Sujet :

Le Cloud computing favorise t elle la sécurité ?

RAPPORT DE VEILLE TECHNOLOGIQUE

RISR

Elaboré par

Tarik Ertam

Ecole IMIE de Bruz

Année 2014-2015

Table des matières

INTRODUCTION

Dès l'apparition du Cloud computing elle a été perçu comme une révolution et pour d'autre une évolution d'un point de vue technique. Ce type d'externalisation pose de nouveaux défis aux professionnels de la sécurité, en charge de la protection des données de l'entreprise et des ressources informatiques. L'externalisation peut concerner des activités et services divers d'une entreprise : l'informatique (externalisation du service), les ressources humaines (la paie), la finance (comptabilité, facturation), le marketing ou la communication (externalisation commerciale). On peut aussi parler d'externalisation pour des infrastructures ou des processus industriels (externalisation logistique). Les offres proposé par le Cloud computing sont souvent riches et comportes de nombreuses fonctionnalités.

Le Cloud computing peut être perçu comme une forme d'externalisation « dans les nuages ». Elle correspond au transfert d'activités d'une entreprise vers un prestataire externe spécialisé dans un domaine ou offrant des capacités de production supérieures. Il s'agit souvent de la sous-traitance d'activités ne correspondant pas au cœur de métier de l'entreprise et lui permettant alors de se recentrer sur celui-ci (définition d'ARMATIS).

Dans ce cadre, le présent sujet se base sur trois axes principaux :

- Présentation du Cloud computing
- Les risques du Cloud computing
- Les solutions de sécurité possible du Cloud computing

1. Présentation du Cloud Computing

Qu'est ce que le Cloud Computing ?

Nous répondrons à cette question en reprenant la defintion dont le NIST a défini et dont nous nous appuierons du fait de sa notoriété en qualité de normalisation.

Le NIST donne sa définition du Cloud Compunting, en énonçant 5 caractéristiques essentielles :

1.Un service en libre-service à la demande ;

2. accessible sur l'ensemble du réseau;

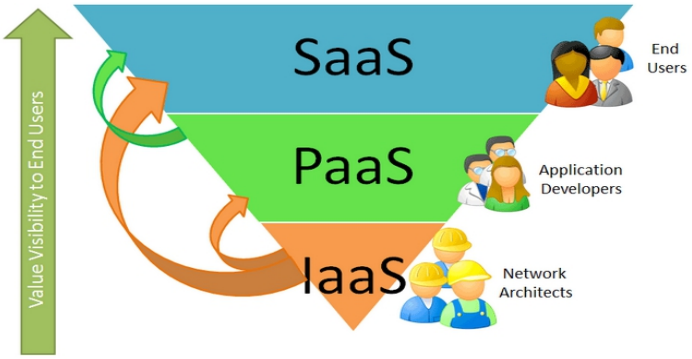
3. avec une mutualisation des ressources;
4. rapidement élastique (adaptation rapide à une variation à la hausse ou à la baisse du besoin);
5. et mesurable (mesure et affichage des paramètres de consommation).

<u>On distingue 3 niveaux de service :</u>

1. **SaaS** : ***software as a Service*** comme par exemple un utilisateur qui "loue" un logiciel de CRM, en ligne, à la demande, chez un prestataire externe;

2. **PaaS** : ***Plateform as a Service***; exemple d'une solution externe qui propose une suite logicielle middleware et les outils d'intégration et de suivi, tels qu'un serveur web (Linux+Apache+MySQL+Php);

3. **IaaS** : ***Infrastructure as a Service***; l'infrastructure matérielle est externe (par exemple une capacité de stockage et une capacité de calcul) accessible à la demande via le réseau.



Le NIST recense 4 modèles hiérarchiques de déploiement :

le nuage privé (au sein d'une même organisation);

1.le nuage communautaire (réservé à une communauté);
2.le nuage public (ouvert au grand public);
3.le nuage hybride (composition de plusieurs types de nuages).

