Cloud Security

أ.نـدى الوادعـي

Security in Cloud:

Cloud Computing is **a security nightmare** and it can't be handled in traditional ways.

John Chambers

- Security in cloud computing is an important concern.
- الأمن في الحوسبة السحابية هو مصدر قلق مهم
- Data in the cloud is necessary to be stored in encrypted form.
- لبيانات في السحابة ضرورية لتخزينها في شكل مشفر
- Encryption helps to protect transferred data as well as the data stored in the cloud.
- يساعد التشفير في حماية البيانات المنقولة وكذلك البيانات المخزنة في السحابة.
- Encryption does not prevent data loss.
- التشفير لا يمنع فقدان البيانات
- It restricts the client from accessing the shared data directly.
- يقيد العميل من الوصول إلى البيانات المشتركة مباشرة.

Security Planning:

- Select which resources to move to cloud and analyze its sensitivity to risk.
- حدد الموارد التي تريد نقلها إلى السحابة وقم بتحليل مدى حساسيتها للمخاطر.
- Consider cloud service models such as IaaS, PaaS, and SaaS.
- ضع في اعتبارك نماذج خدمات السحابة مثل البنية التحتية كخدمة(IaaS) والمنصة كخدمة (PaaS) والبرمجيات كخدمة(SaaS)
- Consider which cloud type such as public, private, community or hybrid.
- أخذ في الاعتبار أيضا أنواع السحابة مثل العامة والخاصة والمشتركة والهجينة
- Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud.
- فهم نظام مزود الخدمة السحابية لكيفية نقل البيانات ومكان تخزينها وكيفية نقل البيانات من وإلى السحابة.

Cloud Security Alliance (CSA):

- A specific service model defines the boundary among the responsibilities of customer and service provider.
- يحدد نموذج خدمة محدد الحدود بين مسؤوليات العميل ومزود الخدمة.
- The boundaries between each service model are defined by Cloud Security Alliance (CSA) stack model.
- يتم تحديد الحدود بين كل نموذج خدمة بواسطة نموذج مكدس Cloud Security Alliance (CSA).

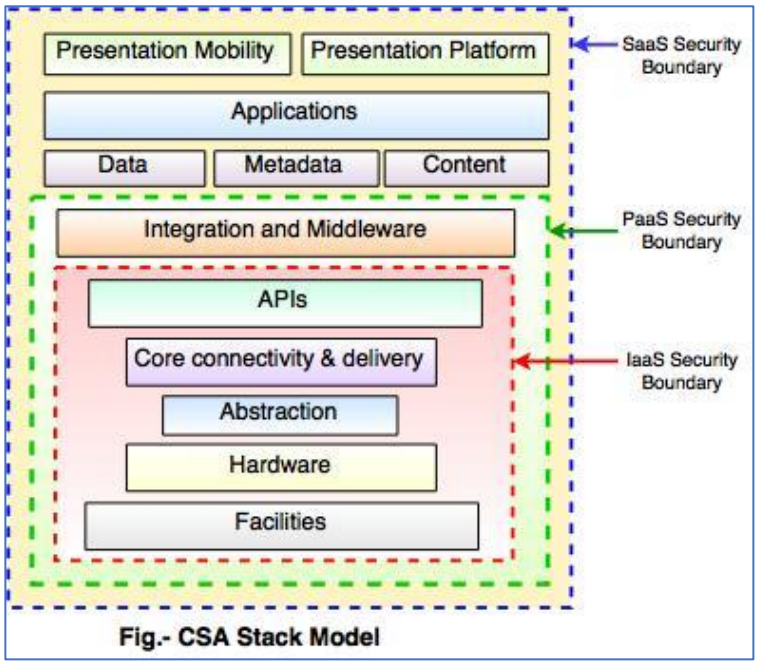


Fig.- CSA Stack Model

Key Points to CSA Model:

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- IaaSهو المستوى الأساسي للخدمة، مع PaaS و SaaSالمستويين التاليين من الخدمات.
- Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- بالانتقال إلى الأعلى، ترث كل خدمة القدرات والمخاوف الأمنية للنموذج الذي يليها.
- IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- توفر IaaS البنية الأساسية، وتوفر PaaS بيئة تطوير المنصة، وتوفر SaaS بيئة التشغيل.

