم أو الجهاز.

ب- **التحكم في الوصول إلى السلطة التقديرية:** هو وسيلة للتحكم في الوصول يقوم فيها مالكو أو مسؤولو النظام أو البيانات أو الموارد المحمية بتعيين السياسات التي تحدد من أو ما هو مخول للوصول إلى المورد. تتيح العديد من هذه الأنظمة للمسؤولين الحد من انتشار حقوق الوصول. انتقاد شائع لأنظمة "DAC–Discretional access control" هو عدم وجود سيطرة مركزية.

ت- **التحكم في الوصول إلى قواعد الدور**: آلية تحكم في الوصول تستخدم على نطاق واسع تقيد الوصول إلى موارد الكمبيوتر استنادًا إلى أفراد أو مجموعات لها وظائف أعمال محددة –المستوى التنفيذي، المستوى الهندسي– بدلاً من هويات المستخدمين الفرديين. يعتمد نموذج الأمان المستند

إلى الأدوار على بنية معقدة من مهام الدور، وتراخيص الأدوار وأذونات الدور التي تم تطويرها باستخدام هندسة الأدوار لتنظيم وصول الموظفين إلى الأنظمة. يمكن استخدام أنظمة "RBAC–Role based access control" لفرض أطر عمل "MAC" و"DAC".

ث- **التحكم في الوصول المستند إلى القواعد** نموذج أمان يحدد فيه مسؤول النظام القواعد التي تحكم الوصول إلى كائنات الموارد. غالبًا ما تستند هذه القواعد إلى شروط، مثل وقت اليوم أو الموقع. ليس من غير المألوف استخدام شكل من أشكال التحكم في الوصول المستند إلى القواعد والتحكم في الوصول المستند إلى الأدوار لفرض سياسات وإجراءات الوصول.

ج- **التحكم في الوصول المستند إلى السمة / الهوية:** منهجية تدير حقوق الوصول من خلال تقييم مجموعة من القواعد والسياسات والعلاقات باستخدام سمات أو هويات المستخدمين والأنظمة والظروف البيئية.

2.4.2.2 آلية تكامل البيانات: الغرض من آلية تكامل البيانات هو توفير وسيلة للمستخدم لاكتشاف ما إذا كان قد تم إجراء أي تغييرات غير مصرح بها على الملفات إما عن قصد أو عن طريق الخطأ أو إتلاف أو فقد الملف عن طريق التأكد من إمكانية اكتشافه. عادةً ما تستخدم وظائف تجزئة التشفير لضمان سلامة البيانات [9]، [10]، [11]، [18].

دالة هاش "Hash function" هي خوارزمية رياضية تقوم بتخطيط بيانات ذات حجم تعسفي إلى تجزئة ذات حجم ثابت. وهي مصممة لتكون وظيفة في اتجاه واحد، غير قابلة للتحويل للعكس [18]. يُطلق عليه أيضًا ملخص الرسالة أو نتيجة هاش أو ببساطة: كما هو مذكور في [18]، [37] تحتوي وظائف الدالة هاش على الخصائص التالية:

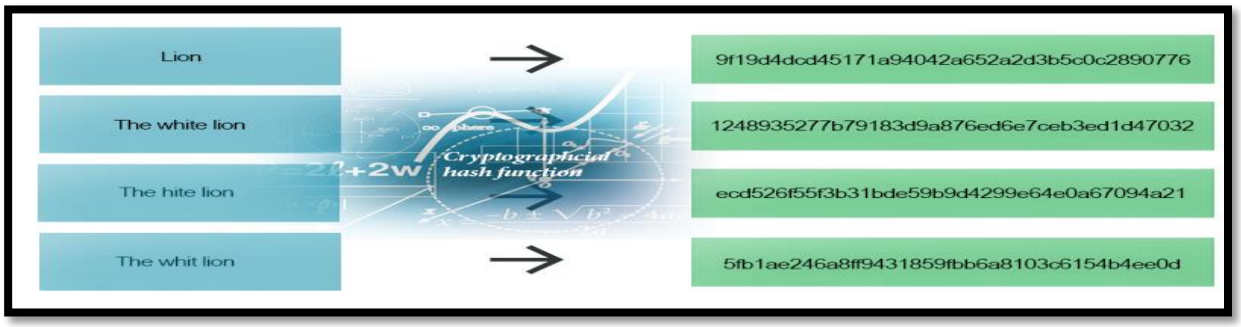
أ- دالة هاش فعالة في حساب وقت المعالجة

ب- باستخدام دالة هاش، يجب أن يكون من المستحيل تجديد رسالة من قيمة هاش الخاصة بها.

ت- يجب تجنب اصطدام هاش، كل رسالة لها تجزئة خاصة بها. من غير المجدي حسابيًا العثور على رسالتين مختلفتين تنتجان نفس قيمة هاش.

ث- كل تغيير في رسالة، حتى أصغرها، يجب أن يغير قيمة هاش. يجب أن يكون مختلفا تماما. يطلق عليه تأثير الانهيار.

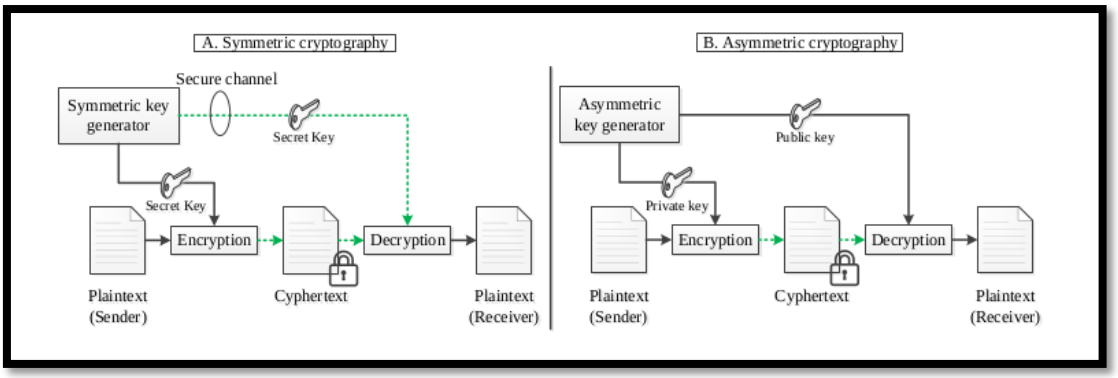
ج- إنه غير ممكن حسابيًا ورسالة تقابل قيمة تجزئة رسالة معينة. حتى أصغر تغيير (حرف واحد) يجعل هاش كلها مختلفة كما هو موضح في الشكل 7.2.



الشكل (7.2) مثال لدالة هاش

3.4.2.2 آلية التشفير: التشفير هو تقنية تشفير تقوم بتحويل رسالة قابلة للقراءة (وتسمى أيضًا نص عادي) إلى رسالة غير قابلة للقراءة (وتسمى أيضًا النص المشفر) باستخدام خوارزمية تشفير متعددة وطرق ، في حين أن القارئ المصرح له فقط يحتفظ بمفتاح سري يمكن استرداد الرسالة الأصلية باستخدام خوارزمية فك التشفير التي تعد متنوعة من خوارزمية التشفير المستخدمة [18]. الهدف من تقنيات التشفير هو تحقيق الهدف الأمني. هناك نوعان من أنظمة التشفير: أنظمة التشفير المتماثل وأنظمة التشفير غير المتماثلة.

1. **التشفير المتماثل:** في الخوارزميات المتماثلة، يستخدم نفس المفتاح لكلا تشفير النص العادي وفك تشفير النص المشفر، حيث يوافق المرسل والمستقبل على مفتاح ثم يستخدمه لتشفير وفك تشفير. تتمتع خوارزميات التشفير المتماثل بالسرعة والكفاءة الحسابية للتعامل مع تشفير البيانات الضخمة.
2. **التشفير غير المتماثل:** هذه تقنية تشفير حديثة، تستخدم فيها الخوارزميات مفتاحين مختلفين (المفتاح العمومي والمفتاح الخاص) للتشفير وفك التشفير. يتم جعل المفتاح العمومي عامًا ولكن المتلقي فقط لديه المفتاح الخاص. يمكن استخدام التشفير غير المتماثل لإنشاء خوارزميات للتشفير والتوقيع الرقمي واتفاق المفتاح. المثال الشائع هو نظام تشفير "RSA". يوضح الشكل 8.2 كيفية عمل التشفير المتماثل وغير المتماثل.



الشكل (8.2) التشفير المتماثل وغير المتماثل

4.4.2.2 رمز توثق الرسائل: رمز توثق الرسالة (غالبًا ما يسمى MAC) عبارة عن كتلة مكونة من بضع وحدات بايت يتم استخدامها للتوثق رسالة. يستطيع المتلقي فحص هذه الكتلة والتأكد من أن الرسالة لم يتم تعديلها من قبل الطرف الثالث. [18]

رمز توثق رسالة هاش ذات المفاتيح "KHMC–Key Hashed Message Code": هو نوع معين من رمز توثق الرسائل "MAC" يتضمن دالة تجزئة التشفير ('H') مع مفتاح تشفير سري. كما هو الحال مع أي "MAC"، يمكن استخدامه للتحقق في وقت واحد من كل من سلامة البيانات وتوثق الرسالة.

5.4.2.2التوقيع الرقمي وعدم التنصل: التوقيع الرقمي هو مخطط رياضي للتحقق من صحة الرسائل أو الوثائق الرقمية. تحتوي التوقيعات الرقمية على العديد من التطبيقات في أمن المعلومات، بما في ذلك التوثق وسلامة البيانات وعدم التنصل [18]، [38]. تعتمد عملية التوقيع على تشفير غير متماثل. مخطط التوقيع هو ثلاثة خوارزميات ("KGen–Key Generation"، Sign، Verify). يمكنك استخدام "KGen" لإنشاء زوج مفاتيح عشوائي SK، pk، sk هو سر ويتم نشر pk بشكل عام. يتم استخدام علامة (m،sk) لحساب توقيع σ تحت المفتاح العمومي pk على الرسالة m. يمكن استخدام التحقق (pk وm وσ) من قبل أي شخص للتحقق من صحة σ.

تُستخدم دالة تجزئة بالاقتران مع التوقيع الرقمي لتكامل البيانات وتوثق المنشأ: حيث يتم تجزئة الرسالة عادةً أولاً، ثم يتم تسجيل قيمة هاش، كممثل للرسالة، بدلاً من الرسالة الأصلية. يوفر التوقيع الرقمي

ميزة مهمة على تقنية "MAC"، وهو خدمة عدم التنصل. توفر هذه الخدمة الحماية من الإنكار الخاطئ للتورط في جمعية [18].

6.4.2.2 تقنيات التوثق في الحوسبة السحابية: في الحوسبة السحابية ، تم تنفيذ العديد من تقنيات التوثق ، ومن أمثلة هذه التقنيات المذكورة في [65] ما يلي:

أ- **توثق اسم المستخدم وكلمة المرور:** من أجل الوصول إلى المعلومات الموجودة في "CSP"، يجب إدخال اسم المستخدم وكلمة المرور من قبل المستخدم إلى النظام. يلاحظ أن كلمات المرور يجب أن تحتوي على أحرف كبيرة وأرقام وعلامات. هذا غير آمن بما فيه الكفاية حيث يمكن تخمين كلمات المرور أو باستخدام هجمات القوة الغاشمة. [65]

ب- **التوثق المتعددة العوامل**: **لجعل** المعلومات أكثر أمانًا في بيئة الحوسبة السحابية، يجب استخدام مجموعة من أساليب التوثق. لا تقوم MFA بالتحقق من صحة اسم المستخدم وكلمة المرور، ولكنها تتطلب أيضًا عاملًا آخر، على سبيل المثال التوثق البيومترية أو أسئلة الأمان. هذا يحسن للغاية أمن التوثق. [65]

ت- **الدخول الموحد:** هذه طريقة للوصول إلى نظام برمجي متعدد مستقل بطريقة تسمح للمستخدم بتسجيل الدخول إلى جميع الأنظمة عندما يقوم المستخدم بتسجيل الدخول إلى النظام. تمنع هذه العملية المستخدم من إدخال كلمات المرور الخاصة به وعددًا كبيرًا، ويمكن أن يمنع الهجمات مثل الخداع والإنسان في الوسط. [65]

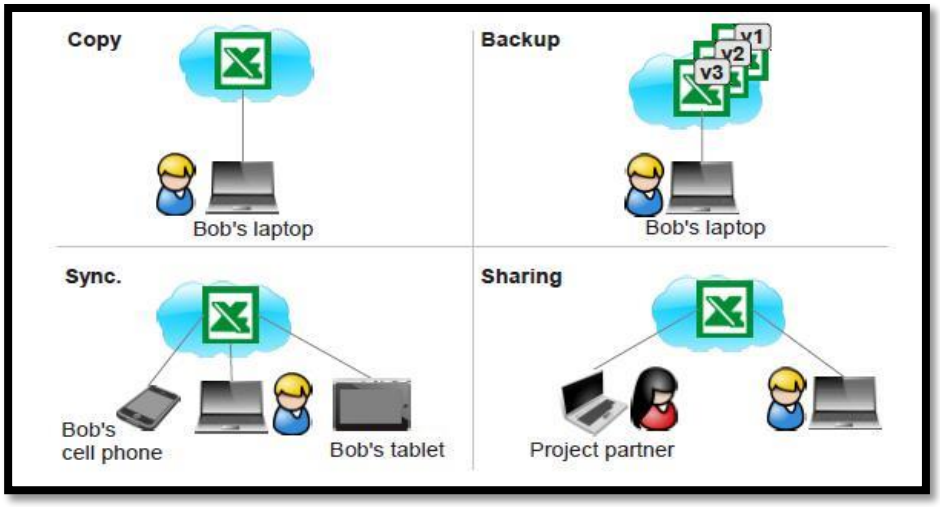
ث- **البنية التحتية للمفتاح العام):** تضمن آلية PKI تكامل البيانات، وسرية البيانات، وعدم التنصل، والتوثق القوي، وكذلك الترخيص. [18] ، [38] ، [65]

ج- **التوثق البيومترية:** هي عملية التحقق من صحة ما إذا كان المستخدم هو الذي يطلب منه أن يكون، والاعتراف بخصائص الفرد السلوكية والفسيولوجية يوفر الأساس لهذه التقنية التوثق. التوثق البيومترية تصنف إلى نوعين: السلوكية والفسيولوجية.البيومترية السلوكية: تعتمد على سلوك المستخدم. في هذا النوع من التوثق البيومترية، يتم استخدام التوقيعات وضربات المفاتيح والمطبوعات الصوتية. البيومترية الفسيولوجية"Physiological": وهي قائمة على الخصائص

الفيزيائية للإنسان. في هذا النوع من التوثق البيومترية، يتم استخدام اليدين والوجوه وقزحية العين وبصمات الأصابع وطباعة النخيل وشبكية العين. [65]

5.2.2 مبادئ خدمات التخزين السحابية

سوف نستكشف الميزة الرئيسية لخدمات التخزين المخزنة. هذه الميزات هي: النسخ والنسخ الاحتياطي والتزامن ومشاركة الملفات. يجب أن تتضمن أي خدمة تخزين واحدة على الأقل من هذه الميزات، وقد تتضمن ميزات متعددة في نفس الوقت. يوضح الشكل 9.2 [58] الملامح الرئيسية لخدمة التخزين السحابية.



الشكل (9.2) الملامح الرئيسية لخدمة التخزين السحابية

1. نسخ

تقوم ميزة النسخ بإنشاء صورة لبيانات المستخدم المحلية في السحابة. يستخدم المستخدم هذه النسخة للتأكد من أن بياناته متوفرة دائمًا حتى لو كان هناك عطل في الأجهزة المحلية (مثل تعطل القرص الصلب). علاوة على ذلك، ستساعد هذه النسخة المستخدم في الوصول إلى بياناته من أي مكان (على سبيل المثال من خلال متصفح الويب) حتى لو كانت أجهزته المحلية غير متوفرة. هذا يعطي المستخدم طريقتين لتخزين بياناته في السحابة. في الطريقة الأولى، يقوم المستخدم يدويًا بتحميل ملفاته ومجلداته في السحابة من خلال متصفح الويب. بينما في الطريقة الثانية، يستفيد المستخدم من برنامج العميل،

المثبت محليًا على جهاز المستخدم، لتحميل ملفاته ومجلداته تلقائيًا من مجلد معين خاص بالعميل إلى وحدة التخزين السحابية. من المهم أيضًا ملاحظة أن ميزة النسخ مختلفة عن ميزة النسخ الاحتياطي. حيث يتم تخزين البيانات في ميزة النسخ الاحتياطي في فترات زمنية محددة مسبقًا، بينما يتم تخزين البيانات في ميزة النسخ بشكل مستمر [59] [60].

2. النسخ الاحتياطي

تسمح ميزة النسخ الاحتياطي للمستخدمين باستعادة أي إصدار تم تخزينه مسبقًا من ملف أو مجلد على مدار فترة زمنية طويلة (عادةً ما تكون سنوات). لإنشاء نسخ احتياطية، عادة ما تستخدم خدمات التخزين السحابية عملية تلقائية. في هذه العملية، يتم نسخ البيانات ونقلها وتخزينها بشكل دوري في السحابة بحيث يتم استردادها في حالة فقد البيانات الأصلية. لتنفيذ هذه العملية، يتعين على مزودي خدمة التخزين السحابية تقديم برنامج عميل مثبت محليًا في جهاز المستخدم. يمكّن هذا البرنامج المستخدمين من تحديد البيانات التي سيتم نسخها احتياطيًا، وتكوين فترة الاستبقاء، وجدولة النسخ الاحتياطية. بالإضافة إلى ذلك، يمكن لهذا البرنامج إما تشغيله بشكل مستمر في الخلفية أو تم تكوينه لإجراء النسخ الاحتياطي بشكل منتظم وذلك لإجراء نسخ احتياطي للملفات التي تم إنشاؤها حديثًا أو التي تم تغييرها. علاوة على ذلك، تتمثل إحدى المهام الأخرى لبرنامج العميل في التحقق من البيانات التي يجب نسخها احتياطيًا. أخيرًا، يمكنه تمكين المستخدمين من مراقبة عملية النسخ الاحتياطي منذ النسخة الاحتياطية السابقة [59]، [60].

3. التزامن

التزامن يعني وجود اتساق بين البيانات المخزنة في مصادر مختلفة. على سبيل المثال، يمكن للمستخدم امتلاك مجموعة من الأجهزة، على سبيل المثال جهاز كمبيوتر، كمبيوتر محمول، أجهزة لوحية وهاتف ذكي، ويريد أن يكون لديه نفس البيانات المتاحة على جميع الأجهزة وعندما يتم تغيير البيانات في جهاز واحد يتم تعديل الآخرين مع هذه التغييرات. لذلك، يتعين على مزودي خدمة التخزين السحابية تزويد المستخدمين ببرنامج عميل قادر على اكتشاف أي تغييرات في أي ملف في أي جهاز ويعكس هذه التغييرات على الأجهزة الأخرى. يمكن لبرنامج العميل هذا القيام بذلك من خلال تقديم عدد من الخيارات للمستخدم: دمج الملفات، الكتابة فوق إصدار واحد، أو الاحتفاظ بكلا الإصدارين عن طريق تطبيق نظام إعادة التسمية [59]، [60].

4. المشاركة

مشاركة البيانات هي عملية مشاركة ملفات البيانات أو المجلدات مع الآخرين. يقدم مزودو خدمة التخزين السحابية للمستخدمين أشكالًا مختلفة من المشاركة. يمكن للمستخدمين مشاركة البيانات مع مشتركين آخرين في نفس الخدمة، أو مع مجموعة مغلقة من الأشخاص من خدمات أخرى، أو مع الجميع. على سبيل المثال، يمكن للمستخدمين التعاون مع الزملاء أو شركاء المشروع أو الأصدقاء. من المهم أيضًا ملاحظة أن أي ملف / مجلد مشترك يحتوي على مجموعة من حقوق الوصول الثابتة أو التي تمت تهيئتها مثل القراءة أو الكتابة أو الحذف [59] [60].

6.2.2 واجهات تستخدم لخدمات التخزين السحابية

1. عملاء البرمجيات الاحتكارية

الواجهة الأكثر راحة التي يقدمها مزودو خدمات التخزين السحابية هي عملاء البرامج الاحتكارية. كل مزود لديه عميل خاص به ويستفيد المستخدمون من برنامج العميل هذا من خلال تثبيته فقط على أجهزتهم. يوفر هذا العميل المملوك للمستخدمين مجموعة متنوعة من الخدمات التي يمكنهم استخدامها. وتشمل هذه الخدمات: اختيار البيانات المراد نقلها إلى السحابة، وإدارة الخدمة وتكوين ميزات مثل المزامنة أو المشاركة [61]، [62].

2. واجهة المتصفح

واجهة متصفح الويب هي طريقة تستخدم للوصول إلى بيانات المستخدم. الميزة الرئيسية لهذه الطريقة هي الوصول إلى البيانات من أي مكان ومن أي جهاز ليس لديه برنامج عميل مثبت. عادة ما تكون واجهة المستعرض مفضلة من قبل المنظمات التي لا ترغب في إنفاق الوقت والمال في إدارة البرامج لموظفيها. علاوة على ذلك، يُفضل أيضًا من قبل المستخدمين النهائيين الذين يرغبون في مشاركة بياناتهم متى أرادوا [62].

3. واجهة برمجة التطبيقات

يوفر معظم مزودي خدمات التخزين السحابية للمستخدمين إمكانية الوصول إلى واجهة برمجة التطبيقات "API–Application Programming Interfaces". ويمكن للمطورين استخدام واجهات برمجة التطبيقات هذه لدمج الوصول إلى خدمة التخزين السحابية في تطبيقاتهم. على سبيل المثال، لتوفير

ألعاب لعبة جهاز محمول عبر أجهزة ومنصات متعددة. لكي يمنح مقدمو خدمة التخزين السحابية العملاء إمكانية الوصول إلى واجهات برمجة التطبيقات، يتعين عليهم كشف خدمة ويب أو تطبيق ويب يمكن الوصول إليه باستخدام بروتوكول اتصال موحد [62].

7.2.2 التحسين في خدمات التخزين السحابية.

في هذا الباب ، سوف نستكشف بعض تقنيات التحسين التي توفرها بعض خدمات التخزين السحابية لتوفير عرض النطاق الترددي. تقنيات التحسين هذه هي: إلغاء التكرار وترميز دلتا وضغط.

1. اعادة الازدواجية

يصف مصطلح اعادة الازدواجية تقنية شائعة تسمح لمقدمي خدمات التخزين السحابية بتقليل مساحة التخزين المطلوبة بشكل كبير. مبدأ إلغاء الازدواجية كما يلي: يتم تخزين نسخة واحدة فقط من كل جزء من البيانات. إذا أراد المستخدم تخزين البيانات التي قام موفر التخزين السحابية بتخزينها بالفعل في الماضي، فسيقوم موفر التخزين ببساطة بإنشاء رابط لتلك البيانات بدلاً من تخزين نسخة أخرى. هناك بعض الاختلافات في كيفية تحقيق إلغاء التكرار: بمعنى آخر، فإن إلغاء التكرار هو تقنية يتم استخدامها بشكل متكرر من قبل موفري التخزين السحابية. تعمل هذه التقنية فقط عن طريق الاحتفاظ بنسخة واحدة من كل جزء من البيانات المخزنة وإذا كان المستخدم يريد تخزين بيانات مخزنة بالفعل، يقوم المزود فقط بإنشاء رابط لهذه البيانات بدلاً من تخزين نسخة أخرى. باستخدام هذه التقنية، يمكن لموفري التخزين السحابية تقليل مساحة التخزين اللازمة لتخزين بيانات المستخدم بشكل كبير. يمكن أن يتخذ إلغاء الازدواجية أشكالًا عديدة كما سنوضحها في الأسطر التالية. [63] ، [64]

(1) إلغاء ازدواجية مستوى الملف مقابل ازدواج مستوى الكتلة.

(2) إلغاء ازدواج جانب الخادم مقابل إلغاء ازدواج جانب العميل.

(3) إلغاء ازدواج مستخدم واحد مقابل إلغاء ازدواج المستخدم.

2. ترميز دلتا

ترميز دلتا هو تقنية تستخدم لتقليل نقل البيانات، وبالتالي توفير عرض النطاق الترددي. إنه يعمل فقط عن طريق تحميل الاختلافات إلى الملف الذي تم تحميله من التغيير الأخير بدلاً من إرسال الملف بالكامل مع التعديلات الجديدة. افترض أن المستخدم يعدل ملفًا معينًا ويريد تخزينه. في هذه الحالة،

بدلاً من تحميل الملف المعدل الجديد، سيكون كافياً إذا قمنا بتخزين التعديلات فقط (فقط أجزاء المتجر التي تم تعديلها). من المهم أن نلاحظ أن تشفير دلتا لا معنى له مع البيانات المشفرة لأن ملف مشفر مع التعديل يختلف تماما عن الملف المشفر دون تعديل [58].

3.ضغط

الضغط هو أسلوب يستخدم لحفظ النطاق الترددي. وهو يعمل عن طريق ضغط البيانات على جانب العميل. العيب الرئيسي لهذه التقنية هو أنها تستهلك القدرة الحاسوبية للمستخدم، وهذا قد يسبب مشاكل للمستخدمين لأن نقل البيانات إلى السحابة هو عملية مستمرة [63].

3.2 النماذج الأمنية وعلاقاتها مع الحوسبة السحابية.