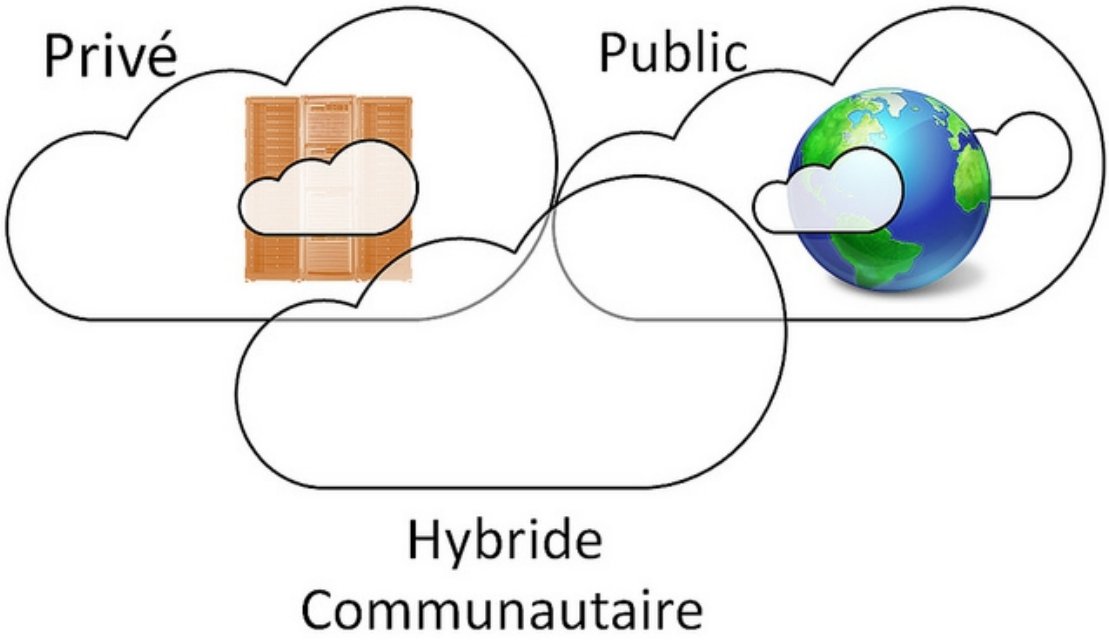


Tableau présentant les solutions commerciales de Cloud catégorisés :

IAAS	**PAAS**	**SAAS**
IBM : Cloud Burst	IBM : SmartBusiness cloud	Google : Drive Apps
Google : Compute Engine	Google : App Engine	Apple : icloud
HP Cloud System	HP : Helion	IBM : Lotus Live
Xerox Cloud	Microsoft : Windows Azure	Microsoft : office 365
OVH : Run above	Oracle : Fusion Middleware	Oracle : CRM on demand
Sales Forces : entreprises	Sales forces: Force on	Sage : CIEL above
Amazon : EC2 et S3	SAP : Business By Design	Sales Force : Chatter
Xen + VMWARE ESX +Openstack + etc ...	RHEL : OpenSHift	

2. Les risques et failles du Cloud computing et ses données (d'un point de vue Client et Serveur)

Lors d'une récente conférence sur le développement d'application de Gartner, des participants ont été interrogés concernant le Cloud Computing. L'un des points ressortant du sondage a été la façon positive d'appréhender le Cloud Computing de la part de la majorité des participants. Tandis que le Cloud Computing est toujours perçu dans la presse informatique comme une approche informatique à haut risque qui n'en est qu'à ses débuts, il est évident qu'il existe un alignement croissant avec les avantages du Cloud Computing parmi les dirigeants informatiques novateurs.

Le seul domaine dans lequel le modèle de Cloud Computing est perçu comme inférieur aux modèles traditionnels est le « pari » qu'un client doit faire avec un fournisseur de service, C'est-à-dire : pouvons-nous faire confiance à ce fournisseur et pouvons-nous en prendre le risque ?