- IaaS has the lowest integrated functionality and security level, while SaaS has the highest.
- تتمتع IaaS بأدنى مستوى من الوظائف المتكاملة والأمان، بينما تتمتع SaaS بأعلى مستوى.

- This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- يصف هذا النموذج حدود الأمان التي تنتهي عندها مسؤوليات مزودي الخدمات السحابية وتبدأ مسؤوليات العملاء.
- Any protection mechanism below the security limit must be built into the system and maintained by the customer.
- يجب أن تكون أي آلية حماية أقل من حد الأمان مدمجة في النظام وصيانتها من قبل العميل.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

على الرغم من أن كل نموذج خدمة لديه آلية أمان، فإن متطلبات الأمان تعتمد أيضًا على مكان وجود هذه الخدمات، سواء كانت خاصة أو عامة أو مختلطة أو سحابية مجتمعية.

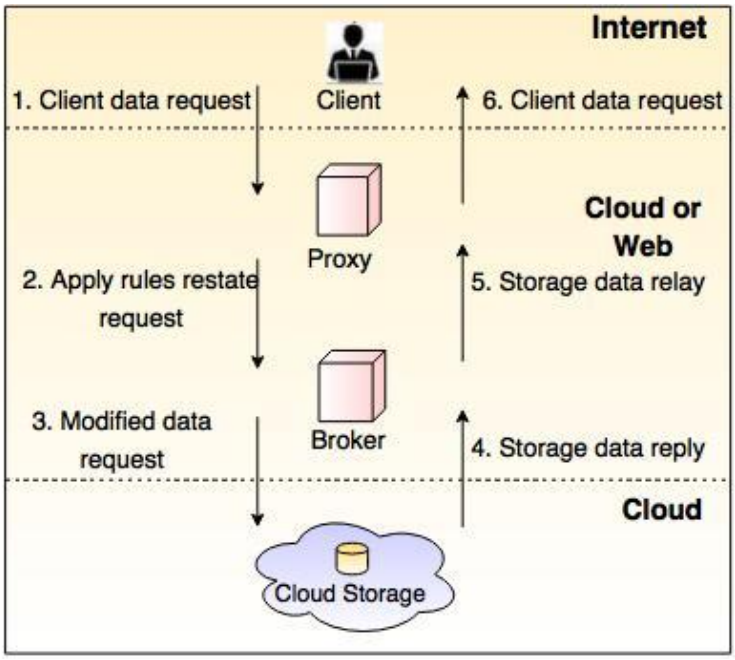
Mechanisms for data protection:

- **Access Control**
  - Ensuring that the access is provided only to the authorized users and hence the data is stored in a secure manner
- لتأكد من أن الوصول متاح فقط للمستخدمين المصرح لهم وبالتالي يتم تخزين البيانات بطريقة آمنة
- **Auditing**
  - Evaluation of the security of a company's information system
- تقييم أمن نظام المعلومات للشركة
- **Encryption**
  - process of making plaintext in to an unreadable format
- عملية تحويل النص العادي إلى تنسيق غير قابل للقراءة
- **Authentication**
  - Ensuring that the right entity is accessing the data.
- التأكد من وصول الجهة الصحيحة إلى البيانات.
- **Authorization**
  - user submits its user identity in order to login to a particular service.
- يقدم المستخدم هوية المستخدم الخاصة به من أجل تسجيل الدخول إلى خدمة معينة.

ISOLATED ACCESS TO DATA:

- Data stored in cloud can be retrieved from anywhere, hence it should have a mechanism to isolate data and protect it from client's direct access.
- يمكن استرجاع البيانات المخزنة في السحابة من أي مكان، وبالتالي يجب أن يكون لديها آلية لعزل البيانات وحمايتها من الوصول المباشر للعملاء.
- To isolate storage in the cloud, Brokered Cloud Storage Access is an approach.
- لعزل التخزين في السحابة، يعد الوصول إلى التخزين السحابي عبر الوسيط أحد الأساليب.
- Following two services are generated in this approach:
  - A broker with complete access to storage, but no access to client.
  - A proxy with no access to storage, but access to client and broker both.
  - وسيط يتمتع بإمكانية الوصول الكامل إلى مساحة التخزين، ولكن لا يمكنه الوصول إلى العميل.
  - وكيل لا يمكنه الوصول إلى مساحة التخزين، ولكن يمكنه الوصول إلى العميل والوسيط معًا.