في البيئة السحابية، تثار العديد من التهديدات وتعد سلامة البيانات أحد التهديدات الرئيسية حيث يجب أن تحتفظ البيانات بمحتوياتها ويجب عدم تعديلها أو تغييرها عن طريق الخطأ أو عن قصد. اقترح الباحثون نماذج وتقنيات مختلفة لتقليل فشل سلامة بيانات التهديدات واختبار سلامة البيانات في سحابة.في هذا الباب سوف نقدم العديد من الدراسات ذات الصلة وفقا لي

1. النماذج الأمنية
2. تدبير الأمان للتخزين في السحابة للحفاظ على سلامة البيانات.
3. تقنيات التحقق من سلامة البيانات.
4. الطرف الثالث يتحقق.
5. نماذج للكشف عن انتهاك تكامل البيانات

1.3.2 النماذج الامنية.

النماذج الأمنية مي إطار يتم فيه تطوير سياسة الامان[68] سنناقش مجموعات من النماذج الرياضية لأمن الكمبيوتر الذي يخدم عدة غرض.يتم استخدام المجموعة الأولى من النماذج لتحديد الظروف التي يمكن للمرء فيها إثبات أنواع الأنظمة الآمنة مثل نموذج مصفوفة التحكم في الوصول. يصف النوع الثاني من النموذج كيفية تطبيق نظام الكمبيوتر على عناصر التحكم مثل نموذج التحكم

في الوصول الإلزامي ونموذج التحكم في الوصول التقديري. النوع الثالث من النماذج يصف السرية والنزاهة مثل نموذجBell–LaPadula ، ونموذجClark–Wilson ، وما إلى ذلك. والنوع الرابع من النموذج هو النموذج المختلط الذي يتخلل نموذج الجدار الصيني الذي يضم مزيجًا من متطلبات السرية والنزاهة[69].

1. النماذج والأمن

المعنى الدقيق لكل حق يختلف من نظام فعلي إلى نظام، والنماذج المذكورة أدناه هي أمثلة.

أ- **نموذج مصفوفة التحكم في الوصول: " Access-Control Matrix Model "**قد يكون نموذج مصفوفة التحكم في الوصول هو أبسط نموذج في أمان الكمبيوتر. يتكون من مصفوفة، تتوافق الصفوف مع الموضوعات والأعمدة التي تتوافق مع الكيانات (الموضوعات والكائنات). يحتوي كل إدخال في المصفوفة على مجموعة من الحقوق التي يتمتع بها الموضوع (الصف) على الكيان (العمود). تلتقط مصفوفة التحكم في الوصول حالة حماية للنظام. لكن النظم تتطور حالة حمايتهم لا تبقى ثابتة. لذلك يجب تغيير محتويات مصفوفة التحكم في الوصول لتعكس هذا التطور. توفر مصفوفة التحكم في الوصول أساسًا نظريًا لآليتي أمان مستخدمتين على نطاق واسع: قوائم التحكم في الوصول وقوائم القدرة. في مجال النموذجة، يوفر أداة لتحليل صعوبة تحديد مدى أمان النظام. [69]

ب- **هاريسون، رزو، أولمان ونتائج أخرى: "Ullman and Ruzzo،Harrison**" إن مسألة كيفية اختبار ما إذا كانت الأنظمة آمنة أمر بالغ الأهمية لفهم أمان الكمبيوتر[72].

ت- **نموذج التحكم في الوصول المكتوب: " Typed Access–Control Model** "يضيف متغير نموذج مصفوفة التحكم في الوصول الكتابة إلى الكيانات. يربط نموذج مصفوفة التحكم في الوصول، المسمىTAM ، نوعًا ما بكل كيان ويعدل قواعد معالجة المصفوفة وفقًا لذل. [72].

2.النماذج والتحكم في الوصول.

تركز نماذج أمان الكمبيوتر على التحكم (من يمكنه الوصول إلى الملفات والموارد وأنواع الوصول المسموح بها). النماذج المذكورة أدناه هي أمثلة.

أ- **نماذج التحكم في الوصول الإلزامية والتقديرية:** "Mandatory and Discretionary Access-Control Models" تستند بعض أساليب التحكم في الوصول إلى القواعد؛ وهذا هو، المستخدمين ليس لديهم السيطرة عليها. لا يمكن تغييرها إلا النظام أو مستخدم خاص يسمى (على سبيل المثال) مسؤول أمان النظام ."SSO" التحكم الإلزامي في الوصول "MAC" هو الأكثر صرامة على جميع مستويات التحكم. تم تحديد تصميم"MAC" ، ويستخدم بشكل أساسي من قبل الحكومة. تتبع"MAC" نهجًا هرميًا للتحكم في الوصول إلى الموارد. تحت بيئة "MAC" المفروضة، يتم التحكم في الوصول إلى جميع كائنات الموارد (مثل ملفات البيانات) من خلال الإعدادات التي يحددها مسؤول النظام. على هذا النحو، يتم التحكم في الوصول إلى كائنات الموارد بشكل صارم بواسطة نظام التشغيل استنادًا إلى إعدادات تكوين مسؤول النظام. لا يمكن للمستخدمين، بموجب تطبيق"MAC" ، تغيير التحكم في الوصول لمورد ما. بخلاف التحكم الإلزامي في الوصول "MAC" حيث يتم التحكم في الوصول إلى موارد النظام بواسطة نظام التشغيل (تحت سيطرة مسؤول النظام)، يسمح التحكم في الوصول التقديري "DAC" لكل مستخدم بالتحكم في الوصول إلى البيانات الخاصة به. عادةً ما تكون "DAC" هي آلية التحكم في الوصول الافتراضية لمعظم أنظمة تشغيل سطح المكتب. [69]

ب- **نموذج التحكم في الوصول الذي يتم التحكم فيه في المنشئ وDRM :" Originator-Controlled Access-Control Model and DRM**" تحتوي الأنواع الأخرى من عناصر التحكم في الوصول على عناصر من عناصر التحكم في الوصول الإلزامي وتقديري. تسمح أداة التحكم في الوصول التي يتحكم بها المنشئ، أوORCON ، لآلية المنشئ بتحديد من يمكنه الوصول إلى مورد أو بيانات.

ت- **نماذج ومجموعات التحكم في الوصول القائمة على الدور:** يقدم " **Role-Based Access-Control Models and Groups**" التحكم في الوصول بناءً على القواعد "RBAC"غموضًا مختصرًا باستخدام نفس اختصار الأحرف الأربعة "RBAC" كمحكم في الوصول إلى الدور.ضمن التحكم في الوصول المستند إلى القواعد، يُسمح بالوصول أو يرفض الوصول إلى كائنات الموارد استنادًا إلى مجموعة من القواعد التي يحددها مسؤول النظام. كما هو الحال مع التحكم في الوصول التقديري، يتم تخزين خصائص الوصول في قوائم التحكم في

الوصول "ACL–Access control list" المرتبطة بكل كائن مورد. عندما يحاول حساب أو مجموعة معينة الوصول إلى مورد، يتحقق نظام التشغيل من القواعد الموجودة في قائمة التحكم في الوصول "ACL" لهذا الكائن[69].

3. النماذج الكلاسيكية

لعبت ثلاثة نماذج دورًا مهمًا في تطوير أمان الكمبيوتر. أثر نموذج Bell–LaPadula، وهو أحد النماذج الرسمية الأولى في أمان الحاسوب، على تطوير الكثير من تقنيات أمان الحاسوب، ولا يزال قيد الاستخدام على نطاق واسع Biba .، التناظرية للتكامل البيانات ، تلعب الآن دورا هاما في تحليل البرنامج. يصف نموذج كلارك ويلسون العديد من الممارسات التجارية للحفاظ على سلامة البيانات.

أ- **نموذج بيل لابادولا:** يتعامل نظام"Bell–Lapadula Model" لأنظمة الحماية مع التحكم في تدفق المعلومات. إنه نموذج خطي غير تقديري. يتكون نموذج الحماية هذا من مجموعة من الموضوعات ومجموعة من الكائنات ومصفوفة التحكم في الوصول والعديد من مستويات الأمان المطلوبة. كل موضوع له خلوص ولكل كائن تصنيف يربطه بمستوى أمان. كل موضوع لديه أيضا مستوى التخليص الحالي الذي لا يتجاوز مستوى التخليص. وبالتالي، يمكن أن يتغير الموضوع فقط إلى مستوى التخليص أسفل مستوى التخليص المخصص له. مجموعة حقوق الوصول الممنوحة لموضوع ما هي للقراءة فقط أو إلحاق أو تنفيذ أو للقراءة والكتابة. سمة التحكم هي سمة تعطى للموضوع الذي ينشئ كائنًا. وبسبب هذا، يمكن لمنشئ كائن تمرير أي من حقوق الوصول الأربعة لهذا الكائن إلى أي موضوع. ومع ذلك، لا يمكن تمرير سمة التحكم نفسها. يُعرف منشئ كائن ما أيضًا باسم وحدة التحكم في هذا الكائ "Bell–Lapadula Model" فرض القيود التالية بالقراءة مما يعني أن الموضوع له حق الوصول للقراءة فقط إلى الكائنات التي يكون مستوى أمانها أقل من مستوى التخليص الحالي للموضوع. هذا يمنع أي شخص من الوصول إلى المعلومات المتاحة في مستويات الأمان أعلى من مستوى التخليص الحالي والكتابة مما يعني أن الموضوع قد ألحق الوصول إلى الكائنات التي يكون مستوى أمانها

أعلى من مستوى التخليص الحالي. هذا يمنع الموضوع من نقل المعلومات إلى مستويات أقل من مستواه الحالي. [70]

ب- **نموذج سياسة بيبا للنزاهة الصارمة:** يعالج نموذج بيبا "**Bibas Strict Integrity Policy Model**" مسألة التكامل البيانات، أي ما إذا كانت المعلومات يمكن أن تتلف. يتم استخدام تسمية جديدة لقياس النزاهة. في حالة ملامسة كائن عالي الأمان لمعلومات ذات مستوى منخفض، أو يمكن معالجتها بواسطة برنامج منخفض المستوى، يمكن خفض مستوى التكامل. على سبيل المثال، إذا استخدم أحدهم برنامجًا غير آمن لعرض مستند آمن، فقد يقوم البرنامج بنسخه سرا إلى جزء آخر من النظام. يتم تجميع البيانات والموضوعات في مستويات مرتبة من النزاهة. تم تصميم النموذج بحيث لا يمكن أن تتلف المواد في مستوى أعلى مرتبة من الموضوع، أو قد تتلف بواسطة بيانات من مستوى أدنى من الموضوع[72]، [71]. تتميز النزاهة عادة بالأهداف التالية للشجرة:

a. البيانات محمية من أي تعديل من قبل المستخدمين غير المصرح لهم.
b. البيانات محمية من التعديل غير المصرح به من قبل المستخدمين المعتمدين (مما يثير السؤال –ما هو التعديل غير المصرح به؛ على سبيل المثال بالنسبة للسجلات، يتم حذف أو تغيير السجلات، بينما يُسمح بإضافة السجلات).
c. البيانات متسقة داخليا وخارجيا. مرة أخرى شيء عن سلامة سجلات كمثال.

ت- **كلارك ويلسون النموذجي:** بدلاً من التعامل مع سرية المستندات و / أو تكامل البيانات، يتعامل نموذج"Clark–Wilson (CW)" مع الأنظمة التي تؤدي المعاملات. ويصف آليات لضمان أن سلامة مثل هذا يتم الحفاظ على النظام عبر تنفيذ الصفقة. تشمل المكونات الرئيسية لنموذج الأسلحة الكيميائية ما يلي:

a. قيود النزاهة التي تعبر عن العلاقات بين الكائنات التي يجب الوفاء بها حتى تكون حالة النظام صالحة.
b. طرق التصديق التي تتحقق من أن المعاملات تلبي قيود السلامة المحددة.
c. فصل قواعد الواجب التي تمنع المستخدم الذي ينفذ المعاملة من التصديق عليها. [72]

ث- **نموذج الجدار الصيني:** تم تصميم نموذج Brewer وNash، والذي يشار إليه عادة باسم نموذج الجدار الصيني، للاستخدام في القطاع التجاري للقضاء على إمكانية تضارب المصالح. لتحقيق ذلك، يقوم النموذج بتجميع الموارد في "فئات تعارض المصالح". يفرض النموذج التقييد الذي يقضي بأن كل مستخدم يمكنه الوصول إلى مورد واحد فقط من كل فئة تعارض في الفائدة. قد يتم تنفيذ هذه السياسة على أنظمة الكمبيوتر لتنظيم وصول المستخدمين إلى البيانات الحساسة أو الخاصة[72]

4. نماذج أخرى

بعض النماذج تدرس بيئات معينة. يأخذ نموذج أمن نظم المعلومات السريرية في الاعتبار حماية السجلات الصحية، مع التركيز على المساءلة والسرية والنزاهة. يصف تراث عملية التسجيل العقاري، الأمر الذي يتطلب تعريفًا صارمًا للنزاهة والمساءلة دون أي قدر يذكر من السرية. نماذج أخرى تعميم النماذج الكلاسيكية. أشهرها هي نماذج الأمن وعدم التدخل وأمن الاستنتاج. كلاهما نماذج أمان متعددة المستويات مع مستويين، "HIGH" عالية ومنخفضة "LOW ". يعرّف نموذج عدم التدخل الأمان بأنه قدرة "HIGH" عالية تخضع للتداخل مع ما يراه موضوع "LOW" منخفض. [72]

2.3.2 تدابير أمنية للتخزين في السحابة للحفاظ على سلامة البيانات

[48] اقترح حماية ثلاثية الطبقات للحفاظ على تكامل البيانات في السحابة، الطبقة (1): توثق المستخدم، الطبقة (2): تشفير بيانات المستخدم، الطبقة (3): استعادة بيانات المستخدم، أطلقوا هذا الدفاع الأول والثاني والثالث، واستخدموا خوارزمية "3DES" لتشفير البيانات وخوارزمية "SHA1" لتكامل البيانات والأمن متعدد المستويات لتأمين البيانات.

[49] ذكر أيضًا أنه للحفاظ على أمان البيانات ، يجب استخدام أساليب الحماية التالية: استخدام التوقيع الرقمي ، واستخدام فك تشفير داخل المعالج ، واستخدام معايير "API" ، وتطبيق تقييد الوصول إلى المعلومات الحساسة ، وتطبيق أدوات المراقبة والنسخ الاحتياطي للبيانات.

3.3.2 تقنيات التحقق من سلامة البيانات.

[43] حيازة البيانات المزودة المقترحة ، يتحقق بروتوكول"PDP" من أن موقع تخزين خارجيًا يحتفظ بملف يتكون من مجموعة من القطع. يقوم العميل بمعالجة الملف مسبقًا، وإنشاء جزء من البيانات التعريفية (المفتاح العام والسري) باستخدام خوارزمية توليد المفاتيح الاحتمالية ويتم تخزينه محليًا قبل نقل الملف إلى السحابة. يتم إرسال المفتاح العام مع الملف إلى الخادم، ويقوم الخادم بتخزين الملف ويستجيب للتحديات التي يصدرها العميل. يصدر العميل تحديا للخادم لإثبات أن الخادم احتفظ بالملف. يطلب العميل أن يحسب الخادم وظيفة الملف المخزن، وبالتالي يقوم العميل بمقارنة نسخة الوظيفة من الخادم والبيانات التعريفية المحلية الخاصة به، إذا كانت تتوافق وهذا يعني أن التكامل لم يحدث، فإن عيب [43] هو أنها لا تتعامل مع البيانات الديناميكية والخصوصية لا تعتبر عالية.

4.3.2 تحقق الطرف الثالث.

[50] اقترح نموذجًا يستخدم الجهة الخارجية "TPA" ، في هذا النموذج ، يقوم مالك البيانات بتحميل الملفات إلى الخادم السحابية ، عندما يكون العميل جاهزًا للحصول على الملف من السحابة ، حيث يقوم مالك البيانات بتعيين فحص تدقيق للعميل ، السحابة يرسل الخادم الملفات إلى "TPA" ويرسل طلبًا لمراجعة تكامل البيانات ، ويقوم 'TPA' بمراجعة تكامل البيانات ويرسل النتائج إلى الخادم السحابية ومالك البيانات ، ويستخدم النظام مزيجًا من "RSA" و "MD5" لتشفير وفك تشفير البيانات حيث "MD5" يستخدم بشكل أساسي لفحص تكامل البيانات و "RSA" للتشفير قبل تحميل الملفات. أثناء استخدام "TPA"، هناك خوف من أنه قد يتسبب في مزيد من تعرض البيانات ولا يجب أن يسبب نقاط ضعف جديدة لسرية بيانات المستخدم [47]، [48]، [49]، [50].

طورت ماي منصور [14] إطارًا أمنيًا للتخزين السحابية، حيث صمموا في بحثهم إطارًا آمنًا لنظام التخزين السحابية يحقق في وقت واحد سرية البيانات والتحكم في الوصول الدقيق على البيانات المشفرة وإلغاء المستخدم القابل للتطوير. تم بناء الإطار على خدمة موثوق بها "TTP" تابعة لجهة خارجية والتي يمكن استخدامها إما محليًا على جهاز المستخدمين أو أماكن عملهم، أو عن بعد على خدمات التخزين السحابية. تقوم الخدمة بتشفير بيانات المستخدمين قبل تحميلها على السحابة وفك تشفيرها بعد التنزيل من السحابة؛ لذلك، فإنه يزيل عبء تخزين وإدارة وصيانة مفاتيح التشفير / فك

التشفير من مالك البيانات. بالإضافة إلى ذلك، تحتفظ هذه الخدمة فقط بالمفتاح (المفاتيح) السري للمستخدم وليس البيانات. علاوة على ذلك، لضمان الأمان العالي لهذه المفاتيح، يقوم بتخزينها على الأجهزة. علاوة على ذلك، تجمع هذه الخدمة بين التشفير القائم على سمات سياسة نص التشفير متعدد المصادر "CP−ABE" والتوقيع المعتمد على السمة "ABS−Attribute based signature" لتحقيق العديد من التحكم في الوصول إلى البيانات المحبب بدقة في خدمات التخزين. علاوة على ذلك، فإنه يلغي بفعالية امتيازات المستخدمين دون الاعتماد على مالك البيانات لإعادة تشفير كميات هائلة من البيانات وإعادة توزيع المفاتيح الجديدة على المستخدمين المصرح لهم. يزيل الحساب الكثيف لإعادة التشفير من المستخدمين ويفوض هذه المهمة إلى خوادم بروكسي موفر الخدمة السحابية (CSP). تحقق خوادم بروكسي هذه إعادة تشفير مرنة وفعالة دون الكشف عن البيانات الأساسية إلى السحابة.

5.3.2 نماذج للكشف عن انتهاك تكامل البيانات

اقترح طاهر [51] نموذجًا لاكتشاف انتهاك سلامة الملفات المشتركة، وفي هذا البحث ذكروا أن معظم حلول مشكلة تكامل البيانات في السحابة هي فقط حلول لملفات البيانات الثابتة ولا تدعم تشغيل البيانات الديناميكي أو لا تدعم مشاركة الملفات. في هذا النموذج، يتضمن كشف تكامل البيانات منطقتين، المخاوف من خارج السحابة والمخاوف من الاستخدام غير المصرح به من المستخدمين الداخليين. يحتوي النموذج المقترح على نظام وسيط للكشف عن انتهاك سلامة الملف عن طريق تجزئة الملف قبل حفظه على السحابة وبعد استعادته، ثم يقارن قيمتي هاش. يدعم النموذج المقترح تشغيل البيانات الديناميكي على الملفات المشتركة، بما في ذلك الإلحاق والتحديث والحذف. أيضًا، ركز النموذج على كيفية الحفاظ على تشغيل العمليات الديناميكية بطريقة التزامن، بحيث لا يمكن لأي مستخدم تعارض عمل مستخدم آخر على ملف مشترك. يحتوي النموذج على نظام وسيط للكشف عن انتهاك تكامل الملف عن طريق تجزئة أجزاء من الملف، باستخدام خوارزمية SHA−256، قبل حفظه على السحابة وبعد استعادتها، ثم مقارنة قيمتي هاش، إذا كانت متطابقة، فهناك لا توجد مشكلة، وإلا انتهكت السلامة وظهرت رسالة تنبيه.

وأخيرًا، أجروا تجارب على سحابة خاصة بأحجام ملفات مختلفة (.doc) تتراوح (من 13 كيلو بايت إلى 5 ميجابايت) لضمان القدرة على اكتشاف انتهاك سلامة البيانات، ولتقييم الدقة والتزامن، وأثبتت

عملية تقييمهم أن طرازهم قد تم يتم إجراؤه بمستوى مقبول وفعال للغاية ضد هجوم تعديل البيانات الضارة. وأوصوا بتحديث نموذجهم في الأبحاث المستقبلية لدعم أنواع مختلفة من الملفات (الصورة والصوت والفيديو) وإجراء فحص دوري للملفات الأقل استخدامًا في السحابة، للكشف عن انتهاك سلامتهم.

أجرى [52] بحثًا عن التحقق من سلامة البيانات في السحابة حيث اقترحوا نموذجًا يستخدم خدمات البنية التحتية والنظام الأساسي، وتم تحديد ثلاثة كائنات للنموذج المعماري وهي مالك البيانات أو المستخدمين أو العملاء ومزود الخدمة السحابية الذي تم نشره على سحابة خاصة. كان التركيز الرئيسي لهذا البحث هو تحديد طريقة لمعالجة كيفية توحيد البيانات الخاصة أو البيانات الحقيقية وكيفية الإشراف عليها من أجل اكتشاف تحديث البيانات المؤذية. تحدد هذه الطريقة بعض بيانات التحكم للتعرف على تحديثات البيانات في حالة قيام مستخدم غير مصرح له بتغيير البيانات، ومن أجل التحقق من سلامة البيانات الحقيقية المدمجة، قاموا بإنشاء بيانات تعريف (يتم الاحتفاظ بها كنص مشفر) وجدول يقوم بتخزين المعلومات حول جميع عناصر البيانات الحساسة كنص عادي. من أجل توليد قيمة تجزئة، استخدموا دالة تجزئة التشفير SHA-512. وقاموس بيانات لتخزين بيانات التعريف. باستخدام المحاكاة، أثبتوا أن الطريقة فعالة حيث أنه عند زيادة عدد الأقسام، يكون هناك انخفاض في وقت المعالجة.

في اقتراحنا، سوف نستخدم توثق المستخدم وتشفير البيانات واستعادة البيانات والنسخ الاحتياطية لتعزيز نموذجنا، وسوف نبني نموذجًا مشابهًا للتحقق من تكامل البيانات مثل [51] Tahir و Katanosh [52] باستخدام" SHA3 وAES وRSA" وسوف دعم أنواع الملفات المتعددة مثل الصور والفيديو. حيث يمكن للمستخدمين المصرح لهم فقط تحميل الملفات والوصول إليها، وسيتم إرسال الإشعارات عند اكتشاف الانتهاك. سوف يدعم نموذجنا أيضًا التحقق بشكل دوري من الملفات الأقل استخدامًا في السحابة، كما سيتطلب النموذج من السحابة عمل نسخ احتياطية متعددة من الملفات.

ملخص

ناقشنا في هذا الفصل نظرة عامة على الحوسبة السحابية التي تتضمن تعريفها وخصائصها ونماذج التسليم والنشر، والفوائد، والمخاطر، والعقبات التي تحول دون اعتماد الحوسبة السحابية،

والعوامل التي تؤثر على الأداء والهندسة المعمارية للحوسبة السحابية. كما شاهدنا مدى الأمان في الحوسبة السحابية ومشكلات التهديدات الأمنية السحابية والأهداف والمتطلبات الأمنية تكامل البيانات في الحوسبة السحابية والحل السحابية الحالي للأمان. أخيرًا، ناقشنا مبادئ خدمات التخزين السحابية، والواجهات المستخدمة لخدمات التخزين السحابية والتحسين في خدمات التخزين السحابية والنماذج الأمنية وعلاقتها مع الحوسبة السحابية ثم تلاولنا بعض النكاذج الأمنية وعلاقاتها مع الحوسبة السحابة.

الفصل الثالث

التحليل

3. مقدمة

نقدم تحليل النموذج ووصفه مع بعض الأمثلة على كيفية عمل هذا النموذج. كما نقدم تصميم النموذج.

1.3 التحليل

الملفات التي تمت مشاركتها أو تخزينها أو معالجتها عبر الإنترنت عرضة للهجمات حيث لا يعتبر الإنترنت آمنًا تمامًا، وكما نوقش في الفصل الثاني، قد تتأثر سلامة الملف بسبب أسباب مختلفة مثل هجمات القراصنة التي يمكن أن تكون هجمات توثق أو المطلعين الخبيثة وما إلى ذلك، وهذا يشكل خوفًا على المستخدم، حيث يقوم موفر السحابة الموجود على جانبه بكل ما في وسعه لمنع وقوع هجمات كهذه ويخبر المستخدمين أن البيانات يتم حفظها بشكل آمن.

2.3 تحليل نمازج تكامل البيانات في الحوسبة السحابية

في هذا الباب سنقوم بتحليل ثلاثة نماذج لتكامل البيانات في الحوسبة السحابية ونطلع على مميزاتهم وعيوبهم والهجمات التي تقاومها والهجمات التي لا تقاومها. النماذج الثلاثة هي:

1. [51] صفاء طاهر لولو، "نموذج لاكتشاف انتهاك النزاهة للملف المشترك في السحابة".
2. [52] موروفات كاتانوش ، "التحقق من تكامل البيانات في الحوسبة السحابية"
3. [48] أنانتوار وآخرون ، "تكامل البيانات والأمن في السحابة".