Risques au niveau administratif :

2.1 Sécurité, confidentialité et conformité	• Données et processus situés et isolés dans un environnement partagé (on peut citer le Cloud public où quiconque peut utiliser des données à des fins diverses et variées). • Règles et problèmes légaux, politiques d'entreprise, conformité, découverte électronique, saisie des données. • Attaques via l'interface de gestion, suppressions de données incomplètes, gestion d'identités. •Mauvaise Gestion des droits des utilisateurs dans des environnements mixtes mélangeant applications locales et dans les nuages. •Mauvaise sécurisation et dimensionnement de la couche de transport.
2.2 Transparence et contrôle	•Pas d'inspection/de contrôle de la mise en œuvre du fournisseur ou de transparence sur les opérations de ce dernier. (manque de visibilité et donc de traçabilité)., ;:! • Processus métiers manquant de souplesse (contrats, accords de niveau de service, évaluations/audits de sécurité, accords de non-divulgation, etc.). • Fournisseurs immatures avec une expérience ou des certifications insuffisantes.
2.3 Problèmes techniques et assurance de service	• Exposition à des pannes de service • Dépendance vis-à-vis d'Internet pour la connectivité •Accords de niveau de service avec souvent peu de valeur (trop simples, contenu peu détaillé)
2.4 Dépendance	• Manque de normes, problèmes de portabilité de données/code

propriétaire/service	• Réversibilité
2.5 Intégration et intégrité du processus	• Niveaux de service manquant de souplesse ou inexistants et incapacité à gérer et à contrôler les services • Intégration entre plusieurs fournisseurs de cloud et entre l'entreprise et le cloud

Risques au niveau Techniques :

2.6. Risque révélé récemment

-**PRISM**(programme de surveillance) : Après la révélation de Snowden ex-consultant de la NSA de PRISM en 2013 qui est un programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électronique. Ce programme classé, relevant de la NSA (National Security Agency) prévoit le ciblage de personnes vivant hors des Etats-Unis. Certain opérateur Cloud « Français » espère tirer profit de cette situation. En effet, les données circulant en France et ne dépassant pas les frontières assure une souveraineté des données et applications informatiques. Ainsi, les entreprises sensibles sur la localisation des données auront une image crédible des fournisseurs tels que Numergy et CloudWatt, fondés par Orange et Thalés. Pour résumé, ce programme a pour risque de violer la confidentialité des données.

-**XKeyscore** est un programme de surveillance de masse créé par la NSA et opéré conjointement avec les services de renseignements britanniques, canadiens, australiens et néo-zélandais. Il permettrait une collecte quasi-systématique des activités de tous les utilisateur sur Internet » grâce à plus de 700 serveurs localisés dans plusieurs dizaine de pays. D'après la NSA elle permettrai de surveiller les pays étranger dans le but de déceler et enfin arrêter des terroristes. Grâce à ce système ils ont pu arrêter plus de 300 terroristes depuis 2008.
XKeyscore récupère tous les données des activités saisies dans les navigateurs web des utilisateurs, il permet donc de suivre la quasi-totalité des activités en ligne d'un internaute. XKEYSCORE offre encore d'autres possibilités. Il est par exemple possible, à partir d'une seule adresse IP, de chercher toutes les activités numériques en lien avec cette donnée. L'outil peut également renseigner sur ceux qui ont fréquenté un site en particulier, en produisant une liste de toutes les adresses IP. Autrement dit, l'historique et l'activité d'un individu n'échappent pas à l'agence américaine.

-**Bullrun** était un programme américain secret jusqu'au jour où Edward Snowden révéla ce fameux programme, utilisé par la NSA ayant pour but de casser des systèmes de chiffrement (VPN, SSL). Ainsi, Bullrun permettrait de décoder à peu près tout ce qui est chiffré sur Internet, qu'il s'agisse d'e-mails, de transactions bancaires en ligne, de conversations, de dossiers médicaux ou encore de secrets commerciaux. Toujours les même propos pour se défendre, leur programmes leur permettrai de veillé à la sûreté nationale et de lutte antiterroriste. Ainsi, la cryptographie qui constitue la base de la confiance en ligne est sans aucun doute un des éléments remisent en question après les révélations faite par Snowden.