ISOLATED ACCESS TO DATA:



How it works:

- The client data request goes to the external service interface of the proxy.
- ينتقل طلب بيانات العميل إلى واجهة الخدمة الخارجية للوكيل.
- The proxy forwards the request to the broker.
- ينتقل طلب بيانات العميل إلى واجهة الخدمة الخارجية للوكيل.
- The broker requests the data from cloud storage system.
- يطلب الوسيط البيانات من نظام التخزين السحابي
- The cloud storage system returns the data to the broker.
- يقوم نظام التخزين السحابي بإرجاع البيانات إلى الوسيط.
- In next step, broker returns the data to the proxy.
- في الخطوة التالية، يقوم الوسيط بإرجاع البيانات إلى الوكيل.
- At the last proxy sends the data to the client.
- في النهاية، يُرسل البيانات من الوكيل الاخير إلى العميل.

Causes of Problems Associated with Cloud Computing:

- Most security problems stem from:
  - Loss of control (فقدان السيطرة)
  - Lack of trust (انعدام الثقة)
  - Multi-tenancy (تعدد الايجارات)
- These problems exist mainly in 3rd party management models
- توجد هذه المشكلات بشكل أساسي في نماذج إدارة الطرف الثالث
  - Self-managed clouds (private and community) still have security issues.
  - لا تزال السحابات المدارة ذاتيا (الخاصة والمجتمعية) تواجهه مشكلات امنيه

Loss of Control in the Cloud:

- Data, applications, resources are located with provider
- توجد البيانات والتطبيقات والموارد مع المزود
- User identity management is handled by the cloud
- تتم إدارة هوية المستخدم بواسطة السحابة
- User access control rules, security policies and enforcement are managed by the cloud provider.
- تتم إدارة قواعد التحكم في وصول المستخدم وسياسات الأمان والتنفيذ بواسطة مزود السحابة
- Consumer relies on provider to ensure
- يعتمد المستهلك على مزود الخدمة للتأكد من
  - Data security and privacy (امن البيانات والخصوصية)
  - Resource availability (توافر الموارد)
  - Monitoring and repairing of services/resources (مراقبة وإصلاح الخدمات/ الموارد)

Multi-tenancy Issues in the Cloud:

- Conflict between tenants' opposing goals
- الصراع بين أهداف المستأجرين المتعارضة
  - Tenants share a pool of resources and have opposing goals
- يتشارك المستأجرون في مجموعة من الموارد ولديهم أهداف متعارضة
- Cloud Computing brings new threats
- تجلب الحوسبة السحابية تهديدات جديدة

- Multiple independent users share the same physical infrastructure.
  - يشترك العديد من المستخدمين المستقلين في نفس البنية التحتية المادية
- Thus, an attacker can legitimately be in the same physical machine as the target
  - وبالتالي، يمكن للمهاجم أن يتواجد بشكل شرعي في نفس الجهاز الفعلي الذي يوجد به الهدف

Security and Privacy Issues in Cloud Computing:

- Infrastructure Security (امن البنية التحتية)
- Data Security and Storage (امن البيانات والتخزين)
- Identity and Access Management (IAM) (إدارة الهوية والوصول)
- Privacy (الخصوصية)

Infrastructure Security:

- **Network Level**
- **Host Level**
- **Application Level**

The Network Level:

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider.
  - ضمان سرية وسلامة بيانات مؤسستك أثناء نقلها من وإلى مزود البيئة السحابية العامة
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider.
  - ضمان التحكم المناسب في الوصول (المصادقة والترخيص والتدقيق) إلى أي موارد تستخدمها في مزود السحابة العامة الخاص بك

- Ensuring availability of the resources in a public cloud that are being used by your organization.
- ضمان توفر الموارد في السحابة العامة التي تستخدمها مؤسستك.

The Host Level:

- SaaS/PaaS
  - Both the PaaS and SaaS platforms abstract and hide the host OS from end users
  - تعمل كل من منصات PaaS وSaaS على تجريد نظام التشغيل المضيف وإخفائه عن المستخدمين النهائيين.
  - Host security responsibilities are transferred to the CSP (Cloud Service Provider).
  - يتم نقل مسؤوليات أمان المضيف إلىCSP (مزود الخدمة السحابية)
  - However, as a customer, you still own the risk of managing information hosted in the cloud services.
  - ومع ذلك، كعميل، لا تزال تتحمل مخاطر إدارة المعلومات المستضافة في الخدمات السحابية.