1.2.3 مميزات النماذج

1. من المميزات النموذج[51] هو انه يدعم الملفات الديناميكيا ومشاركة الملفات بما في ذلك الإلحاق والتحديث والحذف. أيضًا ركز النموذج على كيفية الحفاظ على تشغيل العمليات الديناميكية بطريقة التزامن، بحيث لا يمكن لأي مستخدم تعارض عمل مستخدم آخر على ملف مشترك. يحتوي النموذج على نظام وسيط للكشف عن انتهاك تكامل الملف عن طريق تجزئة أجزاء من الملف، باستخدام خوارزمية "SHA-256"، قبل حفظه على السحابة وبعد استعادتها.

2. من المميزات النموذج [52]هو انه يستخدم خدمات البنية التحتية والنظام الأساسي، وتم تحديد ثلاثة كائنات للنموذج المعماري وهي مالك البيانات أو المستخدمين أو العملاء ومزود الخدمة السحابية الذي تم نشره على سحابة خاصة. تحدد هذه الطريقة بعض بيانات التحكم للتعرف على تحديثات البيانات في حالة قيام مستخدم غير مصرح له بتغيير البيانات، ومن أجل التحقق من سلامة البيانات الحقيقية المدمجة، قاموا بإنشاء بيانات تعريف (يتم الاحتفاظ بها كنص مشفر) وجدول يقوم بتخزين المعلومات حول جميع عناصر البيانات الحساسة كنص عادي. من أجل توليد قيمة تجزئة، استخدموا دالة تجزئة التشفير "SHA-512", وقاموس بيانات لتخزين بيانات التعريف. ومن مميزاته هو انه عند زيادة عدد الأقسام، يكون هناك انخفاض في وقت المعالجة.

3. من المميزات النموذج [48]هو انه حدد ثلاث الطبقات للحفاظ على تكامل البيانات في السحابة.

2.2.3 عيوب النماذج

من العيوب للنماذج [52]،[51] هو انه يستخدم "SHA-512" للتجزئة والتي هو قديم وقد تثبت انه قابل للاصطدام. ومن عيوبهما هو انهما لا تحتفظ قيمة هاش مشفرة. في اقتراحنا، سوف نستخدم مصادقة المستخدم وتشفير البيانات واستعادة البيانات والنسخ الاحتياطية لتعزيز نموذجنا، وسوف نبني نموذجًا مشابهًا للتحقق من تكامل البيانات مثل Tahir [51] وKatanosh [52] باستخدام "SHA3 وAES وRSA" وسوف دعم أنواع الملفات المتعددة مثل الصور والفيديو. حيث يمكن للمستخدمين المصرح لهم فقط تحميل الملفات والوصول إليها، وسيتم إرسال الإشعارات عند اكتشاف الانتهاك. سوف يدعم نموذجنا أيضًا التحقق بشكل دوري من الملفات الأقل استخدامًا في السحابة، كما سيتطلب النموذج من السحابة عمل نسخ احتياطية متعددة من الملفات.

3.2.3 الهجمات التي تقاومها

النماذج[52]،[51] تقاوم من الهجمات على تكامل البيانات من حيث يمكن اكتشافه إذا تم تعديل او مسح محتويات الملف.

4.2.3 الهجمات التي لا تقاومها

النماذج[52]،[51] لا تقاوم من كل هجمات المصادقة مثل الهجمات القوة الغاشمة وهجمات رجل في منتصف إلى آخره.يعرض جدول 1.3 ملخصا للنماذج التي تم تحليلها.

	دراسة أنانتوار[48]	دراسة كاتانوش[52]	دراسة صفاء[51]
مميزات النماذج	حدد ثلاث الطبقات للحفاظ على تكامل البيانات في السحابة 1.التوثق المستخدم 2.تشفير البيانات 3.استرجاع البيانات	استدم تجزئة للكشف عن انتهاك تكامل الملف	1.استدم تجزئة للكشف عن انتهاك تكامل الملف 2. يدعم الملفات الديناميكيا ومشاركة
عيوب النماذج	لا توجد نموذج واضح,هو مجرد طبقة من الامن	1.استدم تجزئة SHA 512 وقد تثبت انه قابل للاصطدام (collision) 2. لا تحتفظ قيمة التجزئة مشفرة عند المتخدم	
الهجمات التي تقاومها		تقاوم من الهجمات على تكامل البيانات من حيث يمكن اكتشافه إذا تم تعديل او مسح محتويات الملف.	
الهجمات التي لا تقاومه	لا تقاوم من كل هجمات المصادقة المستخدم مثل الهجمات القوة الغاشمة وهجمات رجل في منتصف إلى آخره.		

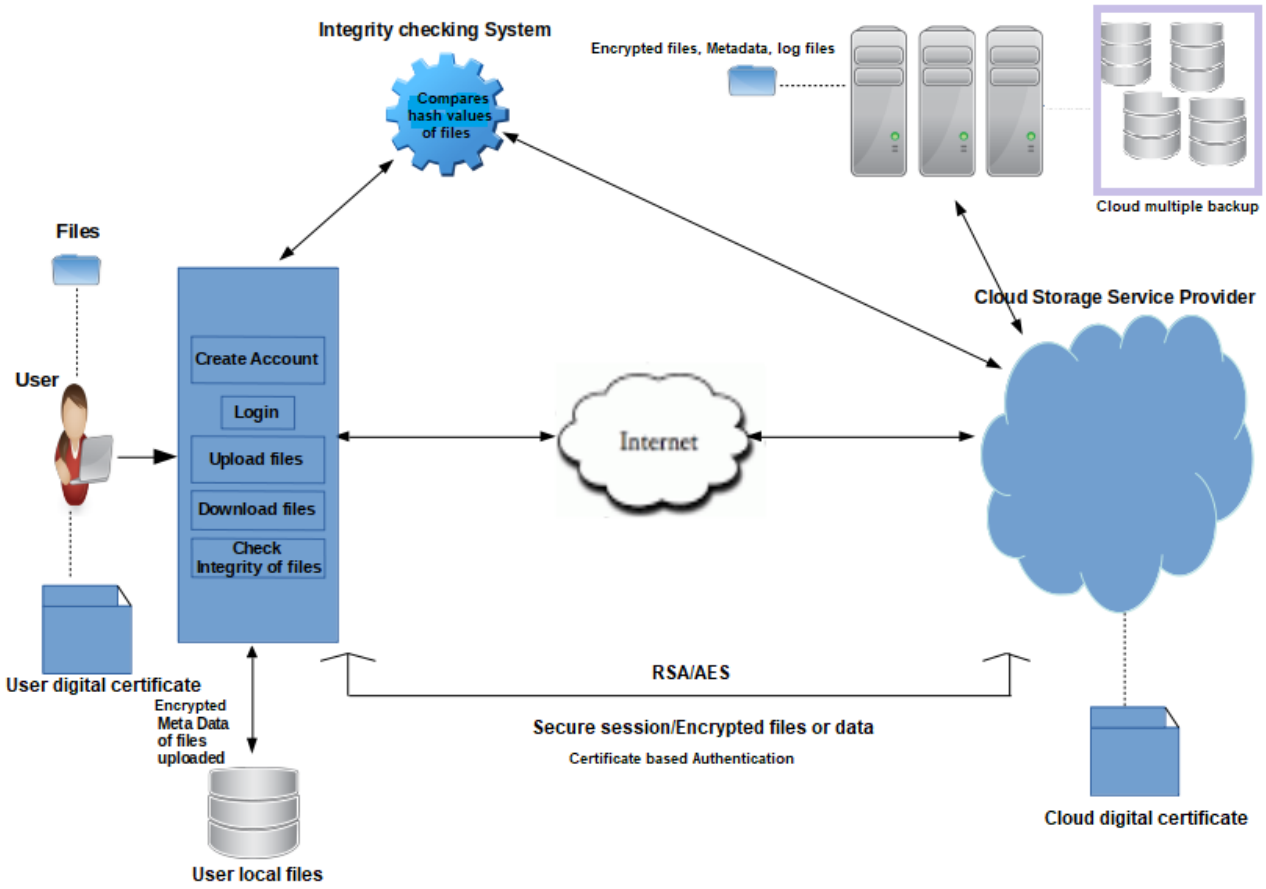
الجدول (1.3): تحليل نماذج

5.2.3 النموذج المقترح

في هذا البحث، يعمل نموذجنا على حل مشكلات الفشل في تكامل البيانات من خلال إنشاء نظام قوي للتوثق المستخدم وتحميل آمن للملفات، مما سيمكن المستخدمين من التحقق من سلامة ملفاتهم الخارجية بسهولة.

باختصار، يحتوي نموذجنا على نظام توثق المستخدم حيث يتم استخدام التحقق من عاملين للتوثق والذي يتضمن اسم المستخدم / كلمة المرور والتوثق المستندة إلى الشهادة، ويتم إرسال الملفات وحفظها إلى السحابة عبر جلسة آمنة حيث يتم تشفير الملفات والبيانات باستخدام "AES" ونظام تشفير "RSA". في حالة وصول العديد من المستخدمين إلى الملف، يتم فرض التفويض من خلال منح إذن

لكل مستخدم. تُستخدم ملفات السجل لحفظ كل عملية تتم على ملف. يغطي نموذجنا المقترح أهم الجوانب التي يمكن أن تؤدي إلى فشل في سلامة البيانات. يوضح الشكل 1.3 الفكرة العامة للنموذج المقترح.



الشكل (1.3) الفكرة العامة للنموذج المقترح.

يعرض الشكل 1.4 النموذج المقترح والذي يتضمن ما يلي:

1. **المستخدمون:** هو المستخدم الذي يرغب في استخدام نظام السحاب لتخزين ملفه ، ولكل منهم حسابه الخاص في النظام.
2. **نظام التوثق:** يصادق نظام التوثق على صحة المستخدم باستخدام التحقق من عاملين (التوقيع الرقمي وكلمة المرور) ، ويغطي نظام التوثق صفحة التسجيل وتسجيل الدخول.

3. **ملفات السجل:** يخزن كل عملية على البيانات في التخزين السحابية ، ويخزن التفاصيل مثل (اسم الممثل الذي وصل إلى الملف ، التاريخ / الوقت ، الاسم ، المعرف ، حجم الملف ، الإجراء الذي تم تنفيذه على الملف (التحميل ، التنزيل ، التحديث ، حذف) الخ

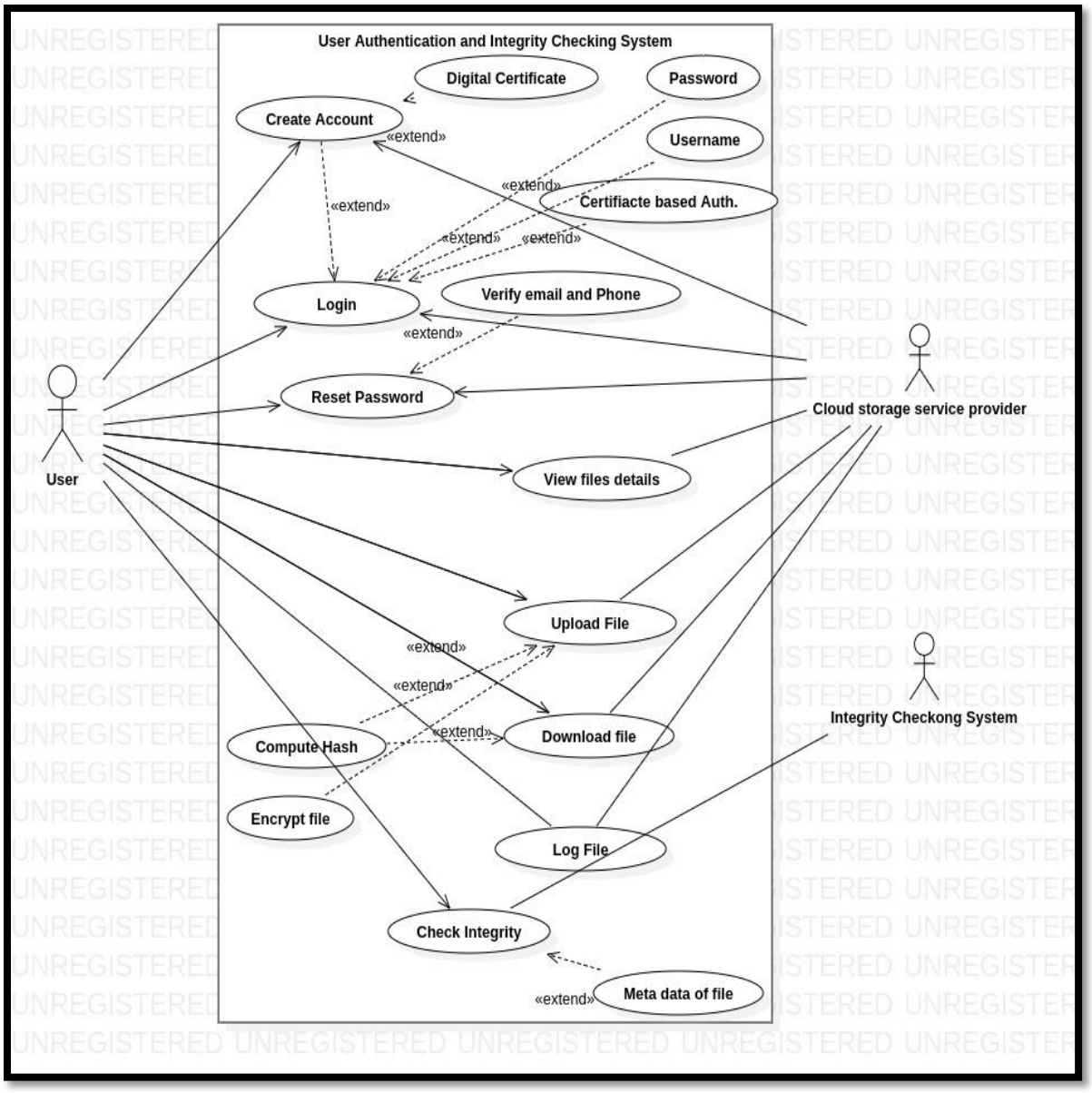
4. **تحميل الملفات**: يسمح للمستخدم بتحميل ملفه بعد التحقق من هويته في نظام التوثق ، لتحميل الملف ، يتم تشفير الملف باستخدام نظام تشفير "RSA (Rijindel)" و "AES" ، كما يتم إنشاء قيمة تجزئة الملف باستخدام نظام هاش SHA3 ثم يتم تخزينه في قاعدة بيانات المستخدمين المحلية جنبا إلى جنب مع تفاصيل حول الملف قبل الملف يتم تحميل الملف في النهاية إلى السحابة.

5. مزود خدمة التخزين السحابية: هذا هو المزود السحابية الذي يقدم خدمات بما في ذلك التخزين.

6. تنزيل الملفات: يتيح للمستخدم تنزيل ملفه بعد التحقق من هويته في نظام التوثق ، وتقوم السحابة بتشفير الملف قبل إرساله إلى المستخدم باستخدام نظام تشفير "AES" ، ثم يقوم المستخدم بفك تشفيره على واجهة التطبيق.

7. نظام فحص سلامة الملفات: يتحقق من سلامة الملفات التي تم تحميلها على السحابة من خلال مقارنة قيمة هاش "SHA3" للملف المخزن في قاعدة بيانات المستخدم المحلية وقيمة هاش لنفس الملف في السحابة.

8. الشهادة الرقمية: يتم استخدام الشهادة الرقمية للتحقق من هوية المستخدم / السحابة باستخدام التوقيع الرقمي. يوضح مخطط التدفق المعروض في الشكل(2.3) كيفية عمل النظام للتوثق المستخدمين والتحقق من سلامة الملفات.



الشكل(2.3) مخطط ا حالات لاستخدام

3.3 متطلبات الأمان

على الرغم من أن تخزين البيانات في التخزين السحابية يوفر تكلفة إدارتها وصيانتها، إلا أنها تتعرض لعدد كبير من التهديدات الأمنية. قد يتم اختراق البيانات من خلال نقلها واستخدامها والراحة. وبالتالي، عند استخدام التخزين السحابية، يجب تخفيف هذه التهديدات الأمنية. سنتناول اثنين من متطلبات أمان البيانات الرئيسية وهماس سرية البيانات وتكاملها، بينما نفترض أن توفر البيانات قد تم استيفائه.

1.3.3 سلامة البيانات

في نموذج الحوسبة السحابية، يزيد تنقل البيانات من التهديدات التي يمكن أن تؤثر على سلامة البيانات. كما يتم نقل البيانات من وإلى العميل ومزود الخدمة السحابية، وكذلك داخل السحابة. لذلك، ينبغي ضمان سلامة البيانات داخل السحابة. يمكن تعريف تكامل البيانات بأنها حماية البيانات من التعديل غير المصرح به والذي يمكن أن يحدث إما بشكل ضار أو عن طريق الخطأ أثناء معالجة البيانات أو تخزينها أو نقلها. عندما يقوم المستخدم بتحميل ملفاته، يجب أن يتأكد من استلامها في خادم السحابية عند إرسالها. يجب الكشف عن أي تعديل غير مصرح به من قبل المستخدم و / أو مزود التخزين السحابية. في هذه الأطروحة، نركز فقط على التحقق من تكامل الملفات التي تم تحميلها وتنزيلها والتأكد من أن الخادم السحابية يحفظ الملف الذي تم تحميله الصحيح.

2.3.3 سرية البيانات

تعد سرية البيانات أحد أهم جوانب أمن البيانات.يُعرّف بأنه التأكيد على عدم الكشف عن المعلومات الحساسة للمستخدمين أو العمليات أو الأجهزة غير المصرح لهم. في البيئة السحابية، يثق مالك البيانات في خدمة التخزين السحابية لإدارة بياناته، لكنه لا يريد أن تصل السحابة إلى البيانات. لذلك، نحتاج إلى التأكد من أن موفر التخزين السحابية والمستخدمين الآخرين غير المصرح لهم غير قادرين على تعلم محتوى البيانات المخزنة. بالإضافة إلى ذلك، يجب حماية المفتاح السري المستخدم للتشفير بشكل آمن حتى لا يكون من السهل التطفل أو السرقة. لذلك، ينبغي اتخاذ تدابير لحماية بيانات المستخدمين السرية من موفري الخدمات السحابية والمهاجمين الخارجيين. في هذه الأطروحة، نركز فقط على سرية البيانات للبيانات في العبور وترك البيانات قيد الاستخدام كعمل في المستقبل. [47, 48, 49]

3.3.3 توثق البيانات

تعد التوثق جانبًا مهمًا في الأمان حيث إنها مرتبطة بكل جانب من جوانب نظام الأمان، إذا كان نظام التوثق ضعيفًا، يصبح النظام بأكمله ضعيفًا.يتحقق المستخدم ماستخدام التوثق. ينبغي اتخاذ التدابير عند تنفيذ نظام التوثق. في هذا البحث، للتوثق المستخدم، نستخدم اسم المستخدم / كلمة المرور وتوقيع الرقمي.[49]

4.3 وصف للنموذج

من أجل تحقيق وظائف النموذج، سيتم اتباع خطوات منهجية النماذج الأولية:

1. **إنشاء الشهادة الرقمية:** يُطلق عليها أيضًا شهادة المفتاح العمومي "كلمة مرور" إلكترونية تحدد هوية الشخص أو المؤسسة لتبادل البيانات بشكل آمن عبر الإنترنت باستخدام البنية التحتية للمفتاح العام. قبل إنشاء المستخدم هناك حاجة لتوليد الشهادة الرقمية،

الخطوة (1) يدرج المستخدم اسمه (الأول، الأوسط، الأخير)، البريد الإلكتروني، رقم الهاتف، إلخ.

الخطوة (2) ثم يتم إنشاء أزواج المفاتيح.

الخطوة (3) يتم إنشاء التوقيع الرقمي والشهادة الرقمية.

2. **إنشاء حساب مستخدم:** لإنشاء حساب مستخدم جديد، يتم إجراء ما يلي.

الخطوة (1) إدراج المستخدم تفاصيله (اسم المستخدم وكلمة المرور ومعرف الشهادة الرقمية، وما إلى ذلك) في النموذج.

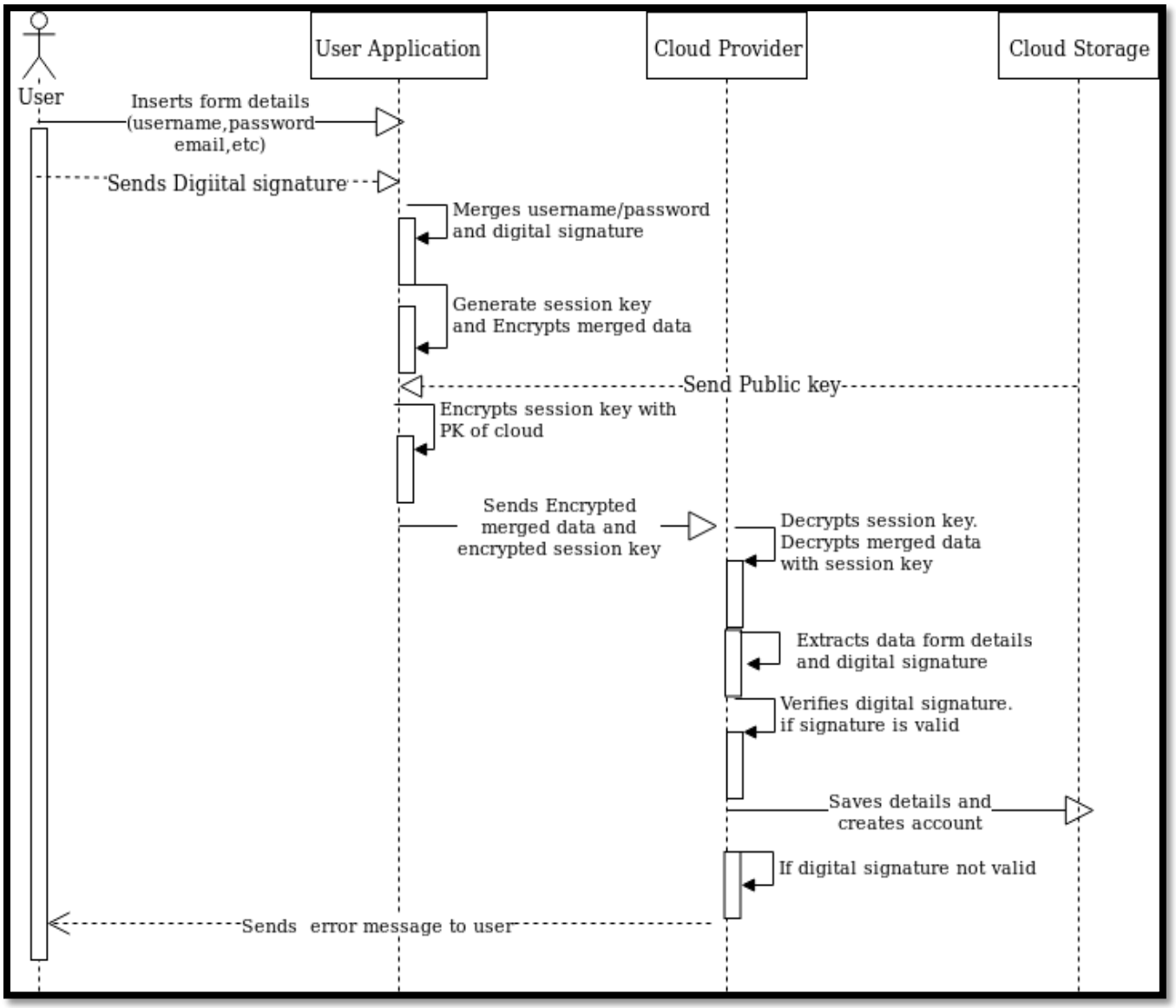
الخطوة (2) يتم دمج التوقيع الرقمي للمستخدمين في التفاصيل المدرجة.

الخطوة (3) ثم يتم تشفير البيانات المدمجة (البيانات الإلكترونية) مع مفتاح جلسة تم إنشاؤه باستخدام نظام تشفير "AES" (معيار التشفير المتقدم AES هو خوارزمية تشفير متماثل).

الخطوة (4) يتم تشفير مفتاح الجلسة باستخدام نظام تشفير "RSA" باستخدام المفتاح السحابية العام ثم يتم إرسال التاريخ المشفر (البيانات الإلكترونية) ومفتاح الجلسة المشفرة (E-Skey) إلى موفر خدمة التخزين السحابية. (تُعد "RSA "Ravist-Shamir-Adlemen خوارزمية تشفير غير متماثلة تستخدم المفتاح العام والخاص للتشفير ، ويُعطى المفتاح العمومي للجميع ويظل المفتاح الخاص خاصًا).

الخطوة (5) يستقبل موفر خدمة التخزين السحابية البيانات المشفرة ومفتاح الجلسة المشفرة، ويقوم بفك تشفير مفتاح الجلسة باستخدام مفتاحه الخاص.

الخطوة (6) فك تشفير البيانات المشفرة باستخدام مفتاح الجلسة، يتحقق من الشهادة الرقمية ثم يقوم بإنشاء الحساب. يوضح الشكل 3.3 أدناه مخطط التسلسل لإنشاء الحساب.