Shellshock : Cette faille permet d'exécuter du code malveillant et à distance sur un ordinateur, permettant à un pirate de potentiellement prendre le contrôle de la machine. Bash, ou Bourne-Again Shell, correspond au programme qui lit et exécute les commandes qu'un utilisateur laisse sur la console. Bash et le système d'exploitation conservent un ensemble de variables dites d'environnement, qui décrivent le contexte dans lequel l'utilisateur évolue : où se trouvent les programmes que vous l'utilisateur utilise, la session, etc. Grâce à cette faille, un pirate peut exploiter ces variables d'environnement pour exécuter du code malveillant.

2.7. Risque de la virtualisation :

Un hyperviseur est une plateforme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.

Les hyperviseurs sont classés selon 2 types d'hyperviseurs :

-hyperviseur de type 1 : un Logiciel qui s'exécute directement sur une Plate-forme matérielle. On peut citer comme solutions logicielles : XEN, ESX, ESXi, KVM, etc …

-hyperviseur de type 2 : appelé aussi hypervisor call, ou hypercall, est un logiciel qui s'exécutant à l'intérieur d'un autre système d'exploitation. On pourra citer comme technologies : QEMU, VirtualBox, VMware Workstation, Virtual PC, etc …

L'hyperviseur améliore la sécurité d'un point de vue sur la Disponibilité (équipement compatible avec le système de virtualisation), l'Intégrité (solution de stockage partagé SAN donc réplication synchrone) et la Confidentialité (permet de concevoir des architectures isolées au sein d'un hôte).

Malgré ces qualités au niveau sécurité, il présente néanmoins des vulnérabilités et donc des risques. On en recense de nombreux risques :

La compromission est la prise de contrôle par un acteur malveillant d'un système invité depuis un autre système invité ou de la couche d'abstraction depuis un système invité. Le risque qui en découle est la fuite d'information ou des perturbations du système pouvant aller jusqu'à l'indisponibilité d'un service. Il est essentiel que chaque brique matériel, système d'exploitation hôte et système d'exploitation invité soient à jour de tous les correctifs de sécurité.

Le risque d'Indisponibilité et donc la panne d'une ressource commune peut engendrer l'indisponibilité simultanée de plusieurs systèmes et potentiellement tous les services hébergés sur la même machine.

Le risque de fuite de donnée : Dans le cas de la virtualisation, les instances, les applications, le système de stockage de données et autres… se partagent une même ressource. De ce fait, il devient difficile de maîtriser les différents échanges internes à une même machine

physique et donc de garantir que les ressources bas niveaux partagés n'introduisent pas de possibilité de fuite d'information.

La gestion des erreurs : Avec la virtualisation il est possible suite à des dysfonctionnements d'arrêter et de redémarrer plusieurs systèmes invités sur un même système hôte mais il devient complexe de gérer ces erreurs sans leur prise en compte globale. Une solution possible étant de mettre en place un système centralisé et une **corrélation** des journaux de l'ensemble des systèmes.

Isolation des machines : Risque de certaines technologies de virtualisation qui ne mettent pas en œuvre l'isolation dans le but de permettre à des applications conçues pour un système d'exploitation, d'être opérationnelles sur un autre système d'exploitation, ce genre de solution permet l'exploitation des failles de sécurités des deux systèmes d'exploitation, et donne aussi un accès sans limites aux ressources de la machine hôte, tel que le système de fichiers. Pour exemple, le partage du presse-papiers dans un environnement virtuel est une fonctionnalité pratique qui permet aux données d'être transférées entre les machines virtuelles et la machine hôte. Mais cette fonctionnalité peut aussi servir de passerelle pour transférer des données entre des codes malicieux agissant en collaboration au sein de différentes machines virtuelles.

La migration à chaud inclut beaucoup d'état de transferts à travers le réseau. Durant la procédure, protéger le contenu des fichiers d'état de la VM est important. La plupart des travaux, pour mettre en œuvre la migration à chaud, se sont concentrés sur l'implémentation de cette migration avec peu ou pas de considération pour la sécurité s'y rattachant. La mémoire est un point crucial par ce qu'il est difficile pour une machine virtuelle d'encrypter sa propre mémoire. Les protocoles de migration à chaud n'encryptant pas les données en cours de transferts, toutes les données migrantes, tel que les mots de passe sont transmises en clair. De plus, après la migration l'environnement d'exécution de la machine virtuelle, aura peut être changé en termes de ressources processeur, mémoire, drivers. De tels changements peuvent être détectés, et un attaquant capable de caractériser ces changements pourrait initier des attaques de type **side-channel**.

Les attaques via les drivers : les hyperviseurs ne peuvent en principe s'attaquer directement l'un l'autre, parce que chaque instance s'exécute dans son propre espace d'adressage et un canal direct de communication n'existe pas entre les hyperviseurs.

Pour contourner cela l'attaquant devra passer par des services partagés par plusieurs hyperviseurs, par exemple les pilotes. Les pilotes utilisent un canal de communication dédié pour chaque hyperviseur. Quand un hyperviseur malicieux exécute une attaque de type déni de service en soumettant trop de requêtes, c'est en fait le pilote peut couper le canal de communication. La première préoccupation de sécurité concernant les drivers et leur utilisation de la (Direct Memory Access). Si une plate-forme n'inclut pas un IOMMU (Input/Output Memory Management Unit), alors tout pilote qui accède directement à la mémoire doit être de confiance. Sur les nouvelles plates-formes qui fournissent une IOMMU, l'hyperviseur réduit l'usage de la DMA, un pilote compromis ou un driver malicieux peut

seulement affecter la disponibilité de son propriétaire, l'intégrité et la confidentialité de la région mémoire qui lui est assignée. Donc si un hyperviseur délègue l'ensemble de la mémoire physique d'une machine virtuelle à un driver alors ce dernier pourra manipuler le VM toute entière. En utilisant la IOMMU l'hyperviseur bloque les transferts vers sa propre zone mémoire et restreint les vecteurs d'interruption disponibles pour les pilotes. Dans les architectures où les drivers sont intégrés à l'hyperviseur, un matériel non sûr peut oublier la sécurité du système dans son entier.

Compromettre le système de cryptographie :

Par exemple, la valeur occasionnelle d'une clé symétrique ne devrait jamais être réutilisée. Si une machine virtuelle est réinitialisée à un état précédent, une même valeur pourrait être répétée. Un attaquant pourrait exploiter cette propriété pour réaliser une attaque contre le système de cryptographie .

Attaque de la mémoire virtualisée :

Bien qu'une machine virtuelle ne puisse directement modifier les structures de données tels les tables, les descripteurs globaux…Ces opérations peuvent être demandées à travers les hypercalls .Si un attaquant peut modifier un hypercall, il peut potentiellement modifier les droits d'accès à ces structures de données . Il peut ainsi avoir accès aux pages mémoire d'autres machines virtuelles ou modifier le code des ces machines. Il peut aussi causer un déni de service à l'encontre des utilisateurs légitimes de la VM.

-VM Escape (référence des failles : CVE-2009-1244,CVE-2011-1751, CVE-2012-0217,CVE-2012-3288) : Un exploit qui permet à un pirate de se déplacer à partir d'une machine virtuelle à l'hyperviseur , d'avoir ainsi l'accès à l'ensemble de l'ordinateur et notamment à toutes les machines virtuelles en cours d'exécution.

-VM Hopping : Similaire à VM Escape, VM Hopping permet à un attaquant de se faire passer pour un serveur virtuel et donc de compromettre d'autre serveur virtuel s'il se trouve sur le même matériel et donc sur le même VM network (c.f. Vcenter_Server, XenApp).

-VM Theft : Ceci à la capacité de voler un fichier de machine virtuelle par voie électronique, qui peut ensuite être monté et dirigé ailleurs. C'est une attaque équivalente comme le vol d'un serveur physique complet sans avoir à entrer de mot de passe et enlever une pièce d'équipement informatique.