الشكل (3.3) مخطط التسلسل لإنشاء الحساب

3. تسجيل دخول المستخدم إلى الحساب: بالنسبة للمستخدم لتسجيل الدخول إلى حسابه الذي تم إنشاؤه

الخطوة (1) يقوم المستخدمون بإدخال اسم المستخدم وكلمة المرور الخاصة به في نموذج تسجيل الدخول

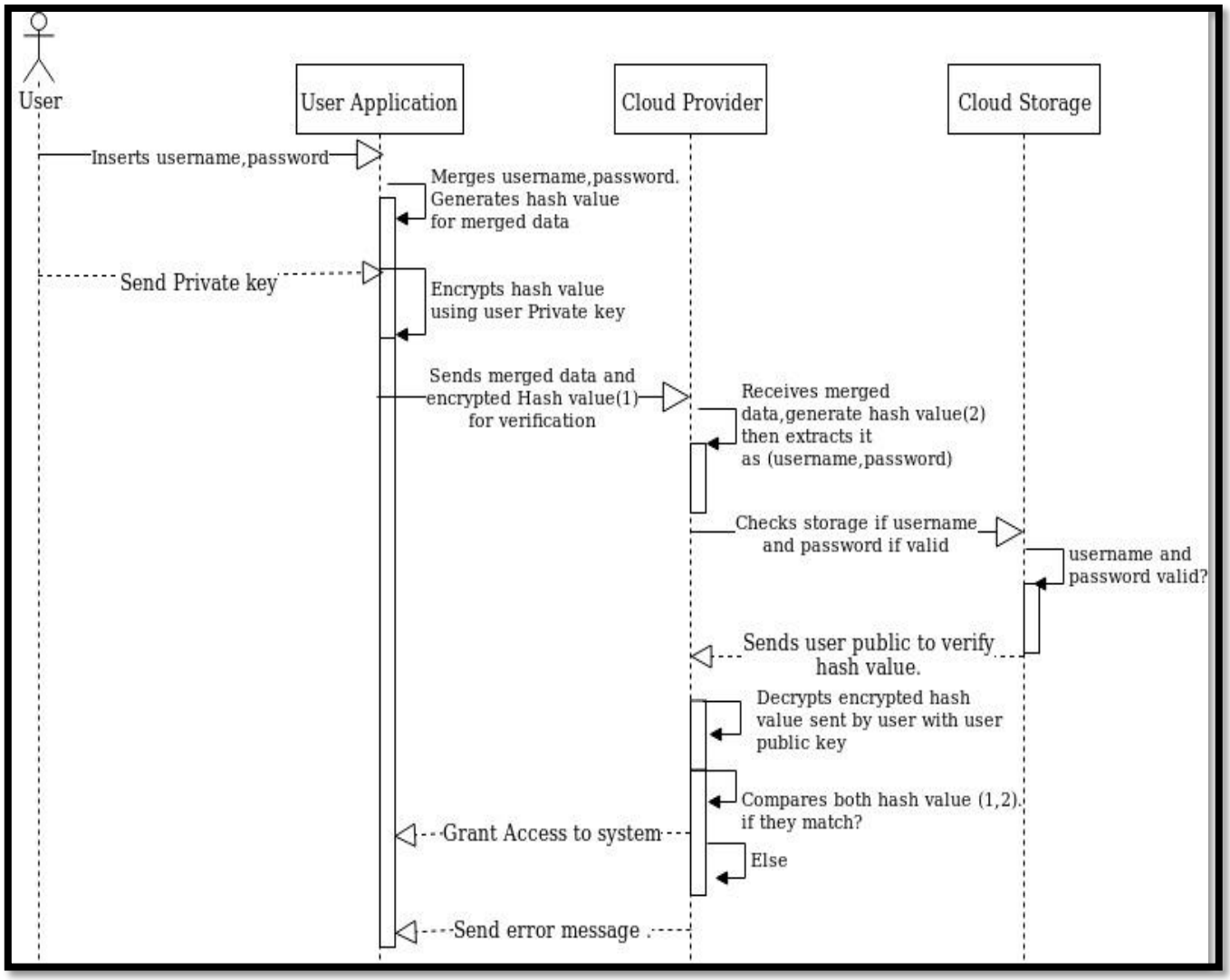
الخطوة (2) يقوم التطبيق بدمج البيانات المدخلة (اسم المستخدم وكلمة المرور) ويقوم بإنشاء قيمة هاش الخاصة به.

الخطوة (3) يقوم التطبيق بتشفير قيمة هاش التي تم إنشاؤها (هاش الإلكترونية) باستخدام المفتاح الخاص بالمستخدم "RSA"، ثم يرسل هاش المشفر (هاش الإلكتروني) والبيانات المدمجة (اسم المستخدم وكلمة المرور) إلى الموفر السحابية عبر الإنترنت للتحقق.

الخطوة (4) يتلقى موفر السحابة هاش المشفرة (هاش الإلكترونية) والبيانات المدمجة ثم استخراج (اسم المستخدم وكلمة المرور).

الخطوة (5) تتحقق السحابة من صحة اسم المستخدم وكلمة المرور، ثم تحصل على المفتاح العمومي للمستخدم من الشهادة التي يحملها معه. ثم فك تشفير (e–hash) المستلم من المستخدم باستخدام المفتاح العمومي للمستخدم.

الخطوة (6) تقوم السحابة بإنشاء بيانات مدمجة بقيمة هاش (اسم المستخدم وكلمة المرور)، وقارن قيمة هاش التي تم إنشاؤها مع قيمة هاش التي تم فك تشفيرها من قبل المستخدم. إذا كانت البيانات صالحة، فإن المستخدم يحصل على حق الوصول إلى حساب آخر لا يمكن الوصول إليه. يوضح الشكل 4.3 أدناه مخطط التسلسل لتسجيل دخول المستخدم إلى الحساب.



الشكل (4.3) مخطط التسلسل لتسجيل دخول المستخدم إلى الحساب

4. لتحميل ملف: لتحميل ملف، يمر عبر مرحلتين

المرحلة الأولى: تحديد ملف المستخدم (ملف البيانات) الذي يريد تحميله بعد ذلك

الخطوة (1) يولد التطبيق قيمة تجزئة الملف المحدد باستخدام خوارزمية هاش الآمنة SHA3 (يعد SHA3 هو أحدث عضو في مجموعة معايير خوارزمية هاش الآمنة، حيث تم إصداره بواسطة "NIST" في أغسطس-2-2015).

الخطوة (2) يتم تشفير قيمة هاش التي تم إنشاؤها باستخدام مفتاح خاص للمستخدم للحصول على (للتوقيع الرقمي للملف من المستخدم) ويتم تشفير نسخة أخرى باستخدام المفتاح العمومي للمستخدم (للسرية)، ويتم تخزين النسخة الثانية في قاعدة البيانات المحلية للمستخدمين مع بيانات التعريف حول الملف الذي تم تحميله.

الخطوة (3) يقوم التطبيق بعد ذلك بدمج وتشفير البيانات (ملف البيانات، معرف المستخدم، اسم الملف، التوقيع الرقمي) باستخدام نظام تشفير "AES (Rijindel)" معيار التشفير المتقدم "AES" هو خوارزمية تشفير متماثل) مع مفتاح جلسة عشوائية تم إنشاؤه ثم إخراج البيانات المشفرة (البيانات الإلكترونية).

الخطوة (4) يقوم التطبيق بعد ذلك بتشفير مفتاح الجلسة "E-Skey" باستخدام نظام تشفير "RSA" مع المفتاح العام لموفر السحابة، ثم دمج البيانات المشفرة "E-Data" ومفتاح الجلسة المشفر "E-Skey"، ثم إرسالها إلى مزود سحابة. ويتم تشفير نسخة أخرى من مفتاح الجلسة باستخدام المفتاح العام للمستخدم (للسرية)، ويتم تخزين النسخة الثانية في قاعدة البيانات المحلية للمستخدم مع بيانات التعريف حول الملف الذي تم تحميله.

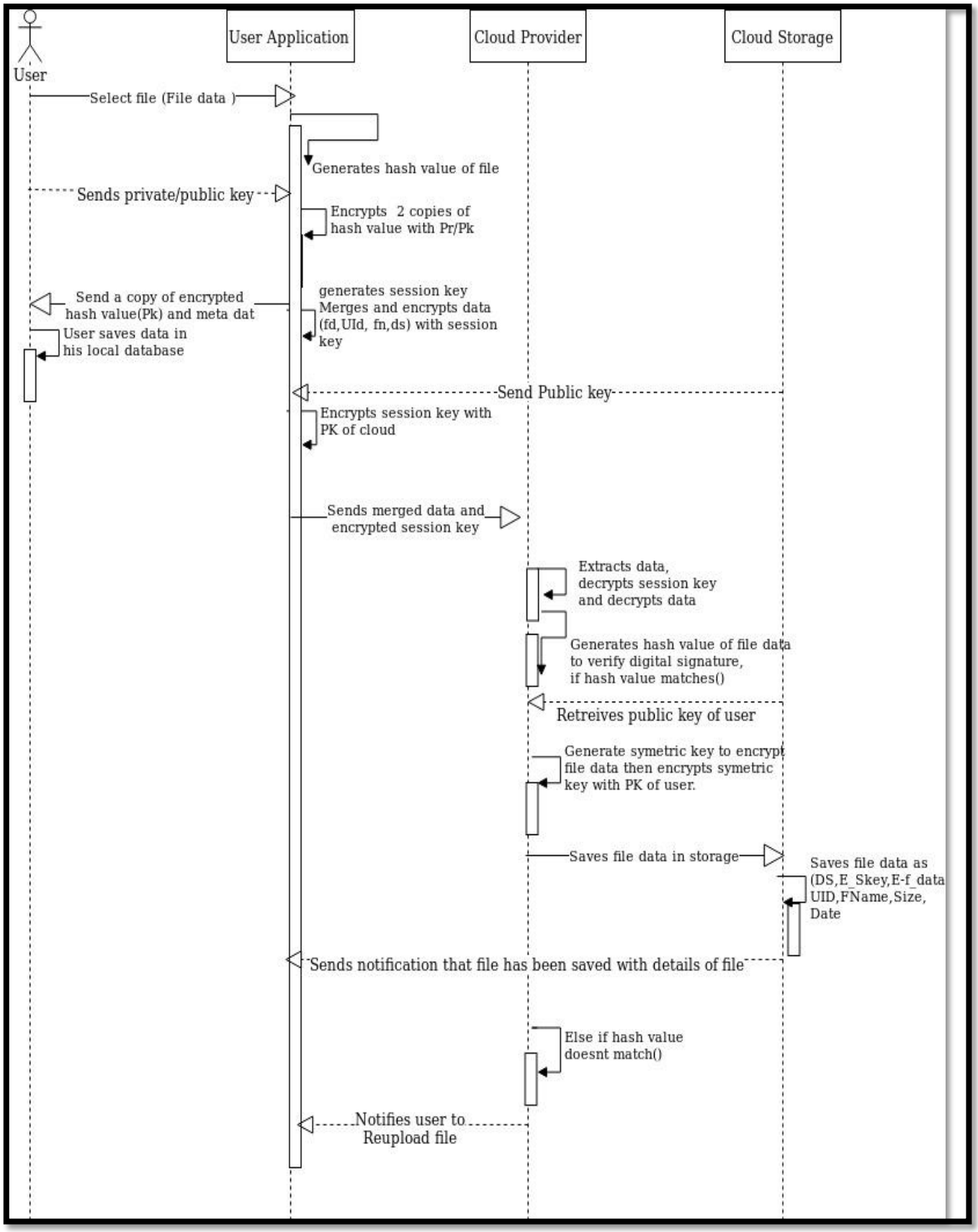
المرحلة الثانية: يستقبل مزود خدمة التخزين السحابية الملف ويستخرجه كبيانات مشفرة (البيانات الإلكترونية) ومفتاح الجلسة المشفرة "E-Skey"،

الخطوة (1) تقوم سحابة بفك تشفير مفتاح الجلسة "E-Skey" باستخدام مفتاحه الخاص، ثم فك تشفير البيانات المشفرة "E-Data" باستخدام "AES" مع مفتاح الجلسة المشفر. بعد هذه العملية، يستخرج البيانات كـ (بيانات الملف، معرف المستخدم، اسم الملف، التوقيع الرقمي)

الخطوة (2) تتحقق السحابة من التوقيع الرقمي عن طريق إنشاء قيمة تجزئة لبيانات الملف (بيانات الملف) ومقارنتها مع التوقيع الرقمي للمستخدم (قيمة هاش المشفرة -التي سيتم فك تشفيرها باستخدام المفتاح العمومي للمستخدم).

الخطوة (3) في حالة تطابق القيمة المجزأة، يقوم تشفير البيانات بالملف المشفر "E-Skey" (لدى المستخدم نسخة من مفتاح الجلسة المشفرة) ثم يحفظ أيضًا بيانات الملفات المشفرة، "E-Skey"، يحفظ أيضًا إلى جانب (التوقيع الرقمي، User_Id، اسم الملف، حجم الملف، التاريخ والوقت) في التخزين السحابية.

الخطوة (4) في حالة نجاح الخطوات السابقة، يقوم الموفر السحابية بإرسال إخطار إلى المستخدم عبر جلسة آمنة حول عملية التحميل الكاملة الناجحة للملف، وإلا يقوم الموفر السحابية بإرسال إشعار إلى المستخدم عبر جلسة آمنة حول فشل التحميل الكامل تشغيل الملف لإعادة إرسال مرة أخرى. يوضح الشكل 5.3 مخطط التسلسل لتحميل الملف.



الشكل (5.3) مخطط التسلسل لتحميل الملف

5. تنزيل ملف من السحابة: لتنزيل ملف، يمر عبر مرحلتين

المرحلة الأولى: يطلب المستخدم الملف الذي يريد تنزيله.

الخطوة (1) يقوم الموفر السحابية بإنشاء مفتاح جلسة والذي سيتم استخدامه لنظام تشفير AES.

الخطوة (2) تجمع السحابة البيانات (التوقيع الرقمي، مفتاح التناظر المشفر (E-Sym_Key)، بيانات الملفات المشفرة (E-file_data)، اسم الملف، حجم الملف، file_ID).

الخطوة (3) ثم يتم تشفير البيانات المدمجة باستخدام نظام تشفير AES باستخدام مفتاح جلسة مفتاح الجلسة الذي تم إنشاؤه مسبقًا باسم (E-data) ثم يتم تشفير مفتاح الجلسة كـ (E-Skey) باستخدام نظام تشفير "RSA" مع مفتاح المستخدم العمومي.

الخطوة (4) يقوم التطبيق بعد ذلك بدمج البيانات المشفرة (E-Data) ومفتاح الجلسة المشفر (E-Skey)، ثم يرسلها إلى المستخدم.

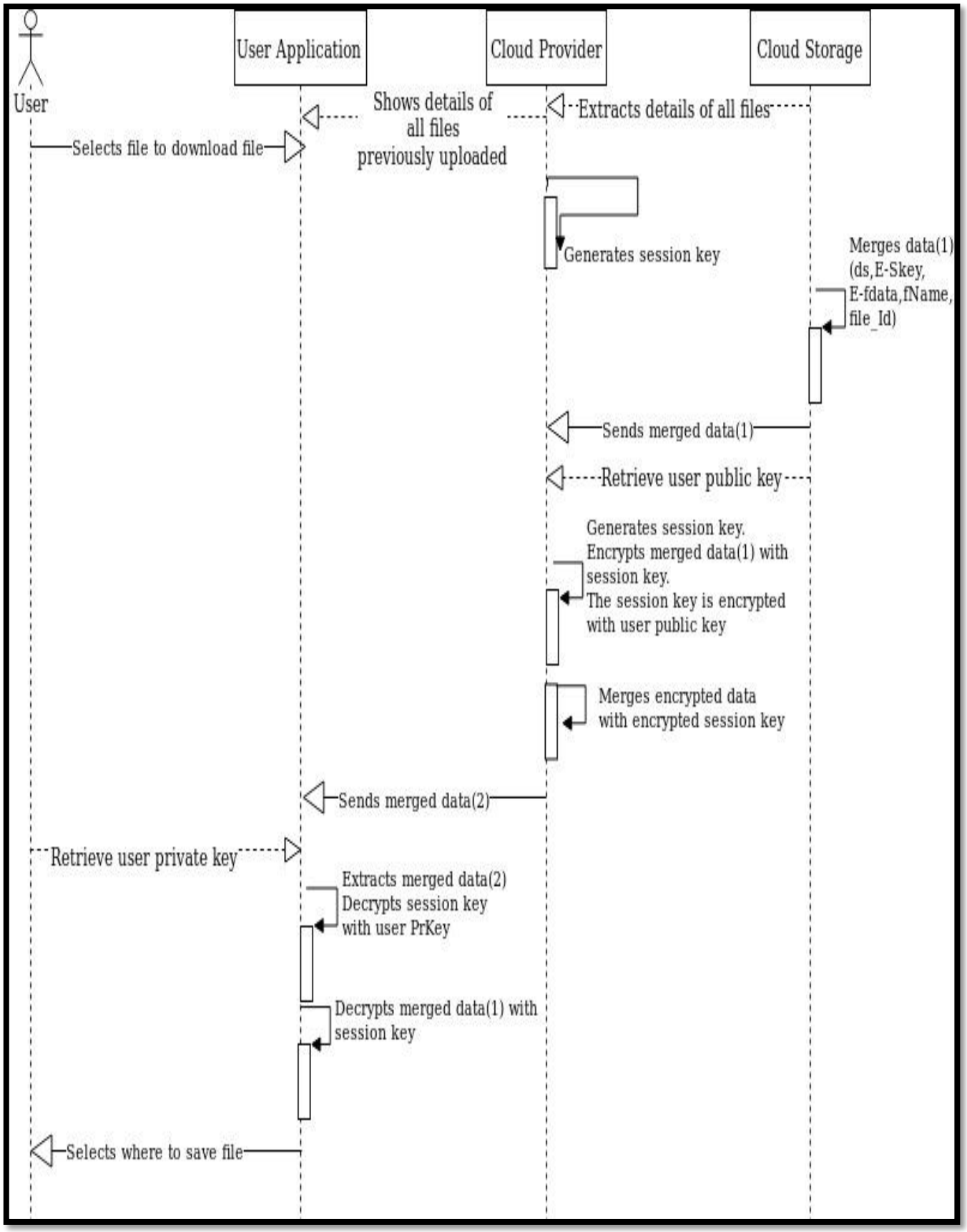
المرحلة الثانية: يتلقى المستخدم البيانات ويستخرجها كبيانات مشفرة (E-Data) ومفتاح جلسة مشفرة (E-Skey).

الخطوة (1) يقوم التطبيق بفك تشفير مفتاح الجلسة (E-Skey) باستخدام "RSA" باستخدام مفتاحه الخاص وكذلك فك تشفير البيانات المشفرة (E-Data) باستخدام مفتاح الجلسة المشفر باستخدام AES.

الخطوة (2) ثم يتم استخراج البيانات كـ (التوقيع الرقمي، مفتاح التناظر المشفر (E-Sym_Key)، بيانات الملفات المشفرة (E-file_data)، اسم الملف، حجم الملف، file_ID).

الخطوة (3) يقوم تطبيق المستخدم بفك تشفير المفتاح المتماثل المشفر (E-Sym_Key) باستخدام مفتاح الخاص، ثم يقوم بفك تشفير بيانات الملفات المشفرة (E-file_data) باستخدام مفتاح الجلسة المشفر.

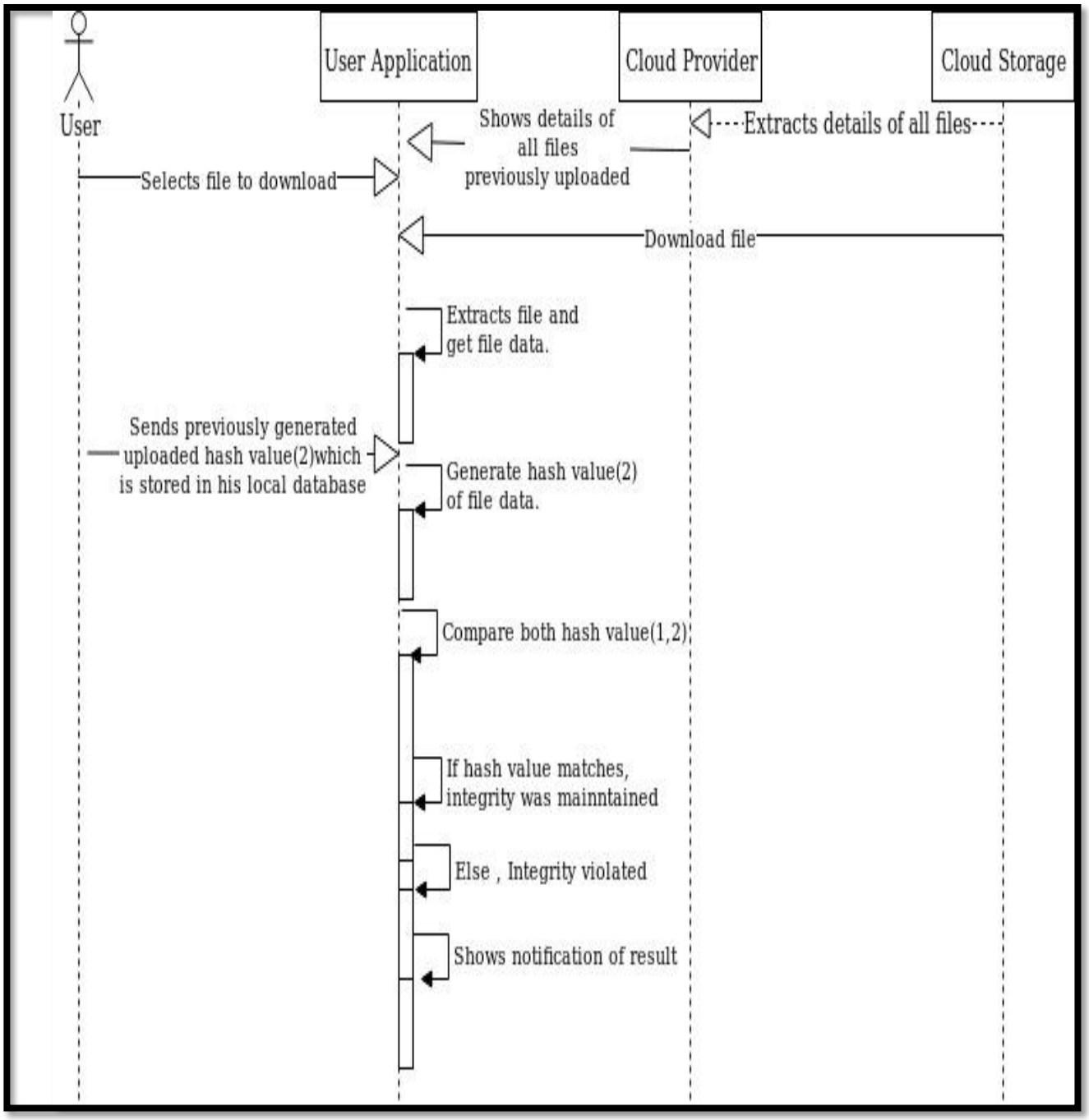
الخطوة (4) يتحقق التطبيق من التوقيع الرقمي عن طريق إنشاء قيمة تجزئة لبيانات الملف (ملف البيانات) ومقارنتها مع التوقيع الرقمي المستلم (قيمة هاش المشفرة –التي سيتم فك تشفيرها باستخدام المفتاح العمومي للمستخدم). إذا تطابقت القيمة المجزأة، فاختر مكان حفظ الملف في محرك الأقراص المحلي وتنزيل الملف. يوضح الشكل 6.3 مخطط التسلسل لتنزيل الملف.



الشكل (6.3) مخطط التسلسل لتنزيل الملف

6. تحقق من تكامل الملف: للطعن في تكامل الملف، يمكن للمستخدم القيام بذلك بطريقتين:

1. يمكنه تنزيل الملف كما هو موضح أعلاه، ثم إنشاء قيمة هاش للملف (بيانات الملف) ومقارنتها بقيمة هاش التي تم تنزيلها من خلال (توقيع رقمي) أو نسخته من قيمة هاش. يوضح الشكل 7.3 مخطط التسلسل للمستخدم للتحقق من سلامة الملف



الشكل (7.3) مخطط التسلسل للمستخدم للتحقق من سلامة الملف

2. يمكنه التحقق من سلامة الملف من خلال هذه الخطوات بعد أن يطلب المستخدم الملف الذي يريد التحقق من سلامته.

الخطوة (1) يقوم الموفر السحابية بإنشاء مفتاح جلسة والذي سيتم استخدامه لنظام تشفير "AES".

الخطوة (2) تجمع السحابة البيانات (التوقيع الرقمي، مفتاح التناظر المشفر (E-Sym_Key)، بيانات الملفات المشفرة (E-file_data)، اسم الملف، حجم الملف، file_ID).

الخطوة (3) ثم يتم تشفير البيانات المدمجة باستخدام نظام تشفير AES باستخدام مفتاح جلسة مفتاح الجلسة الذي تم إنشاؤه مسبقًا باسم (E-data) ثم يتم تشفير مفتاح الجلسة كـ (E-Skey) باستخدام نظام تشفير "RSA" مع مفتاح المستخدم العمومي.