2.8. Risque VPN : PPTP

-PPTP : Le principe du protocole PPTP (*Point To Point Tunneling Protocol*) est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.

Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectés par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP. Le PPTP étant l'un des protocoles le plus vulnérable et le plus obsolète. Ainsi, il est très intéressant de parler de ce protocole dont les entreprises utilisent assez fréquemment (source CCM).

En effet, au cours de la conférence Defcon 20 sur la sécurité qui s'est tenue du 26 au 29 juillet 2012 à Las Vegas, des chercheurs ont livré deux outils permettant de casser le cryptage de toute session PPTP (Point-to-Point Tunneling Protocol) et WPA2-Enterprise (Wi-Fi Protected Access) utilisant le protocole d'authentification MS-CHAPv2. (source LMI)

2.9. Risque SSL

-HTTPS (Hypertext Transfer Protocol Secure): est la combinaison du http avec une couche de chiffrement comme SSL ou TLS. Théoriquement, pour qu'une attaque puisse être réalisée sans échec, elle doit d'abord réussir à s'interposer entre le navigateur et le site web cible. Ensuite, il ne reste plus au hacker qu'à effectuer une injection de code dans le navigateur du poste cible, en restant dans le cadre de la session HTTPS qu'il souhaite accéder. Sur le plan pratique, la réalisation d'une telle démarche n'est pas toujours aussi simple. Cependant, avec l'apparition de l'outil BEAST, la sécurité du protocole https, est totalement remise en question.

BEAST agit comme un cheval de Troie cryptographique, et il suffit que le pirate informatique possède des connaissances approfondies en matière de programmation Java, et qu'il arrive à injecter un code de JavaScript dans le navigateur de sa cible, pour compromettre la connexion https. Le code JavaScript peut collaborer avec le renifleur (sniffer) réseau pour exploiter la vulnérabilité du protocole https, en attaquant directement sa confidentialité.

-Heartbleed (source Wikipedia) : est une vulnérabilité logicielle présente dans la bibliothèque de cryptographie open source OpenSSL depuis mars 2012, qui permet à un « attaquant » de lire la mémoire d'un serveur ou d'un client pour récupérer, par exemple, les clés privées utilisées lors d'une communication avec le protocole Transport Layer Security (TLS). Découverte en mars 2014 et rendue publique le 7 avril 2014, elle concerne de nombreux services Internet. Ainsi 17 % des serveurs web dits sécurisés, soit environ un demi-million de serveurs, seraient touchés par la faille au moment de la découverte du bogue

2.10. Limite de la supervision

Complexification de la supervision :

Les opérations de supervision peuvent s'avérer complexes du fait de l'incompatibilité entre le cloisonnement nécessaire des machines virtuelles et la nécessité de vision d'ensemble de la part de la supervision. Dès lors il devient difficile de tracer un événement ou une action de bout en bout.

3. Les solutions de sécurité du Cloud computing entreprise par les entreprises

3.1 Récupération des données

La perte de donnée est l'une des plus grandes inquiétudes des entreprises qui souhaitent intégrer dans leur Système d' Information le Cloud. Les entreprises qui offrent des solutions du Cloud se charge automatiquement de la récupération de donnée. Ainsi, elle garantit une sauvegarde et une restauration des données plus rapides que la plupart des sociétés qui gèrent eux même le processus de sauvegarde et restauration de donnée. Une étude menée par Aberdeen Group à montrer que les résolutions des problèmes étaient réactif comme l'exemple suivant le démontre :

« [...]2,1 heures en moyenne, soit presque quatre fois plus rapidement que les entreprises qui n'y avaient pas recours (8 heures). [...] »

Source tiré du site salesforce.