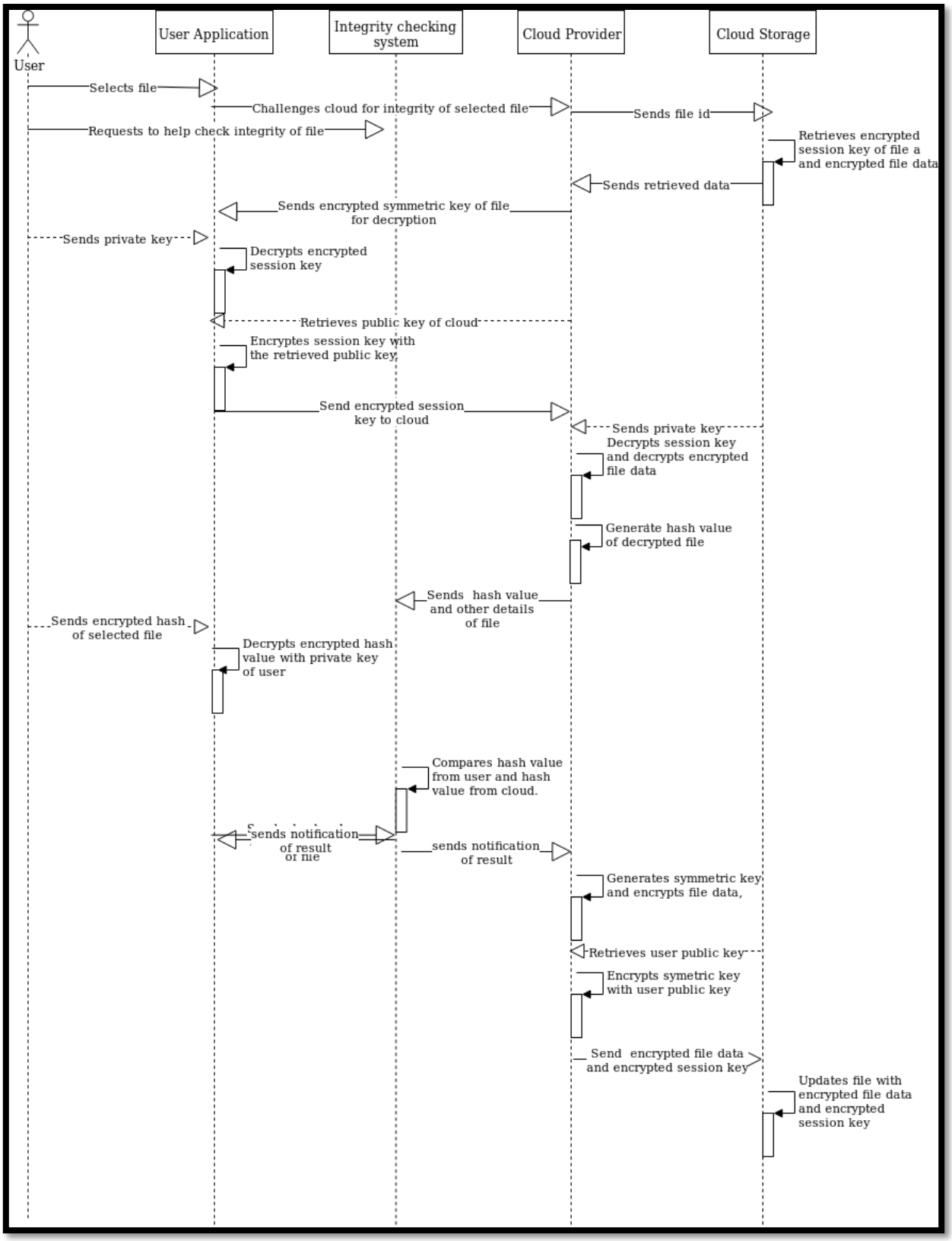
الخطوة (4) يقوم التطبيق بعد ذلك بدمج البيانات المشفرة (E-Data) ومفتاح الجلسة المشفر (E-Skey)، ثم يرسلها إلى المستخدم.

الخطوة (5) يتلقى المستخدم البيانات ويستخرجها كبيانات مشفرة (E-Data) ومفتاح الجلسة المشفرة (E-Sky). يقوم التطبيق بفك تشفير مفتاح الجلسة (E-Skey) باستخدام "RSA" باستخدام مفتاحه الخاص وكذلك فك تشفير التشفير المشفر البيانات (البيانات الإلكترونية) مع مفتاح جلسة فك التشفير باستخدام "AES".

الخطوة (6) ثم يتم استخراج البيانات كـ (التوقيع الرقمي، مفتاح التماثل المشفر (E-Sym_Key)، بيانات الملفات المشفرة (E-file_data)، اسم الملف، حجم الملف، file_ID).

الخطوة (7) يقوم تطبيق المستخدم بفك تشفير المفتاح المتماثل المشفر (E-Sym_Key) باستخدام مفتاحه الخاص، ثم يقوم بفك تشفير بيانات الملفات المشفرة (E-file_data) باستخدام مفتاح الجلسة المشفر.

الخطوة (8) يتحقق التطبيق من التوقيع الرقمي عن طريق إنشاء قيمة تجزئة لبيانات الملف (ملف البيانات) ومقارنتها مع التوقيع الرقمي المستلم (قيمة هاش المشفرة –التي سيتم فك تشفيرها باستخدام المفتاح العمومي للمستخدم). إذا تطابق كلا القيمة المجزأة، فهذا يعني الحفاظ على التكامل. يوضح الشكل 8.3 الرسم البياني التسلسلي للمستخدم للتحقق من سلامة الملف باستخدام نظام فحص للسلامة الملفات.



الشكل (8.3) الرسم التسلسلي للمستخدم للتحقق من سلامة الملف باستخدام نظام فحص للسلامة الملفات.

7. **إعادة تعيين كلمة المرور**: إذا نسي المستخدم كلمة المرور الخاصة به، فيمكنه استرداد كلمة المرور الخاصة به من النظام، وذلك بتأكيد رابط تم إرساله إلى بريده الإلكتروني، ثم أدخل رقمًا تم إرساله إلى رقم هاتفه المحمول.
8. **تحديث ملف**: لتحديث ملف إذا كان المستخدم المصادق عليه هو منشئ الملف أو إذا كان لديه أذونات مطلوبة لتحديث الملف، يقوم المستخدم بتحديد الملف، ويقوم بتنزيله ثم يقوم بإجراء التحديثات ثم يقوم بتحميله مرة أخرى. يمكن فقط للمستخدم المسموح به مع أذونات الملف الصحيحة تحديث الملف.

المستخدم محذوف من ملف: لحذف ملف، يقوم المستخدم المصادق باختيار الملف، ثم يحذفه، إذا كان هو منشئ الملف، فسيتم حذف الملف وبيانات التعريف الخاصة به في السحابة وفي قاعدة بياناته المحلية، إذا تم التوثق المستخدم ليس مالك الملف وليس لديه إذن مطلوب فقط سيتم حذف نسخته من الملف.

9. **تطوير ملف السجل**: لتعيين التغيير في الملف، سيحتوي النظام على ملف سجل، وملف السجل يحفظ جميع العمليات التي تتم في الملف ومن قام بالعملية، بحيث يكون كل مستخدم مسؤولاً عن العملية التي قام بها هذا الملف. يمثل الجدول 2.3 عينة من محتوى ملف السجل.

جدول (2.3): نموذج لمحتوى ملف السجل

Action carried	File_ID	Name	User	Time & data
Upload	01	File.doc	Raji	**09- -2019 09-11 00**
Download	02	Sample.docx	Adam	**09- -2019 00-11 10**
Delete	02	Sample.docx	Adam	**09- -2019 00-11 11**
Update	01	File.doc	Raji	**09- -2019 09-09 12**

ملخص

في هذا الفصل، قدمنا التحليل لنماذج تكامل البيانات في حوسبة السحابية ومتطلبات الامن ثم النموذجنا المقترح لتوثق المستخدم والتحقق من سلامة البيانات للملفات في السحابة العامة بهيكلها وأوصافها للنماذج العامة. ثم يتم شرح المنهجية مع بعض الأمثلة على كيفية عمل النموذج باستخدام مخطط التسلسل لنموذج ومخطط تدفق المحادثة.

الفصل الرابع

التصميم والتنفيذ

4. مقدمة

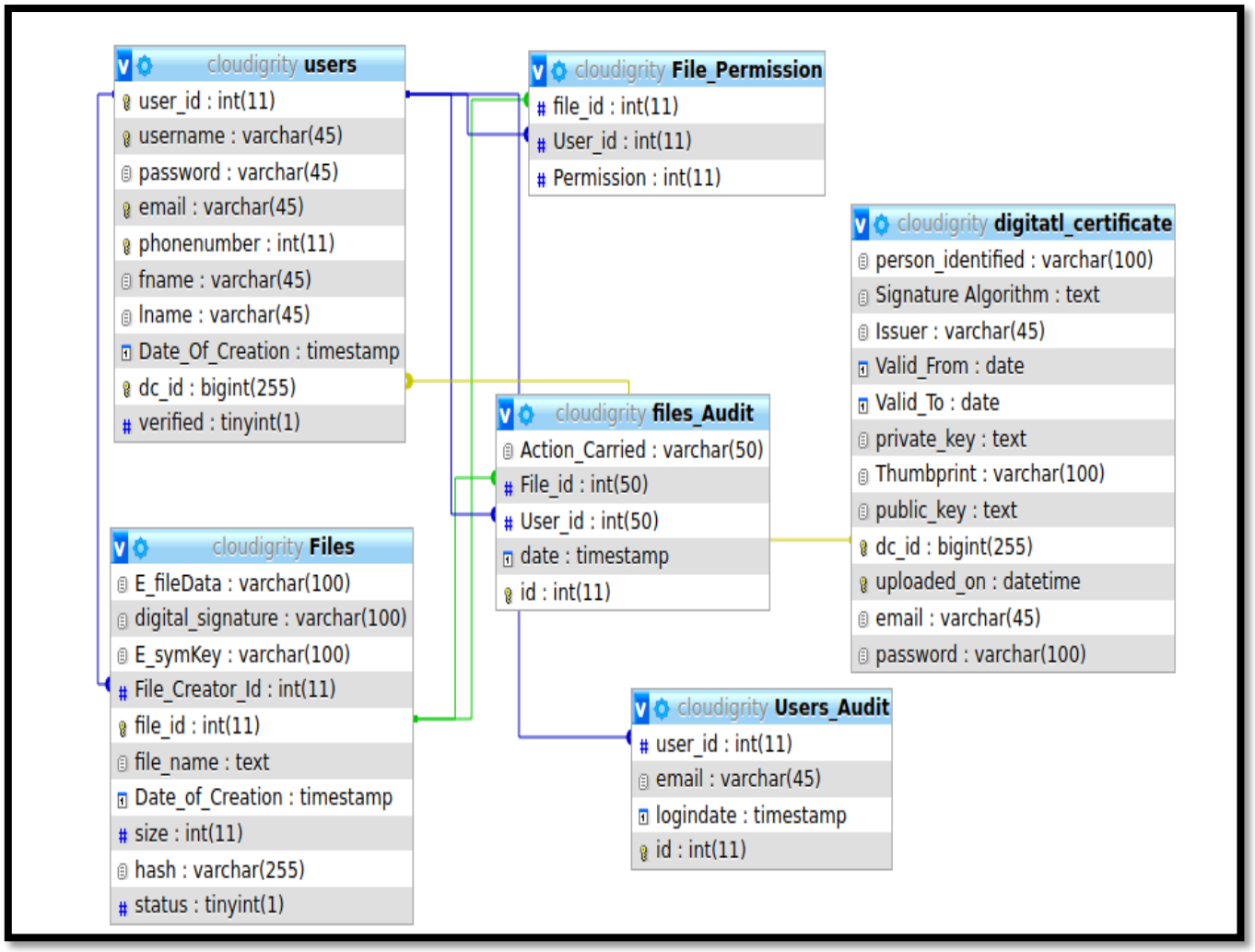
نقدم التصميم النموذج من حيث تصميم قاعدة البيانات و تصميم عمليات والواجهات ثم التنفيذ بإستخدام تقنيات و ادوات المختلفة ثم وتجارب علي النموذج لتقييمها.

1.4 التصميم

في هذا الباب ، نقدم تصميم النموذج المقترح وكيف سيبدو النظام الأساسي وتصميم قاعدة البيانات وتصميم العملية وتصميم الواجهة.

1.1.4 تصميم قاعدة البيانات

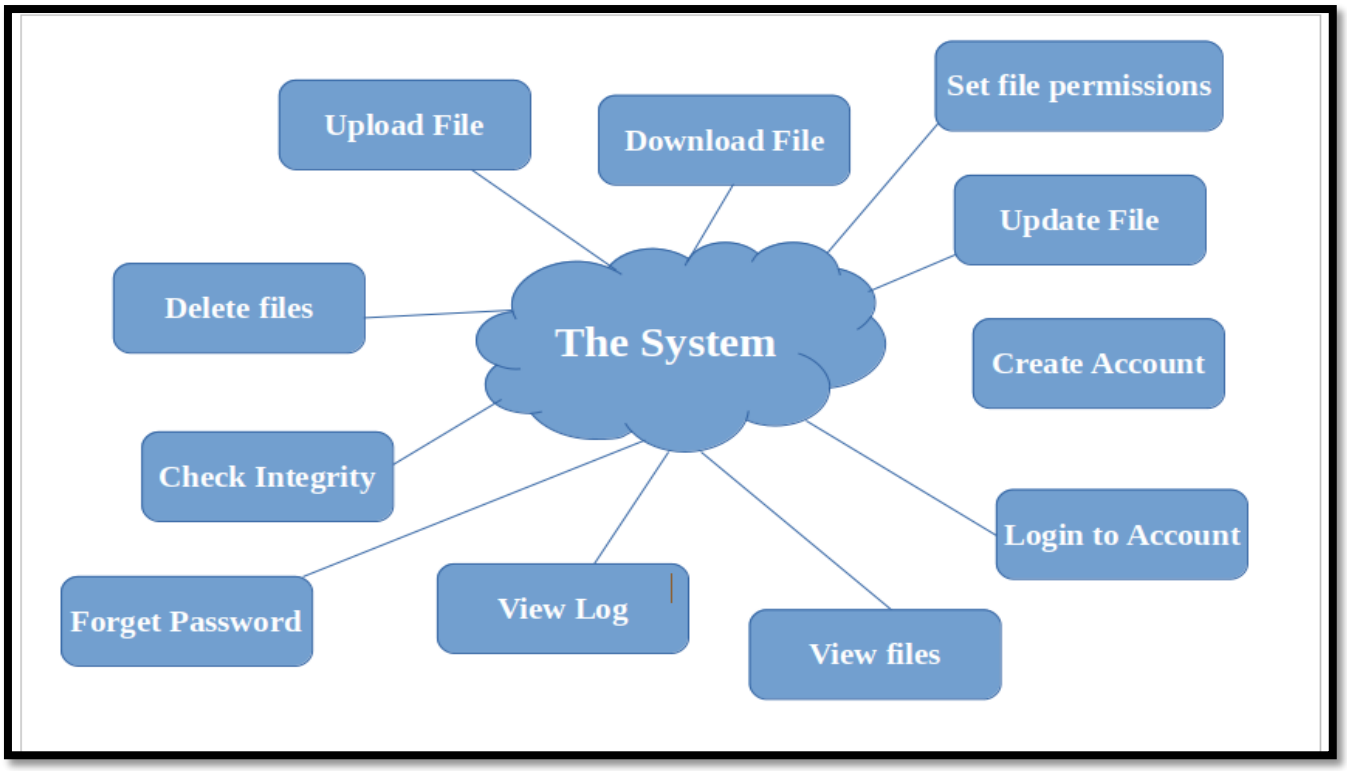
تصميم قاعدة البيانات هو تنظيم البيانات وفقًا لنموذج قاعدة البيانات، ونحدد البيانات التي يجب تخزينها وكيف تترابط عناصر البيانات مع بعضها البعض. لتنفيذ النموذج المقترح، يمكن استخدام أنواع مختلفة من قواعد البيانات سواء كانت علائقية أو موجهة للكائنات، نستخدم MySQL لقاعدة البيانات العلائقية لتنفيذ النموذج المقترح. MySQL هو نظام إدارة قواعد البيانات العلائقية مفتوح المصدر. يظهر تصميم قاعدة البيانات في الشكل 1.4 أدناه.



الشكل.(1.4) تصميم لقاعدة البيانات

1.1.4 تصميم العمليات

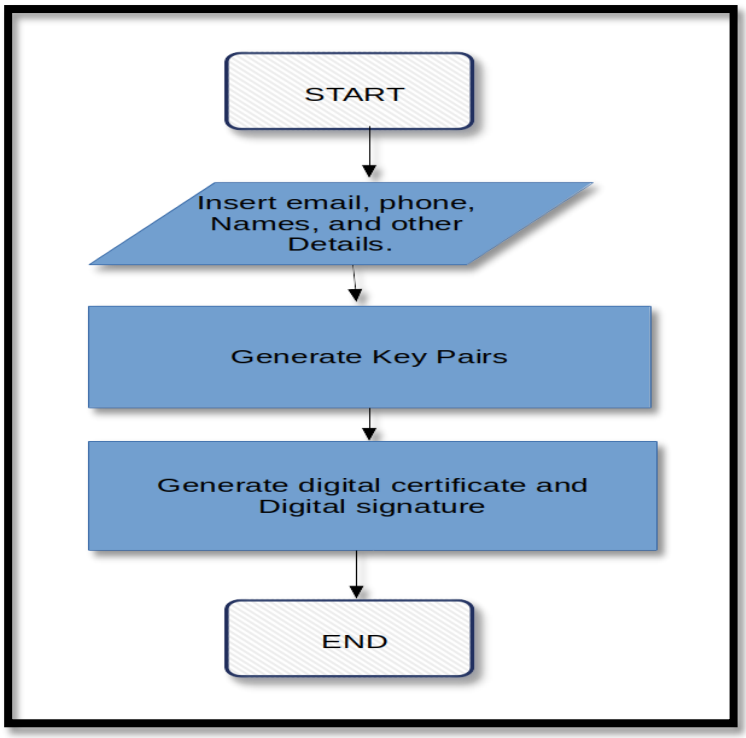
نقدم تصميم العملية، وسنذكر هنا عمليات الجهات الفاعلة وفقًا لتحليلنا. يمثل الشكل 2.4 الوحدات الرئيسية للنظام الوسيط الذي يتكون من (إنشاء حساب، تسجيل الدخول إلى الحساب، تحميل الملف، تنزيل الملف، التحقق من تكامل الملف، عرض الملف، تحديث الملف، حذف الملف، تنظيم أذونات عمليات الملفات (القراءة أو الكتابة) وعرض ملفات السجل). يحتوي النظام على هذه الوظائف كما هو مبين في الشكل 2.4:



الشكل (2.4): وحدات النظام

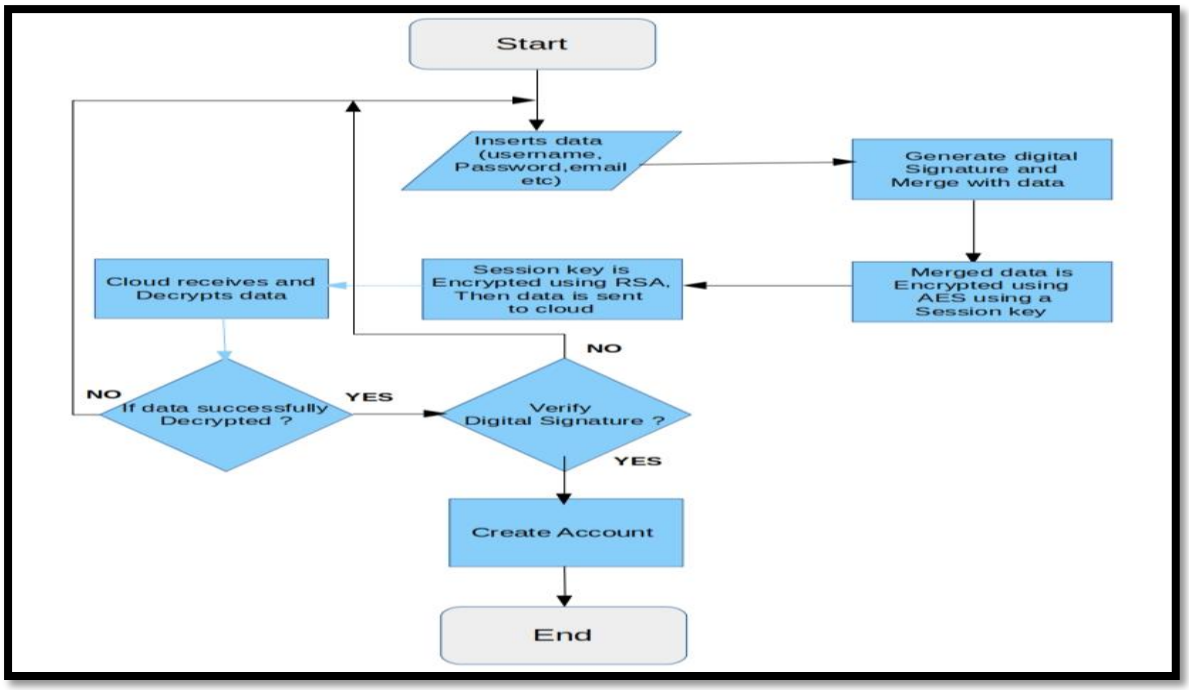
2.1.4 عمليات مفصلة

انشاء شهادة الرقمية: يمكن للمستخدم إنشاء شهادة الرقمية عن طريق ملء بياناته الشخصية، ثم يتم توليد مفاتح و الشهادة الرقمية وتوقيع. يعرض الشكل 3.4 مخطط انسيابي لإنشاء شهادة الرقمية.



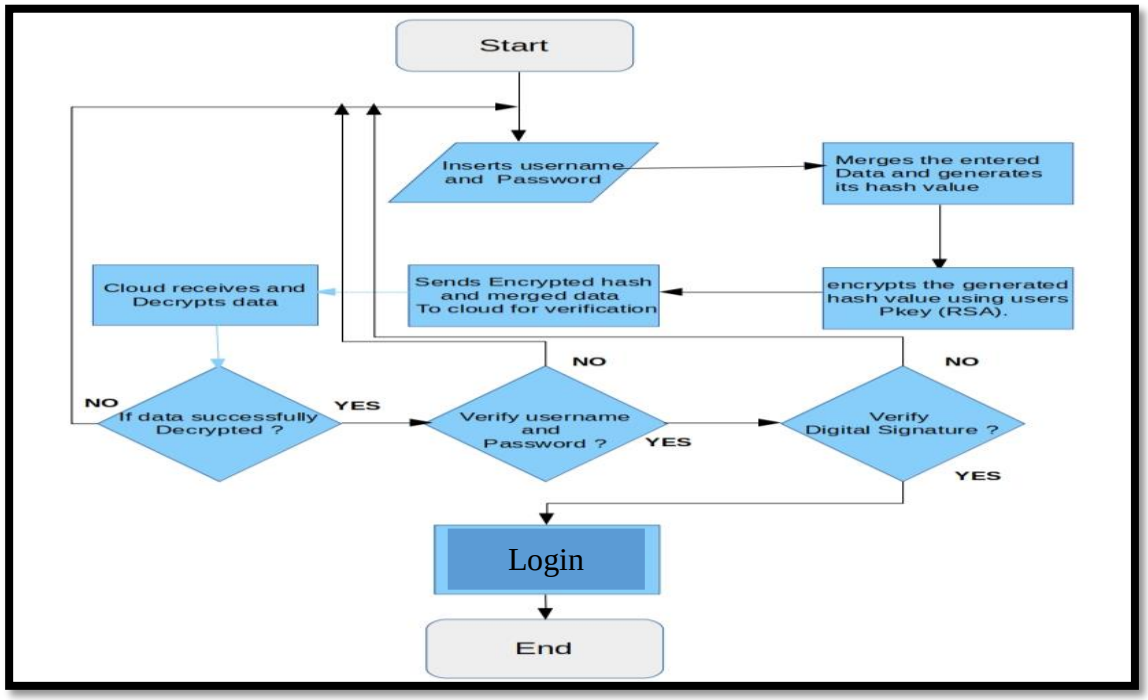
الشكل (3.4) الرسم البياني لعملية إنشاء شهادة الرقمية

إنشاء حساب مستخدم: يمكن للمستخدم إنشاء حساب جديد عن طريق ملء بياناته الشخصية، ثم يتم دمج الشهادة الرقمية قبل إرسالها إلى السحابة للتحقق منها وإنشاء الحساب. يعرض الشكل 4.4 مخطط انسيابي لإنشاء المستخدم للحساب.