3.2 Solution à la réversibilité

L'association des DSI européens recommande de recourir à des formats de données ouverts, seuls capables, à leurs yeux, de faciliter les opérations de réversibilité entre les différents Clouds. Afin de minimiser les risques liés à la réversibilité, il est recommandé d'annexer au

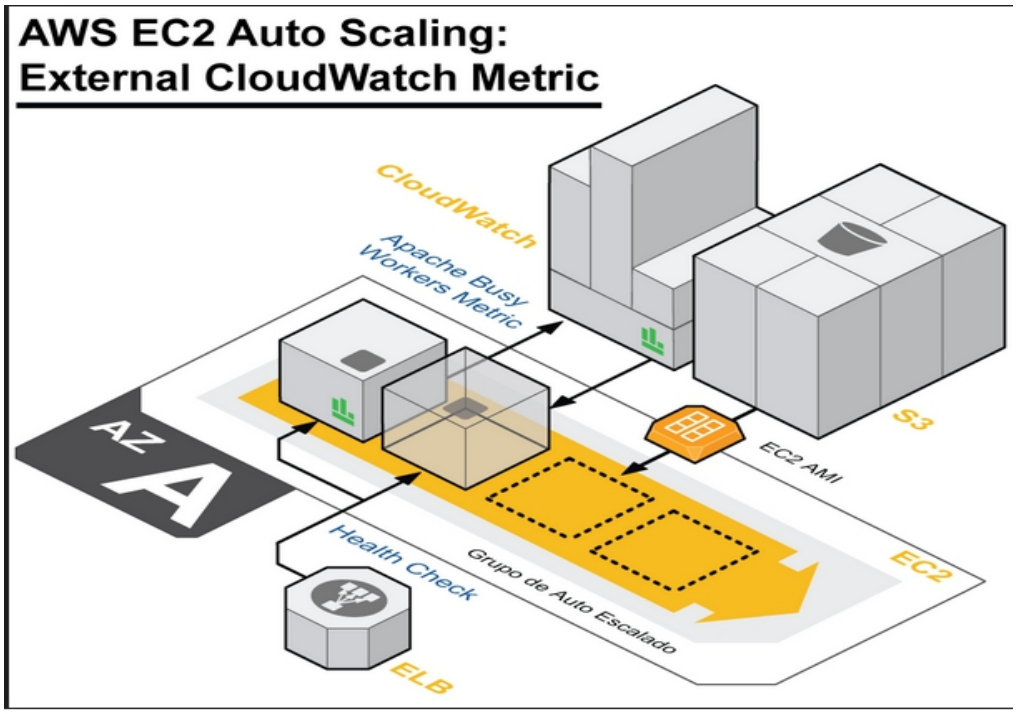
contrat Cloud un plan de réversibilité qui détaille la procédure de restitution des données et d'inclure des clauses précisant la fréquence de mise à jour et les tests de *restitution*.

3.3 Mises à Jour

Avec le Cloud Computing, la maintenance de serveur est réalisée par des professionnels dont leur métier et de réaliser ces mises à jour en temps et en heure. Leur réputation repose sur des pratiques de maintenance assez stricte.

3.4 Journalisation

La gestion de logs est une des techniques privilégiées par les RSSI pour détecter et endiguer les attaques informatiques. Les logs permettent de repérer la présence d'un intrus ou de transactions anormales dans les systèmes. On peut cité chez AWS (Amazon Web Services) les services suivantes : CloudWatch pour la surveillance des ressources en nuages AWS et divers APIs AWS notamment pour le réseau et autres services.



3.5 Tunnelisation et Chiffrement

VPN : Le Cloud utilise forcement comme support de transmission un protocole d'encapsulation (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel** (noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les hôtes des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

PKI (Public Key Infrastructure) est un système de gestion des clefs publiques utiliser dans le Cloud et donc employer par le VPN. PKI permet de gérer des listes importantes de clefs publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur.

Les principaux protocoles de tunneling sont les suivants :

- **PPTP** (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.

- **L2F** (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète.

- **L2TP** (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.

- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il s'appuie notamment sur AH et ESP. Protège les adresses sources et destination, plus, le message qui doit transiter.