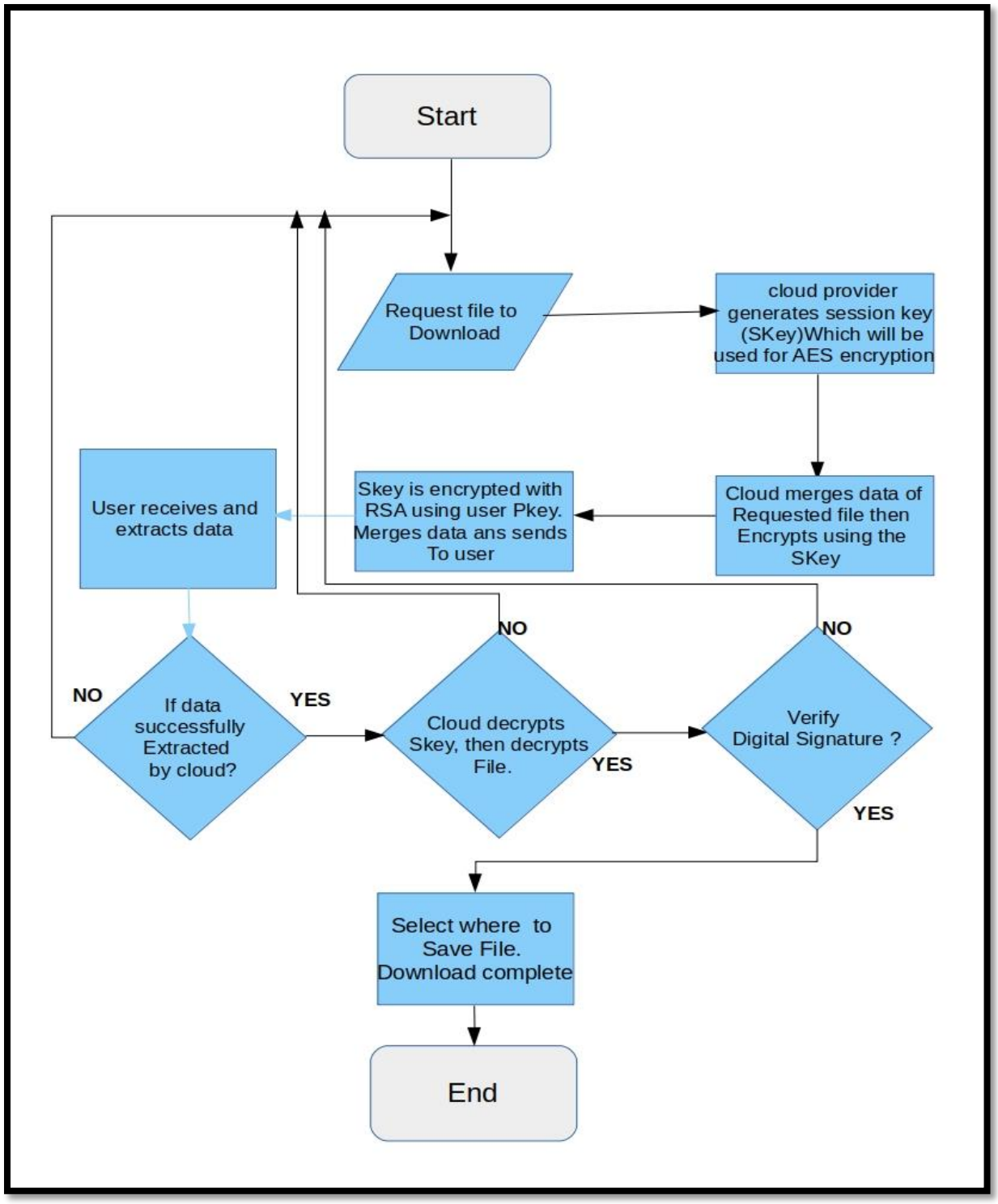
الشكل (4.4) الرسم البياني لعملية إنشاء حساب

تسجيل الدخول إلى الحساب: يمكن للمستخدم تسجيل الدخول إلى حسابه عن طريق إدخال اسم المستخدم وكلمة المرور ثم التوثق المستندة إلى الشهادة المستخدمة للتحقق من صحة المستخدم قبل الوصول إلى الحساب. يوضح الشكل 5.4 مخطط انسيابي لتسجيل الدخول إلى الحساب.



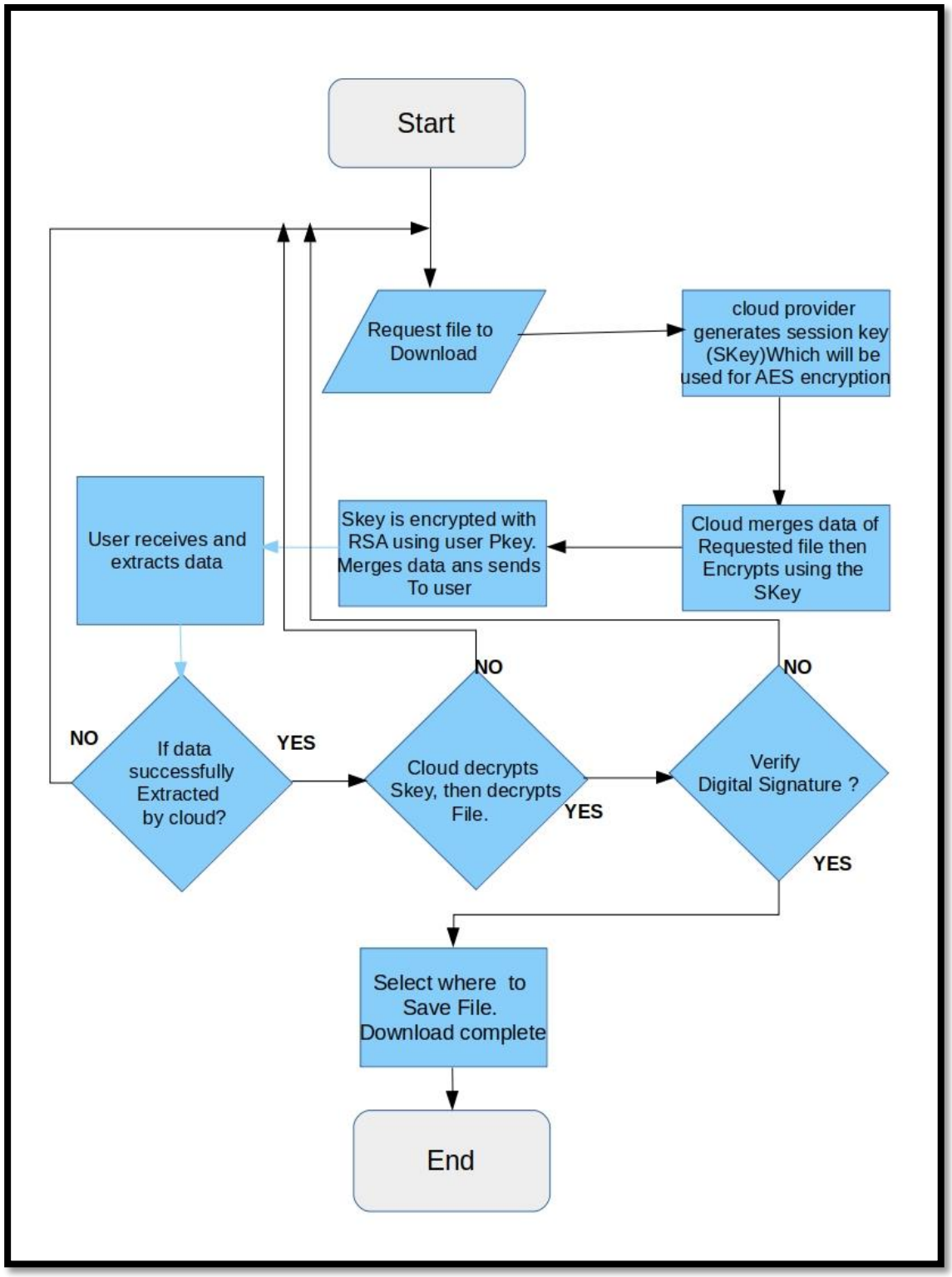
الشكل (5.4) الرسم البياني لعملية تسجيل الدخول

تحميل الملف: يمكن للمستخدم اختيار ملف من أي امتداد (مستندات، jpeg،mp3، mp4، pdf ، rar، zip،txt إلخ) من جهازه وتحميله ببساطة إلى النظام الوسيط. يوضح الشكل 6.4 مخطط انسيابي لتحميل الملف.



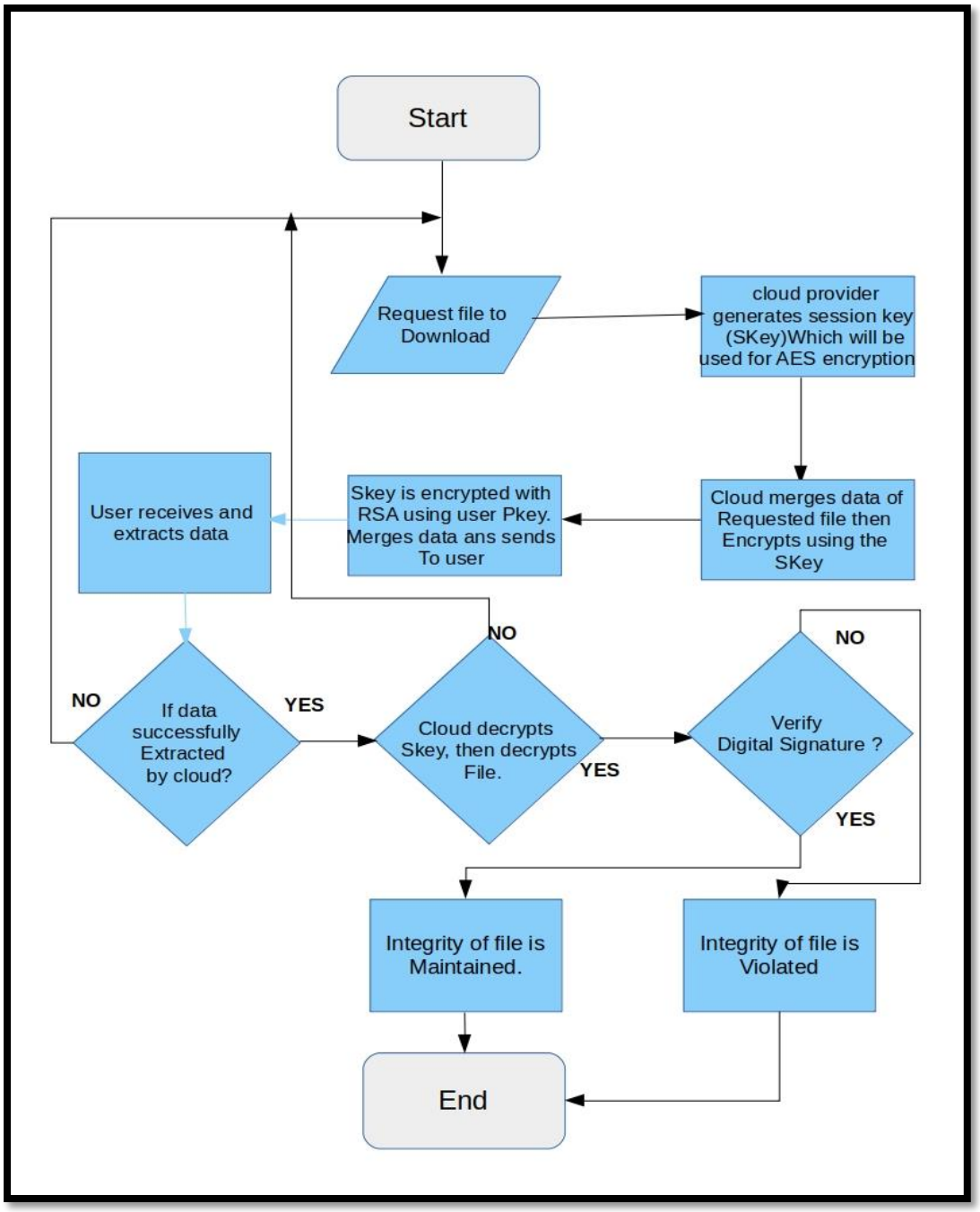
الشكل (6.4) الرسم البياني لعملية تحميل الملف

تنزيل الملف: يمكن للمستخدم تنزيل ملف قام بتحميله مسبقًا أو ملف لديه إذن بتنزيله. يعرض الشكل 7.4 مخطط انسيابي لتنزيل الملفات.



الشكل (7.4) الرسم البياني لعملية تنزيل الملف

التحقق من سلامة الملفات: يمكن للمستخدم التحقق من سلامة ملفه الذي تم تحميله كما يظهر في الرسم البياني 8.4 المخطط.



الشكل (8.4) الرسم البياني لعملية التحقق من سلامة الملفات

3.1.4 عمليات اخري

حذف الملف: عندما لم تعد هناك حاجة إلى الملف، يمكن لأي مستخدم حذفه. يمكن حذف الملف نهائيًا من قِبل منشئ الملف أو مستخدم لديه إذن كامل بالملف.

تحديث الملف: يمكن للمستخدم تحديث ملف عن طريق تحديد الملف الذي يرغب في تحديثه وإعادة تحميله.

ضبط عملية الملف: يمكن للمستخدم الذي قام بإنشاء الملف أو لديه إذن كامل بالملف تعيين أذونات على الملف.

عرض الملف: يمكن للمستخدم في النظام عرض الملف الذي حمّله، أو الملفات التي لديه إذن بقراءتها.

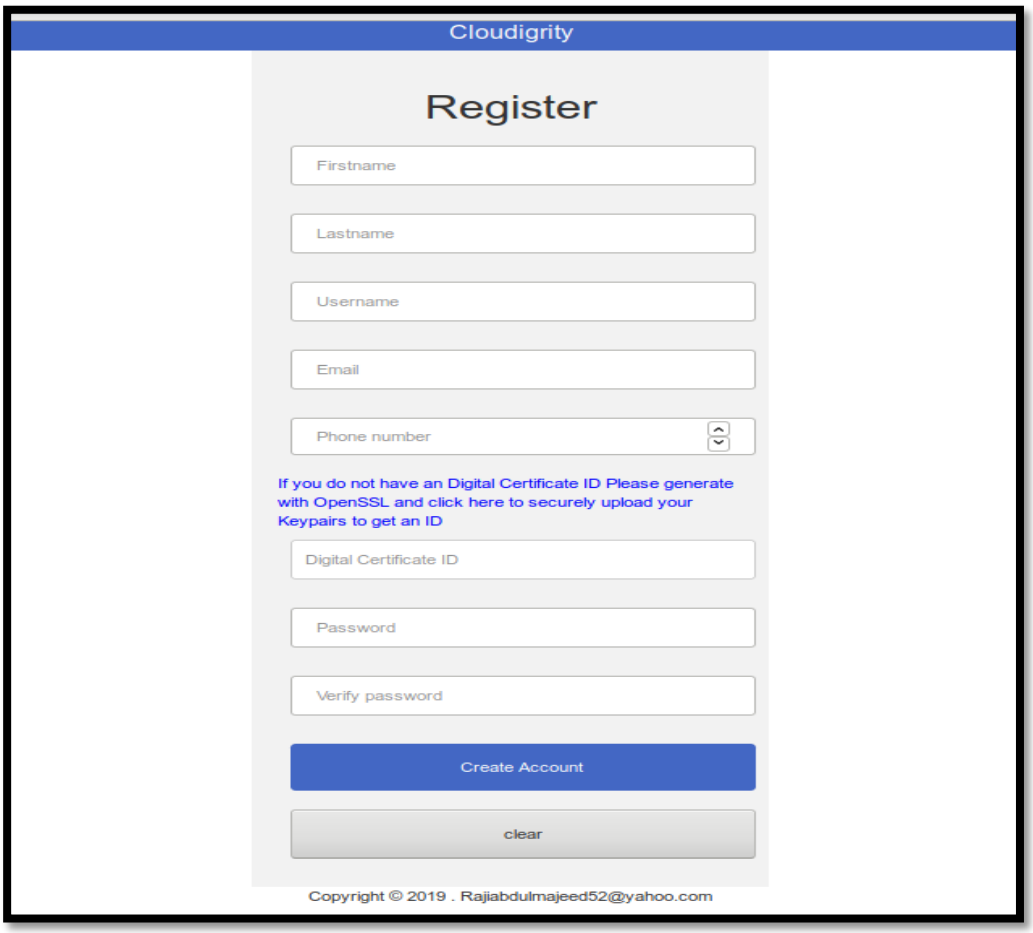
عرض السجل: يتم حفظ جميع العمليات على الوصول إلى الحساب أو الملف في ملف السجل.

نسيت كلمة المرور: يمكن للمستخدم إعادة تعيين كلمة المرور الخاصة به إذا نسيها.

4.1.4 تصميم الواجهات

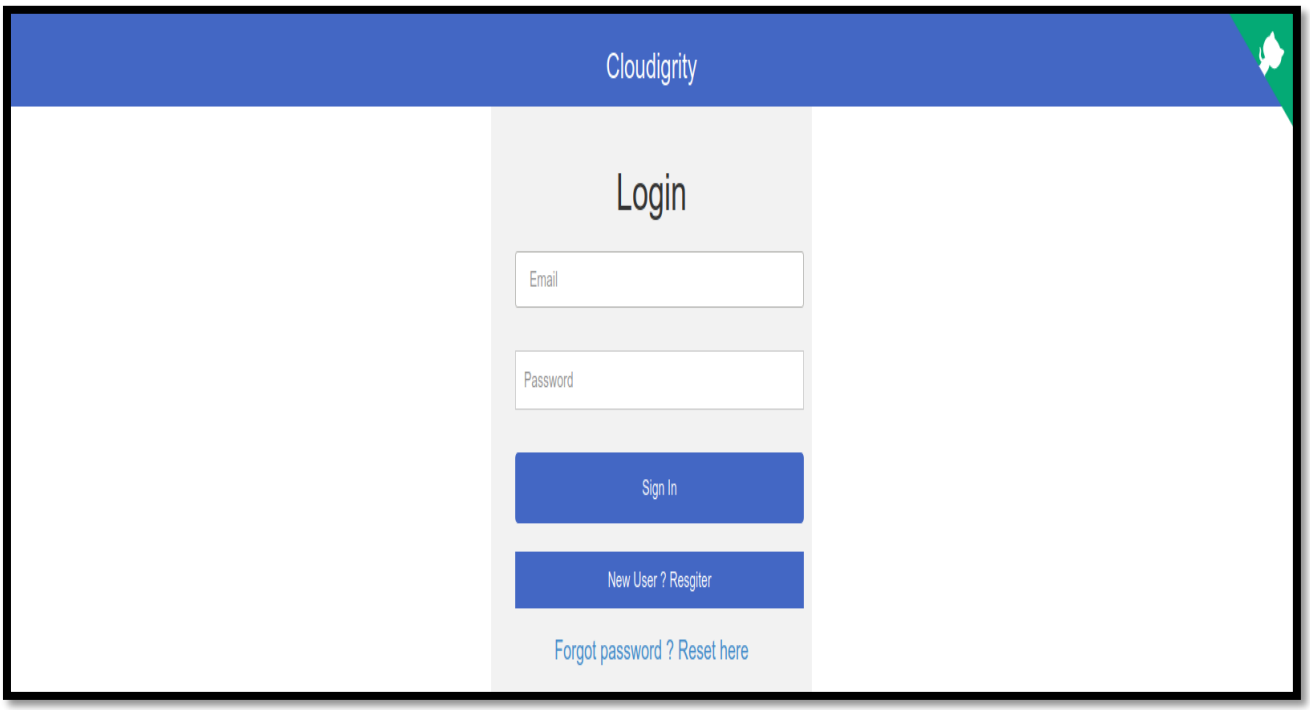
إنشاء حساب مستخدم: ينشئ المستخدم حسابه عن طريق ملء بياناته وإدخال معرف الشهادة الرقمية.

يوضح الشكل 9.4 تصميم صفحة إنشاء الحساب.



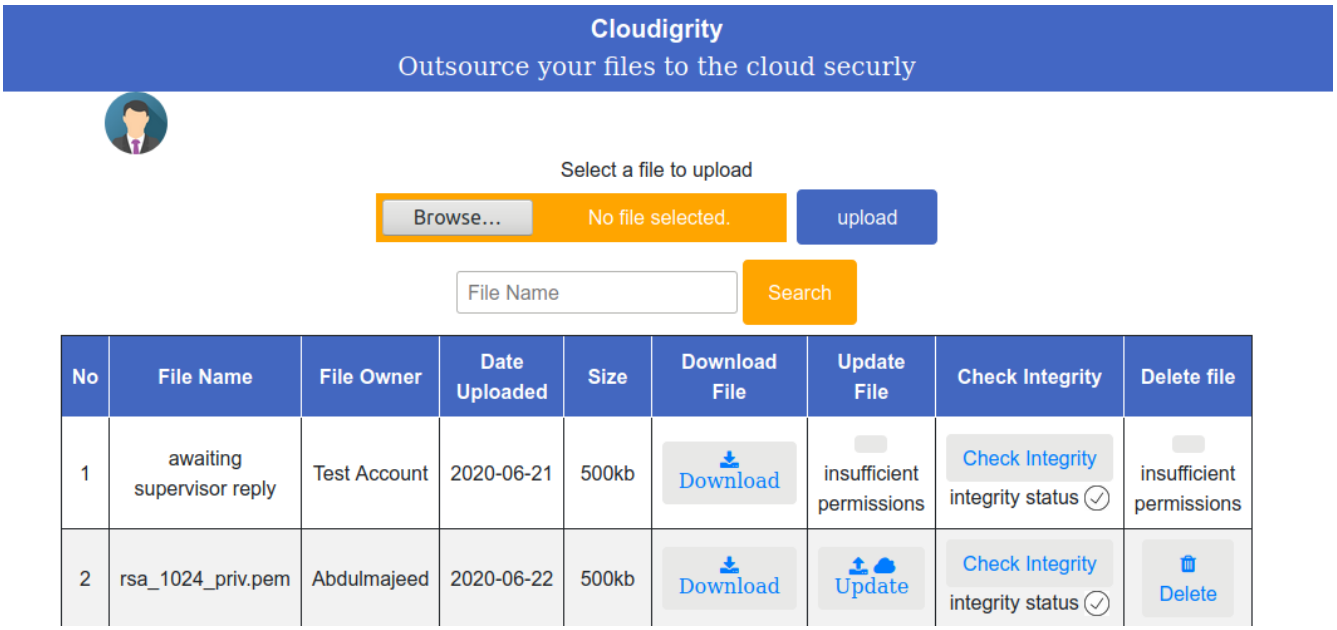
الشكل (9.4) التصميم لصفحة إنشاء الحساب

تسجيل الدخول إلى الحساب: تسمح هذه الصفحة للمستخدمين بتسجيل الدخول إلى الحساب. يوضح الشكل 10.4 تصميم صفحة تسجيل الدخول إلى الحساب.



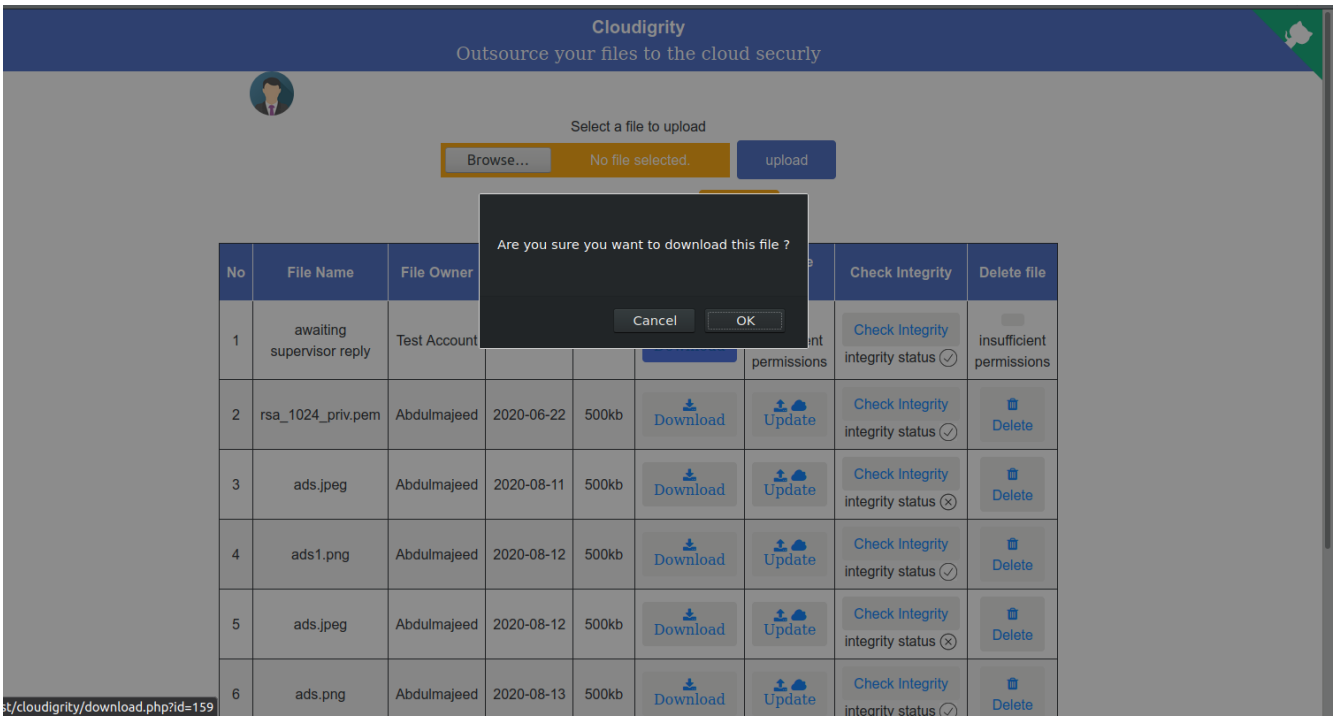
الشكل (10.4) التصميم لصفحة تسجيل الدخول

الصفحة الرئيسية: يمكن للمستخدم الوصول إلى الصفحة الرئيسية بعد إدخال تفاصيله الصحيحة. يوضح 11.4 أدناه الصفحة الرئيسية للنظام.



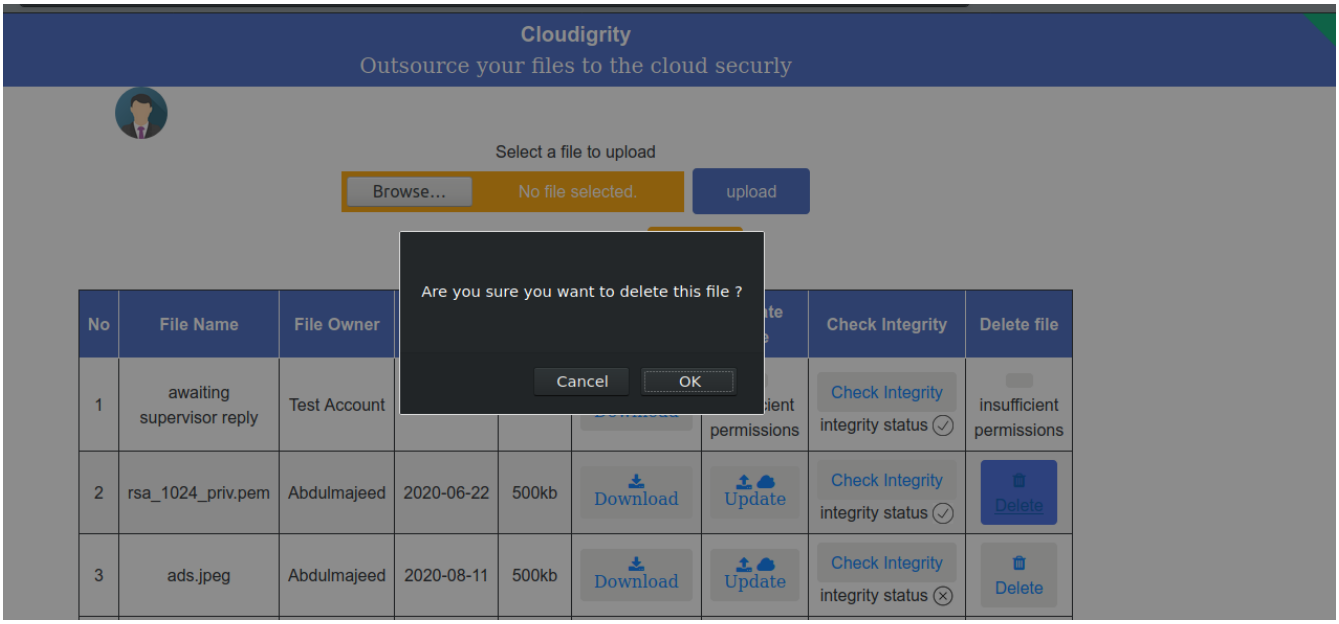
الشكل (11.4) التصميم للصفحة الرئيسية للنظام

الصفحة لتحميل الملف : يوضح الشكل 12.4 أدناه الصفحة لتنزيل الملفات للنظام



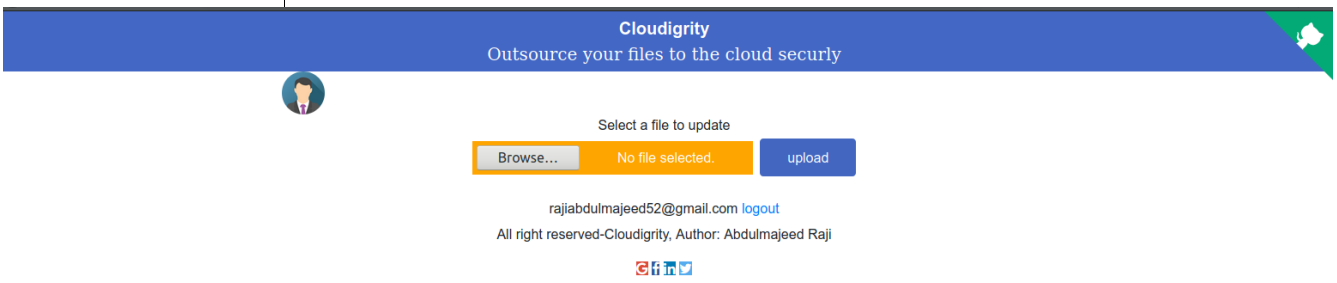
الشكل (12.4) التصميم للصفحة للتنزيل الملف

الصفحة لحذف الملف : يوضح الشكل 13.4 أدناه الصفحة لحذف الملفات.



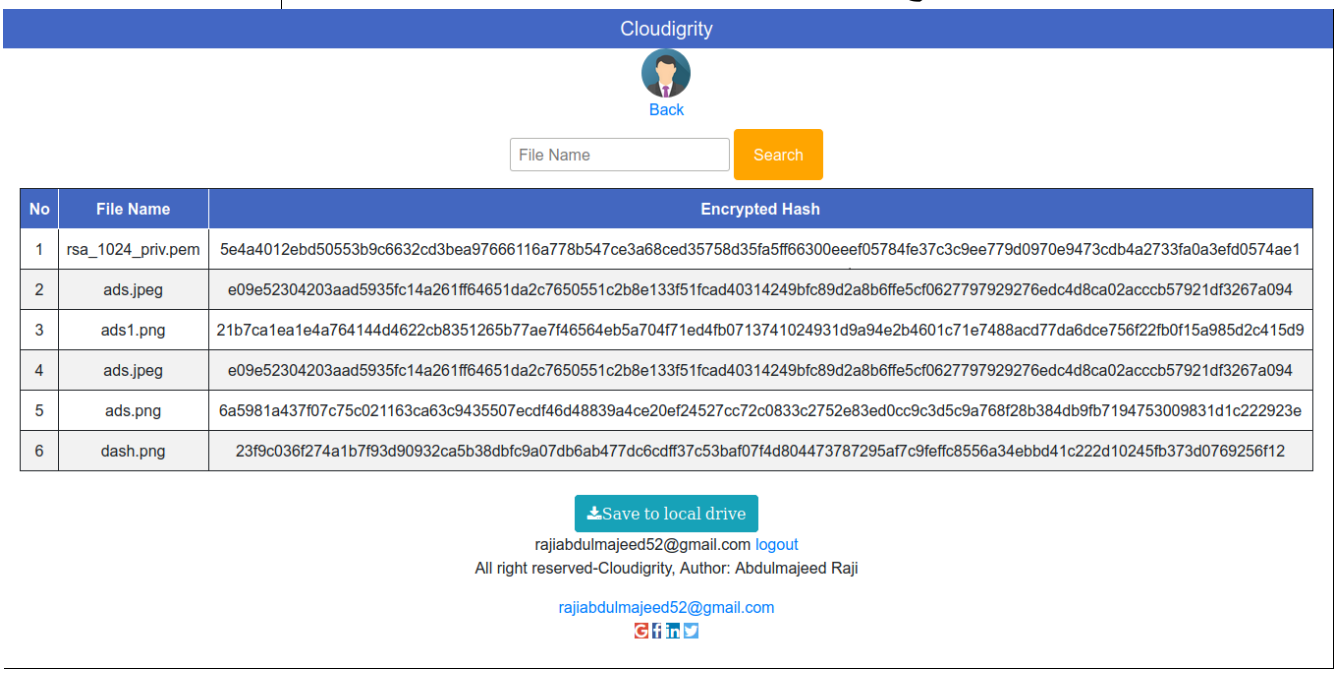
الشكل (13.4) التصميم للصفحة لحذف الملف

الصفحة لتحديث الملف : يوضح الشكل14.4 أدناه الصفحة لتحديث الملفات.



الشكل (14.4) التصميم للصفحة لتحديث الملف

الصفحة لهاشات الملف : يوضح الشكل 15.4 أدناه الصفحة لهاشات الملفات.



الشكل (15.4) التصميم للصفحة لهاشات الملف

2.4 التنفيذ و التجارب

تم بناء نموذج الأولي لموقع مع العديد من المكونات, الشكل16.4 يظهر الصفحة الرئيسية للنظام. بعد التنفيذ وكتابة الكود تم تجربة عليه بشكل عام وأثبتت انه يؤدي مهامه الوظيفي وانه سليم من الاخطاء.

الشكل(16.4). الصفحة الرئيسية للنظام

تم إجراء خمس تجارب على تطبيقنا لإظهار قدرتها على التحقق من سلامة الملفات والسماح للمستخدمين المصادق عليهم فقط بالوصول إلى الملفات، ويمكن إدراج هذه التجارب على النحو التالي:

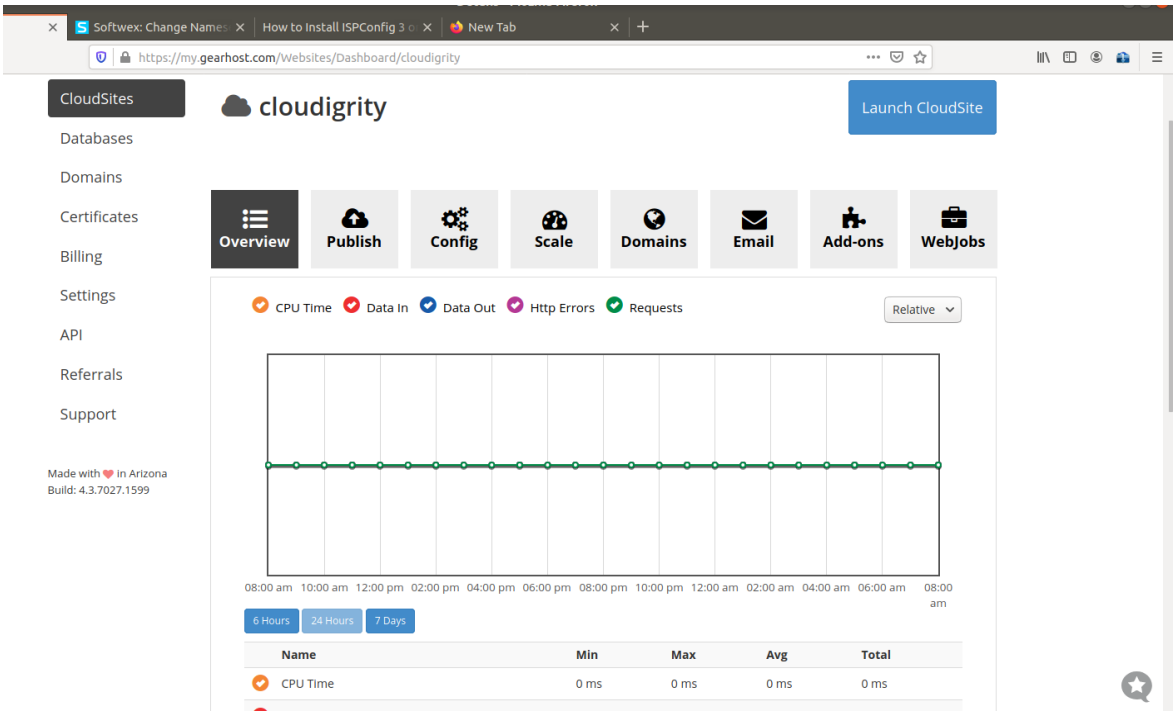
1. استخدام مفتاح خاص خاطئ أثناء محاولة الوصول إلى حساب المستخدم.
2. استخدام رجل في منتصف الهجوم لمعرفة ما إذا كان يمكن تحرير ملفات المستخدم أثناء إرسالها أو تلقيها من السحابة.
3. استخدام أحجام ملفات مختلفة لاختبار التحقق من تكامل البيانات.
4. اختبار جميع وحدات النموذج.
5. استخدام طريقة لتغيير بعض وحدات البايت في أي ملف (طريقة الاختراق) ومعرفة ما إذا تم الكشف عن فشل تكامل البيانات.

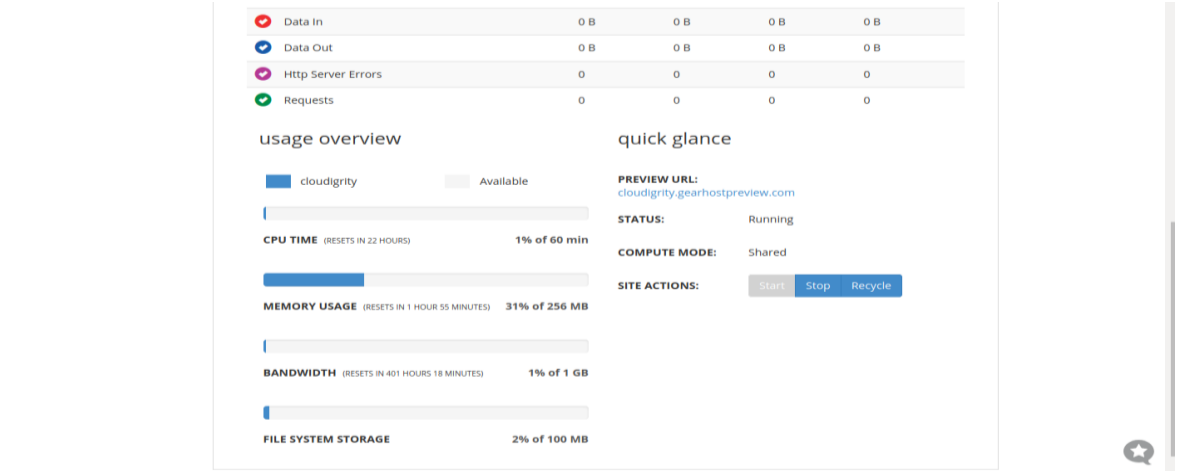
1.2.4 البيئة والأدوات التجريبية

يتم إجراء تجاربنا مع جهاز كمبيوتر محمول (HP)، يعمل بنظام تشغيل Linux (Ubuntu x64 bits) مع core i5، مع ذاكرة RAM 6 جيجابايت.

2.2.4 إعداد سحابة عامة

لقد أنشأنا موقعًا على الويب يمكّن المستخدمين من تحميل ملفاتهم أو تحديثها أو قراءتها أو حذفها. يتم استضافة هذا الموقع على منصة GearHost عبر الإنترنت Cloud Platform كخدمة كما هو مبين في الشكل 17.4 المضيف سحابة العامة. يمكن الوصول إلى الموقع على http://cloudigrity.gearhostpreview.com.



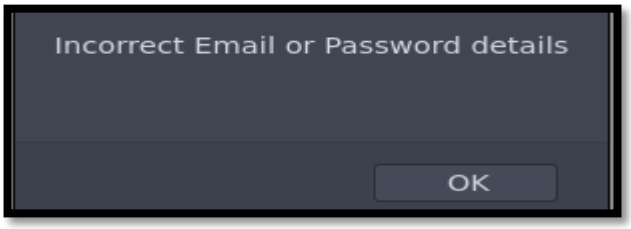


الشكل (17.4): مضيف السحابة العامة

3.2.4 التجارب للنموذج

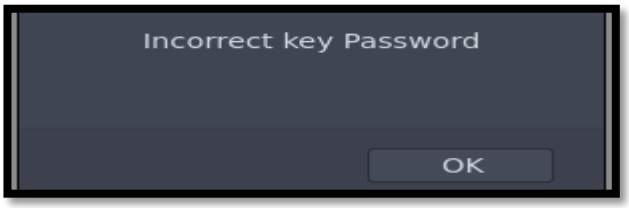
بعد جمع مجموعة بيانات مناسبة (تحتوي على أحجام مختلفة)، تم إنشاء أربعة أنواع مختلفة من التجارب.

التجربة (1)، الوصول إلى حسابات المستخدمين باستخدام اسم مستخدم / كلمة مرور للوصول إلى الحساب: أول تجربة استخدام اسم مستخدم / كلمة مرور غير صحيحة. أثبت النموذج أنه لا يمكن الوصول إلى الحساب باستخدام كلمة مرور خاطئة كما هو موضح في الشكل 18.4.



الشكل (18.4): التجربة الأولى

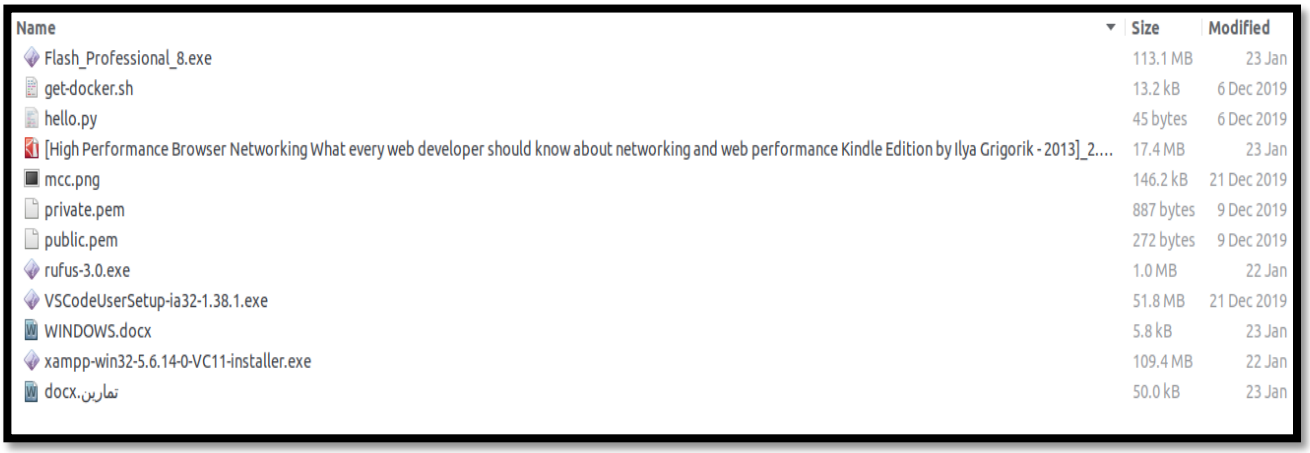
التجربة (2)، الوصول إلى حسابات المستخدمين باستخدام كلمة مرور زوج / مفتاح زوج خاطئ للوصول إلى الحساب: التجربة الثانية هي استخدام أزواج مفاتيح خاطئة للتوثق متعددة العوامل، كما هو متوقع لا يمكن الوصول إلى الحساب بأزواج أو مفاتيح خاطئة إقران كلمة المرور كما هو موضح في الشكل19.4.



الشكل (19.4): التجربة الثانية

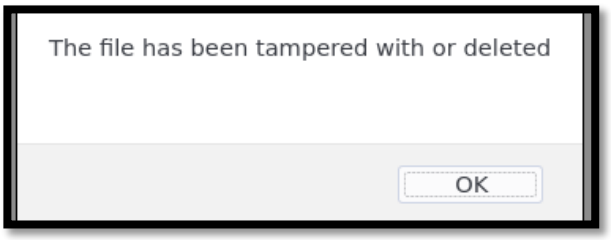
التجربة (3)، تحميل / تنزيل الملفات على السحابة: أثناء تحميل / تنزيل الملفات وإتاحة الفرصة للمتطفل للوصول بشكل غير قانوني إلى الملف، هل يمكنه قراءة الملفات أو تحريرها في الوسط: حيث يتم تشفير الملفات أثناء التحميل والتنزيل حتى إذا تمكن المتسلل من الوصول إلى الملفات، فسيكون من الصعب فك تشفيرها لأنه لا يمكنه الحصول على المفتاح الخاص للمستخدم أو المزود السحابية.

التجربة (4)، والكشف عن انتهاك سلامة الملفات بعد القرصنة المقصود: محاولة تعديل محتوى الملف دون تعديل قيمة هاش. تم تحميل العديد من أنواع وأحجام الملفات على حساب المستخدم كما هو موضح في الشكل 20.4 وتم تخفيف بعض الملفات.



الشكل (20.4): التجربة الرابعة

بعد تعديل محتويات الملف، كان النظام قادرًا على اكتشاف أي تغيير في انتهاك السلامة وبالتالي كما هو موضح في الشكل 21.4.



الشكل (21.4): التجربة الخامسة

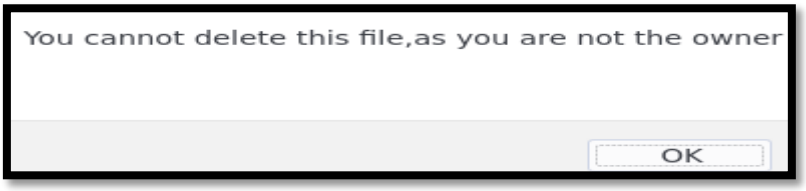
التجربة (5)، قم بتحديث الملف نفسه عدة مرات متتالية لاختبار ما إذا كان يتم إعادة حساب قيمة هاش بعد كل تحديث دون أي تعارض: بما أن دالة هاش (SHA3) لا يوجد بها تضارب، فإن كل ملف مختلف له قيمة تجزئة فريدة كما هو موضح في الجدول 1.4.

جدول (1.4): مثال لتجزئة SHA3-512

Text	Hash value in SHA3-5 Examples 12
My name is Abdulmajeed	f9cd0dfcd13d73aa7868c3ea83baf75f205bfb71b141cf6546f685e67d7b7713b8a62e6f9d88ac63405dab1bb17b83426b0b7eb8c152cac4464c51d6f4aef009
My name is	84c29669d6b2c3fd26088c445e3942a18c7584b196b09f2b26410f58ca71cf5aa3a0d437c4d0952880eaf9daabdd77318afe71238f797d05c7e335015b5c885d
My name	784d7296672a4505e113ed36c38dcb428a811a0c3fb1239ea6bc2d46049aeafd2e09bdeceed3c83cf7b5cb6e7705354466fab74e4833cae6418ce8bd5a44d124

التجربة (6)، القرصنة بواسطة أنواع مختلفة من التعديل، قم بتعديل أجزاء صغيرة جدًا من محتويات الملف لاختبار ما إذا كانت قيمة هاش قد تغيرت أم لا: بعد تعديل محتويات الملف بغض النظر عن صغر حجمها، كان النظام قادرًا على اكتشاف أي تغيير في الملف وبالتالي انتهاك السلامة.

التجربة (7)، حذف ملف من قبل مستخدم ليس منشئ الملف: يثبت النظام أن منشئ الملف فقط يمكنه حذف ملف يمكن للمستخدمين الآخرين فقط عرضه أو تنزيله كما هو موضح في الشكل22.4.



الشكل (22.4): التجربة السابعة

3.4 تقييم النموذج

المقياس الأكثر أهمية في نموذجنا هو الدقة، من حيث الأمن؛ يتم قياسه من خلال تمكين المستخدمين من تنزيل الملفات وتحميلها بشكل آمن وأيضًا إجراء تغييرات غير قانونية على ملف المستخدم واكتشاف انتهاك تكامل هذا الملف عند كل وصول. يتمثل الإجراء الآخر في تقييم نظام التوثق من خلال محاولة الوصول إلى حسابات المستخدمين باستخدام تفاصيل تسجيل دخول خاطئة (كلمة المرور والتوقيع الرقمي).

1.3.4 تقييم الدقة

تشير الدقة إلى ما إذا كانت البيانات تسجل بشكل صحيح كائن الأعمال أو الحدث الذي تمثله. له متطلبان: يجب أن تكون القيمة الصحيحة ويجب أن تمثل القيمة في شكل متسق مع جميع العروض الأخرى التي لها نفس القيمة.

ينصب تركيزنا على تحميل الملفات وتنزيلها بشكل آمن والتحقق من انتهاك سلامة الملفات التي تم تحميلها. أجريت ثلاث تجارب من أجل تقييم الدقة:

1. أثناء نقل الملف إلى مجموعة النظراء، قم بإجراء التحرير (القرصنة) على تفاصيل الملف ومعرفة ما إذا كانت السحابة لا تزال تحفظ الملف المخترق. (التحرير عن طريق: إضافة وحذف وتغيير البايتات في الملف) ،
2. أثناء نقل الملف إلى المستخدمين، قم بإجراء التحرير (القرصنة) على تفاصيل الملف ومعرفة ما إذا كان المستخدم يعترف بأن الملف صحيح أم لا. (التحرير عن طريق: إضافة وحذف وتغيير بايت في الملف).

3. قم بإجراء تغييرات (القرصنة) على قيمة هاش"SHA3" لملف ومعرفة ما إذا كانت السحابة / المستخدم يتعرف على التغيير. لقد وجدنا أن "SHA3" مقاوم لهجمات التصادم، حيث لا يوجد أي تطابق بين قيمتي تجزئة ملفين.

بعد إجراء جميع هذه الاختبارات، وجدنا أن نظامنا قادر على ضمان تحميل وتنزيل ملف آمنين من وإلى المستخدم وأيضًا ضمان دقة الملفات واكتشاف كل نوع من تعديلات الملفات.

2.3.4 تقييم نظام التوثق

ينصب تركيزنا على منح الوصول الآمن للمستخدمين الذين تم التحقق منهم إلى الحساب، وقد أجريت التجارب التالية، من أجل تقييم الدقة:

1. تسجيل الدخول باستخدام اسم المستخدم وكلمة المرور خاطئة.
2. قم بإجراء تغييرات على أزواج المفاتيح وحاول تسجيل الدخول ومعرفة ما إذا تم التحقق من الشهادة الرقمية أم لا.
3. افترض كلمة مرور مستخدم هاش للتجزئة، هل يمكنه تخمين المفتاح الخاص / المفتاح العام بشكل صحيح.

بعد إجراء هذه الاختبارات، وجدنا أن نظامنا قادر على ضمان وصول آمن وموثوق للحساب طالما ظلت أزواج المفاتيح آمنة.

ملخص

في هذا الفصل قدمنا تصميم للنموذج من حيث تصميم قاعدة البيانات و تصميم العمليات وتصميم الواجهات للموقع ثم التنفيذ باستخدام العديد من الأدوات والبرامج التي تتضمن لغة PHP وجافا سكريبت و OpenSSL وغيرها. قدمنا الوظائف الرئيسية للنموذج الذي يتضمن (إنشاء الحساب، تسجيل الدخول إلى الحساب، تحميل الملف، تنزيل الملف، التحقق من سلامة الملف، عرض الملف، تحديث الملف، حذف الملف، تنظيم أذونات عمليات الملفات (القراءة أو الكتابة) وعرض ملف السجل) ويتم نشر النموذج المطبق على السحابة العامة. تم تقديم التجارب التي أجريت على نموذجنا وتم تحليل النتائج، وأيضًا تقييم النظام، لتعزيز نظام للتوثق المستخدم والتحقق من سلامة البيانات في السحابة

العامة باستخدام توثق متعددة العوامل (كلمة المرور والتوقيع الرقمي) وباستخدام خوارزمية هاش الآمنة "SHA3" لفحص تكامل البيانات. لقد استنتجنا أن هذا النموذج فعال وموثوق للتوثق المستخدم والتحقق من تكامل البيانات.

الفصل الخامس

النتائج,التوصيات والخاتمة

5. مقدمة.

نقدم النتائج ومناقشات النتائج والمساهمات والتوصيات لدراسات المستقبلية ثم الخاتمة.

1.5 النتائج

في هذه البحث، نعالجٍ مشكلة توثق المستخدم والتحقق من سلامة الملفات في السحابة العامة من خلال تصميم نموذج لخدمة التوثق للمستخدم الآمنة، وخدمة تحميل / تنزيل ملف آمن، وخدمة تجزئة الملفات الآمنة. حصلنا على النتائج التالية.

1. تحسين الأمن السحابية العام لمستخدمي السحابة من خلال اعتماد نظام التشفير المتماثل وغير المتماثل.
2. اقترحنا نموذجًا جديدًا لتأمين بيانات المستخدم؛ يوفر النموذج للتوثق المستخدم والتحقق من سلامة الملفات والسرية.
3. أثبتت التجارب التي أجريت أن نموذجنا المقترح قابل للتطبيق وقوي ضد هجمات تكامل والتوثق.
4. أثبتت التجارب التي أجريت أيضًا أن أداء النموذج مقبول نظرًا لأنه يتم استخدام طاقة حساب أقل لتحقيق درجة عالية من الأمان.
5. يوفر النموذج الكشف السريع عن التلاعب غير المصرح به أو تغيير الملفات.
6. يوفر النموذج مستويين من التوثق للمستخدم، والذي يتضمن كلمة المرور والتوثق المستندة إلى الشهادة، والتي تستخدم التوقيع الرقمي.
7. يحمي النموذج البيانات أثناء النقل والتخزين في السحابة.
8. أثبتت التجارب التي أجريت أن النموذج يمكن استخدامه لأي نوع وحجم ملف بسهولة وبسرعة.
9. يثبت النموذج أنه حتى مزودي الخدمة السحابية لا يمكنهم تعديل الوصول إلى الملفات المحمية الخاصة بالمستخدمين، وبالتالي فإن الملفات محمية ضد انتهاكات السحابة على الرغم من وجود مستوى جيد من الثقة بين مزود السحابة ومستخدمي السحابة.

2.5 مناقشات النتائج

يعمل هذا النموذج على تحسين الأمان السحابية العام من خلال اعتماد استخدام التشفير المتماثل وغير المتماثل، وفي التشفير المتماثل نستخدم نظام التشفير المتقدم "AES" (نظام التشفير المتقدم) حيث يتم إنشاء مفتاح جلسة لتشفير الملفات لإنشاء نقل آمن ونستخدم تشفير "RSA" تشفير قيم هاش الناتجة لأي بيانات يتم تحميلها أو تنزيلها.

اقترحنا نموذجًا جديدًا لتأمين بيانات المستخدم؛ يوفر النموذج للتوثق المستخدم والتحقق من سلامته وسريته، ويتم تعزيز للتوثق المستخدم من خلال التوثق متعددة العوامل ويستخدم نظام التحقق من تكامل البيانات خوارزمية هاش الآمنة وللسرية، نستخدم نظام التشفير المتماثل وغير المتماثل.
يضمن النموذج المقترح أن المستخدمين الذين تم التحقق منهم فقط يمكنهم الوصول إلى الحساب باستخدام التوثق متعددة العوامل لكلمة المرور والتوثق المستندة إلى الشهادة. كما يتم تشفير جميع الملفات والبيانات أثناء إرسالها إلى الموفر السحابية / المستلم من قبل المستخدم، وهذا يجعل من المستحيل على المهاجم عرض المحتويات أو تحريرها إلا إذا كان لديه حق الوصول إلى أزواج المفاتيح لمزود السحابة والمستعمل. يضمن النموذج المقترح أيضًا تشفير الملفات التي يتم الاستعانة بمصادر خارجية إلى السحابة باستخدام نظام تشفير التناظر المتماثل بها "AES" وغير المتماثل بها "RSA" قبل إرسالها. قبل تحميل ملف، يتم إنشاء قيمة هاش (SHA3) وتشفيرها والتي يمكن استخدامها في أي وقت للتحقق من سلامة الملف عن طريق إنشاء قيمة تجزئة جديدة ومقارنتها بقيمة هاش السابقة التي تم إنشاؤها أثناء تحميل الملف.

أجريت تجارب على النموذج المقترح باستخدام أنواع وأحجام ملفات مختلفة لضمان قدرة النموذج على السماح للمستخدمين المصادق عليهم فقط والكشف عن فشل تكامل البيانات في الملفات التي تم الاستعانة بمصادر خارجية فيها وتقييم دقتها. تثبت التجارب أيضًا أنه حتى مزودي السحابة لا يمكنهم تعديل الوصول إلى الملفات المحمية الخاصة بالمستخدمين، وبالتالي فإن الملفات محمية ضد انتهاكات السحابة على الرغم من وجود مستوى جيد من الثقة بين مزود السحابة ومستخدمي السحابة. يوضح النموذج أيضًا أن الأداء فعال للغاية حيث يتم استخدام طاقة حسابية أقل لتحقيق درجة عالية من الأمان.

مع هذا، حققنا أهداف هذا البحث. كما حققنا الهدف (1 و2) في الفصل الثاني حيث ناقشنا ودرسنا بداية فن الأمن في الحوسبة السحابية. لقد حققنا الهدف (1 و2) أيضا في الفصل الثالث حيث

قمنا بدراسة وتلخيص نموذج أمان تكامل البيانات المعروف. وتم تحقيقه هدف رقم (3) من حيث تم اقتراح نموذج حماية تكامل البيانات وتم التأكد من أن البيانات المخزنة كما كانت قبل إرسال وإنشاء جلسة آمنة تم تحقيق هدف حيث يستخدم نموذجنا وظيفة تجزئة SHA3 لحساب قيمة تجزئة الملف والتي يمكن استخدامها لاحقًا للتحقق سلامتها. كما استخدمنا "AES" للتشفير المتماثل و"RSA" للتشفير غير المتماثل للملفات. لقد حققنا اهداف هذا البحث الذي أثبتت تجاربنا أن النموذج يخدم نظام التوثق قويًا باستخدام كلمة المرور والتوقيع الرقمي. أخيرًا، تم تحقيق الهدف (3) أيضا حيث تم تطبيق نموذجنا المقترح ونشره في بيئة سحابية عامة وتم اختبار دقته، بعد إجراء العديد من التجارب والاختبارات في بيئة سحابية عامة حية، تحققنا من أن النموذج في مستوى مقبول وفعالة للغاية للتوثق المستخدم وفعالة ضد التعديل الضار للبيانات.

3.5 المساهمة

1. لقد حددنا نظام توثق مستخدم آمن يستخدم شهادة رقمية لدعم نظام اسم المستخدم وكلمة المرور التقليديين، مما يتيح للمستخدم تسجيل الدخول الآمن إلى حساباتهم دون خوف من الوصول غير القانوني إلى الحساب. بعد أن يقوم المستخدم بإدخال اسم المستخدم وكلمة المرور الخاصة به يتم إرسالها إلى الخادم للتحقق منها، يتم إجراء التوثق المستندة إلى الشهادة. توفر هذه الخدمة أمانًا عاليًا للتوثق المستخدم وتوفر سرية بيانات اعتماد تسجيل الدخول التي يتم توصيلها بين المستخدم والسحابة، والتي يمكن استخدامها محليًا أو عن بُعد.
2. حددنا أيضًا نظامًا آمنًا لتحميل الملفات وتنزيلها والذي يستخدم استخدام الشهادة الرقمية وخوارزمية هاش الآمنة، ويتم تشفير الملفات وتجزئها قبل التحميل / التنزيل، كما يتم الاحتفاظ بقيم تجزئة الملفات مشفرة حتى لا يكون لدى المستخدم أي عدالة. الهجوم على ملف هاش. مقارنة بـ [51] حيث يتم تخزين قيم تجزئة الملفات دون تشفيرها مما يجعلها مفتوحة للهجمات. النظام المقترح لا يدعم التحقق من سلامة الملفات فحسب، بل يدعم أيضًا السرية وعدم التنصل.

4.5 توصيات

كما قد تظهر التحديات المستقبلية، نوصي بما يلي:

1. يمكن تحسين النظام للتحقق من سلامة الملفات ديناميكية التي يشاركها عدة مستخدمين في نفس الوقت.
2. لخصوصية الملفات، يمكن عرض الملفات أو الوصول إليها من قبل المستخدمين المسموح لهم فقط.
4. توسيع نطاق العمل لتشمل توطين الخطأ واستعادة الخطأ.
5. يمكن إجراء مزيد من الدراسات لحل مشكلة التصيد الاحتيالي، والتي يمكن استخدامها للحصول على بيانات اعتماد تسجيل دخول المستخدم.
6. يمكن تنفيذ النموذج على تطبيق الأجهزة المحمولة حيث إننا نطبق فقط للأنظمة المستندة إلى الويب.
7. يمكن ترقية النموذج للتكيف مع خوارزميات الأمان الجديدة.

5.5 الخاتمة

في هذا البحث، عالجنا مشكلة توثق المستخدم والتحقق من سلامة الملفات التي يتم الاستعانة بمصادر خارجية في السحابة العامة بسبب وجود اتجاه متزايد نحو الاستعانة بمصادر خارجية البيانات بها إلى خوادم سحابة عن بعد وأنه من الضروري التأكد من أن البيانات يتم الاحتفاظ بشكل صحيح وضمان سلامتها بشكل صحيح. مع الأخذ في الاعتبار تقنيات التوثق القوية هذه يجب تنفيذها لمنع الوصول غير القانوني أو غير المصرح به إلى الملفات، مما قد يؤدي إلى فشل تكامل البيانات. درسنا الحالة الراهنة للأمن في الحوسبة السحابية وقمنا بتحليل النماذج المقترحة مسبقًا المستخدمة للتحقق من سلامة البيانات في السحابة. ننتقل إلى تطوير نموذجنا الذي يستخدم كلمة المرور و"المصادقة القائمة علي الشهادة" للتوثق القوية للمستخدم، ويستخدم النموذج خوارزمية هاش الآمنة للتحقق من سلامة الملفات ونظام تشفير متماثل وغير متماثل لتعزيز الاتصال الآمن للملفات. تم تنفيذ النموذج باستخدام العديد من الأدوات الحديثة ولغات البرمجة وتم نشر موقع ويب النموذج الأولي في بيئة السحابة العامة. تم إجراء العديد من التجارب وأثبتت أن النموذج يدعم التوثق القوية للمستخدم والتحقق من سلامة الملف وسرية الملف وعدم التنصل.

المراجع

[1] P. Mell and T. Grance, "The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology" Special Publication 800-145.2011

[2] Sultan Aldossary* and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions "(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[3] https://aws.amazon.com/what-is-cloud-storage/. Accessed on 18/08/2019 4:00pm.

[4] https://aws.amazon.com/agreement/. Accessed on 18/08/2019 4:04pm.

[5] Michael Arrington "Gmail Disaster: Reports on Email deletions" Available at https://techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/.

[6] Suneeta Mohanty ,Mrinmoy Ganguly,Prasant Kumar Pattnaik, "CIA Triad for Achieving Accountability in Cloud Computing Environment" International Journal of Computer Science and Mobile Applications, National Conference on "The Things Services and Applications of Internet of Things", Gandhi Institute for Education and Technology (GIET) Baniatangi, pg. 39-44. ISSN: 2321-8363. Impact Factor: 5.515 available online at http://ijcsma.com/publications/NCSIOT/NCSIOT06.pdf. 23-24 March 2018.

[7] Navi Mumbai, "Third Party Public Auditing scheme for Cloud Storage" 7th International Conference on Communication, Computing and Virtualization 2016 .Available online www.sciencedirect.com.

[8] Wale Amol D and Vedant Rastogi ," Data Integrity Auditing of Cloud Storage" , International Journal of Computer Applications (0975 – 8887) Volume 133 – No.17, January 2016

[9] Jaspreet Kaur & Jasmeet Singh , "TPA Ensuring Data Integrity in Cloud Environment" ,lobal Journal of Computer Science and Technology Software & Data Engineering Volume 13 Issue 13 Version 1.0.Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350 ,2013.

[10] Neha Thakur and Aman Kumar Sharma "Data Integrity Techniques in Cloud Computing: An Analysis", International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-8), 2017.

[11] Dr. Rahma Teirab and Dr. Ahmed Khameis Sharaf ,"A Survey on Cloud Computing Techniques for Data Integrity Checking" ,International Journal of Innovation Education and Research www.ijier.net Volume:-7 No-6, 2019

[12] Ramakrishnan Krishnan, "Security and Privacy in Cloud Computing", Master's thesis Western Michigan University 2017.

[13] "Cloud Computing "available at https://www.javatpoint.com/virtualization-in-cloud-computing accessed on 15-09-2019 09:00pm.

[14] Mai Mansour Dahshan, "Data security in cloud storage services" Theses at THE AMERICAN UNIVERSITY IN CAIRO, SCHOOL OF SCIENCES AND ENGINEERING, 2013.

[15] Textbook by The art of service, "Cloud computing – The complete cornerstone guide to cloud computing best practices ", Australia, link to website: http://theartofservice.com.

[16] Murtada Malik 1 and Hana GesmElseed , " Improving User Data Security in Cloud Computing Using AES (Rijindel) , RSA, Two fish Encryption and SHA- 256 Algorithms" Faculty of Computer Science and Information Technology ,2017.

[17] Textbook by Judith Hasurwitz ,Robin Bloor , Marcia Kaufman ,Fern Halper ," Cloud Computing Delivery Models " link to book https://www.dummies.com/programming/networking/cloud-computing-delivery-models/

[18] Ahmed Lounis,"Security in cloud computing ", PhD thesis, other. Université de Technologie de Compiègne, 2014. English. NNT: 2014COMP1945. Tel-01293631, 2016.

[19] Yuliya Shaptunova, "Top 4 Cloud delivery models you need to know", link to website https://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/ Accessed on 18/09/2019 9:04pm.

[20] Textbook by Tutorialspoint.com "Cloud computing tutorial"

[21] Anthony T. Velte and Toby J. Velte, Ph.D. and Robert Elsenpeter," Cloud Computing: A Practical Approach", MC Graw hill companies, New York ISBN: 978-0-07-162695-8.MHID: 0-07-162695-6, 2010.

[22] "NIST Cloud Computing Standards Roadmap", NIST Special Publication 500-291, Version 2 (Supersedes Version 1.0, July 2011), July 2013.

[23] Muhammad Kazim and Shao Ying Zhu, "A survey on top security threats in cloud computing" , (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[24] CSA Releases New Research - Top Threats to Cloud Computing: Egregious eleven. Accessed at https://cloudsecurityalliance.org/articles/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/. Accessed on 27th September 2019.

[25] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[26] Bob Violino, "The dirty dozen: 12 top cloud security threats", link: https://www.csoonline.com/article/3043030/the-dirty-dozen-12-top-cloud-security-threats.html. Accessed on 27 September 2019.

[27] James Sanders, "Data breaches increased 54% in 2019 so far", link: https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/, Accessed on 27 September 2019.

[28] CSA Releases Top Threats to Cloud Computing: Deep Dive, Link: https://cloudsecurityalliance.org/articles/csa-releases-top-threats-to-cloud-computing-deep-dive/ Accessed on 27 September 2019.

[29] Jerry Archer et all," Top Threats to Cloud Computing V1.0" Prepared by Cloud security alliance. 2010.

[30] Lawrence Abrams ,"Amazon AWS Outage Shows Data in the Cloud is Not Always safe" , Link :https://www.bleepingcomputer.com/news/technology/amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe/?fbclid=IwAR2fgzFqQYRzDffhtH4uigSl_ATDeMut_QEnGX5oy2x9KiamBDKOZ8cydVM. , Accessed on 27 September 2019.

[31] Christine Haughney and Nicole Perlroth ," Times Site Is Disrupted in Attack by Hackers - 2013" Link to article: https://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html.Accessed on 27 September 2019.

[32] Sreenivas Sremath Tirumala and Hira Sathu and Vijay Naidu, "Analysis and Prevention of Account Hijacking based INCIDENTS in Cloud Environment" DOI: 10.1109/ICIT.2015.29 Conference: 14th International Conference on Information Technology, ICIT-2015, and At Bhubaneswar, India. 2015. Link paper: https://www.researchgate.net/publication/284158931_Analysis_and_Prevention_of_Account_Hijacking_based_INCIDENTS_in_Cloud_Environment.

[33] Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013". Link: http://www.cloudsecurityalliance.org/topthreats 2013.

[34] Jan de Muijnck-Hughes," Data Protection in the Cloud "Master's thesis 2011.

[35] Takahiko Koriyama, "CLOUD COMPUTING SECURITY: HOW RISKS AND THREATS ARE AFFECTING CLOUD ADOPTION DECISIONS", MSc thesis San Diego State University, 2012.

[36] https://searchsecurity.techtarget.com/definition/access-control Accessed on 29th September 2019 8:19pm.

[37] Jscambler, "Article on hashing algorithm" Accessed on https://blog.jscrambler.com/hashing-algorithms/ Accessed on 29th September 2019 8:19pm.

[38] https://en.wikipedia.org/wiki/Digital_signature#The_current_state_of_use_%E2%80%93_legal_and_practical Accessed on 30th September 2019 4:44am.

[39] Pokharel, M., Lee, S., & Park, J. S. "Disaster Recovery for System Architecture using Cloud Computing". (2010).

[40] Patil, S. R., Shiraguppi, R. M., Jain, B. P., & Eda, S," Methodology for Usage of Emerging Disk to Ameliorate Hybrid Storage Clouds", IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp.1-5). 2012. Link : http://dx.doi.org/10.1109/CCEM.2012.6354615

[41] Mohammad Ali Khoshkholghi and Azizol Abdullah and Rohaya Latip and Mohamed Othman, "Disaster Recovery in Cloud Computing: A Survey", Published by Canadian Center of Science and Education , ISSN 1913-8989 ,E-ISSN 1913-8997, Computer and Information Science; Vol. 7, No. 4; 2014.

[42] Mr.Akshay A. Gharat, Mr. Devendra E. Mhamunkar, "Disaster Recovery in Cloud Computing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015

[43] Giuseppe Ateniese and Joseph Herring and Randal Burns and Lea Kissner and Reza Curtmola and Zachary Peterson and Dawn Song, "Provable Data Possession at Untrusted Stores", 14th ACM Conference on Computer and Communications Security (CCS 2007).

[44] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files", Proc. *14th ACM Conf. Computer and Communications Security*, 2007.

[45] K David Raju, K Vijay Kumar *, K Anthony Rahul Showry, B Lohit Krishn, " Techniques of providing data integrity in cloud computing", International Journal of Engineering & Technology, 7 (1.1) (2018) 223-225

[46] Seyed Milad Dejamfar and 2 Sara Najafzadeh, "Authentication Techniques in Cloud Computing: A Review " , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 1, January 2017, Available online at: www.ijarcsse.com.

[47] Dr. Rahma Teirab Abaker Haroun and Dr. Ahmed Khameis Sharaf Eldein AlKabour , " A Survey on Cloud Computing Techniques for Data Integrity Checking" , International Journal of Innovation Education and Research .Online ISSN :2411-2933 PRINT -ISSN :2411-3123, Available at: www.ijier.net .Volume :-7 No-6, 2019.

[48] Ku. Swati G. Anantwar and Prof. Karuna G. Bagde, “Data Integrity and Security in Cloud”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.

[49] Nedhal Al-Saiyd and Nada Sail, “Data integrity in cloud computing security”, Journal of Theoretical and Applied Information Technology · December 2013 Available at: https://www.researchgate.net/publication/259493377.

[50] B. Mahalakshmi and Suseendran G. ,” An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions: Proceedings of ICDMAI 2018, Volume 2” ,Chapter in Advances in Intelligent Systems and Computing · January 2019 ,Available at: https://www.researchgate.net/publication/327536170

[51] Safaa Taher Lulu,” A Model to Detect the Integrity Violation of Shared File in the Cloud”, MSc Theses, The Islamic University–Gaza, 2017.

[52] Morovat Katanosh, "Data Integrity Verification in Cloud Computing" (2015). Theses and Dissertations. 1125. Available at : http://scholarworks.uark.edu/etd/1125

[53] “Text book :Cloud Computing Tutorial”

[54] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu ,”Data Security and Privacy in Cloud Computing “, “International Journal of Distributed sensors” ,2014 ,Available at https://journals.sagepub.com/doi/full/10.1155/2014/190903

[55] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. Weippl, " Dark clouds on the horizon: Using cloud storage as attack vector and online slack space," In Proceeding of the 20th USENIX Conference on Security, 2011.

[56] Securing the worlds data, link to article https://spideroak.support/hc Accessed 20 November 2019.

[57] W.Hu, T. Yang, and J. N. Matthews. "The good, the bad and the ugly of consumer cloud storage." ACM SIGOPS Operating Systems Review, pp. 110–115, 2010.

[58] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M. Richter, U. Viebeg, and S. Vowe, "On the Security of Cloud Storage Services," Fraunhofer Institute for Secure Information Technology SIT, March, 2012, [Online]. Available: http://www.sit.fraunhofer.de/en/cloudstudy.html

[59] E. Hamburger ,"Google Drive vs. Dropbox, SkyDrive, SugarSync, and others: a cloud sync storage face-off," The verge, April 24, 2012, [Online].Available:http://www.theverge.com/2012/4/24/2954960/google-drive-dropbox-skydrive-sugarsync-cloud-storage-competition

[60] W. Mossberg, "Many Devices, Many Files and Four Ways to Share Them," All Things, July 31, 2012, [Online]. Available: http://allthingsd.com/20120731/many-devices- many-files-and-four-ways-to-share-them.

[61] "Open Source vs. Proprietary Software," bloomtools, January 31, 2012. [Online]. Available: http://www.bloomtools.com/articles/open-source-vs-proprietary-software.html

[62] bS. Lesem, "Understanding Cloud Storage APIs: Standards, Functions, Lock-in, and what's Next," November 17, 2009, [Online]. http://cloudstoragestrategy.com/2009/11/understanding-cloud-storage-apis.html

[63] D. Floyer, "Integration of the Storage Optimization Stack," Wikibon, June 09, 2010, [Online].http://wikibon.org/wiki/v/Integration_of_the_Storage_Optimization_Stack#Storage_Optimization_Techniques

[64] Y. V. Lokeshwari, B. Prabavathy, and ChitraBabu, "Optimized Cloud Storage with High Throughput De-duplication Approach," International Conference on Emerging Technology Trends, 2011.

[65] National Institute of Standards and Technology, systems, "Guide for developing security plans for federal information systems", vol.800-18, February2006, [Online].Availablefrom:http://csrc.nist.govpublications/nistpubs/800-18-Rev1/sp800-18-Rev1final.pdf/, [accessed December 2013].

[66] (2014 - 1997)جون كوجيسهول، سيمون كورتيسي، بيتر كاوبورن، دانيال إيغبرغ ، "PHP Manual "، تم الوصول إليها في ديسمبر. 22، 2019، من http://php.net/manual/en/intro-whatis.php.

[67] Jasode وصلة في "هاكر جديد"، https://news.ycombinator.com/itme?id=14455282 الوصول في 17 يناير 2020. 7:18 مساءً.

[68] GI Global "ما هو نموذج الأمان"،https://www.igi-global.com/dictionaty/reviewing-the-security-features-in-contemporary-security-policies-and-models-for-multiple-platforms/26110..2020/مارس/03 تم الوصول إليها في

[69] أساسيات أمان الكتب المدرسية "إلزامية، تقديرية، دور وقاعدة تحكم بالوصول المستندة إلى قاعدة" الارتباط إلى الصفحة: https://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control..11/01/2020 تم الوصول إليها في

[70] قاسى مانوشا "الحماية: بيل لابادولا النموذجي" رابط: http://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/.11/01/2020 الوصول في

[71] [http://simonpierre.org/inldk25jedhds/ykbjsk4j5hfsd.php?eebxdvz4rff=clark-wilson-model-ppt.11/01/2020 الوصول إليها في

[72] سيمور بوسورث،إم.إي. كاباي، إيريك وايتن. "الكمبيوتر الأمن كتيب الطبعة السادسة" ، 2013041083 ، وصلةhttp://it-ebookdds.info/.

ملحق

تم تقديم ورقة علمية في مؤتمر علوم الحاسوب والتقانة المعلومات السابع – السودان

7th International Conference of computer Science and Information Technology (SCCSIT'7), Khartoum Sudan.

بعنوان

Title: "Enhancing public cloud security by developing a model for user authentication and data integrity checking"

Authors: Abdulmajeed Atoyebi Raji, Murtadha Adam Malik El-hajj.