  Le chiffrement est une opération mathématique, c'est en réalité un algorithme. Pour les applications cryptographiques (VPN, chiffrement de documents, etc...) il est conseillé actuellement de choisir **AES** et **RSA-1024** pour le chiffrement et **SHA-256** pour le hachage. Triple-DES vit certainement ses dernières années de robustesse. Au jour d'aujourd'hui, les chiffrements les plus sûrs sont ceux qui emploient des algorithmes asymétriques comme RSA. L'algorithme asymétrique comparé à l'algorithme symétrique est plus sécurisé du faite qu'elle utilise une clé privée dont seul l'utilisateur concerné peut défricher la donnée.

Dans le Cloud le chiffrement est utilisé dans différents points sensibles d'accès :

- Chiffrement de l'accès à l'interface de contrôle d'accès aux ressources du Cloud
- Chiffrement des accès administratifs aux instances d'OS
- Chiffrement de l'accès aux applications
- Chiffrement des données stockées des applications 45

3.5 L'authentification Multi-facteur :

L'authentification multi-facteurs s'assure qu'un utilisateur est bien celui qu'il prétend être. Plus on utilise de facteurs pour vérifier l'identité d'une personne, plus on peut avoir confiance dans le résultat.

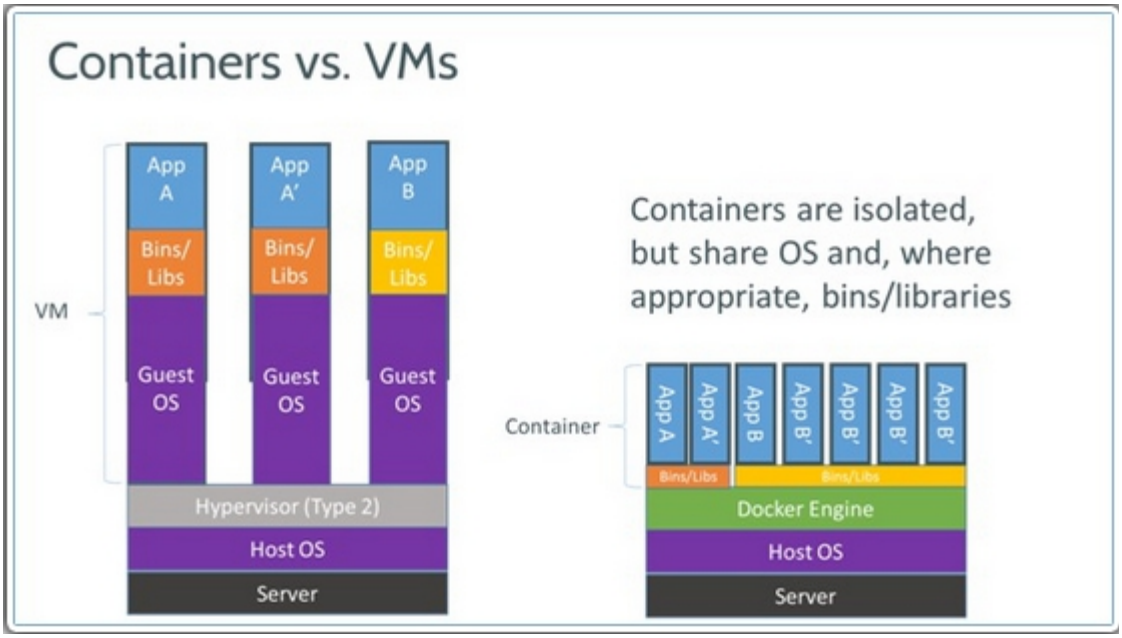
L'authentification multi-facteurs peut se faire via une combinaison des facteurs suivants :

- *Une connaissance : un mot de passe ou un PIN*
- *Une possession : un token ou une smartcard (authentification à deux facteurs)*
- *Une caractéristique personnelle : un facteur biométrique comme une empreinte digitale (authentification à trois facteurs)*

La sécurisation par authentification multi-facteurs exige plusieurs preuves d'identité lors de la connexion, elle est donc considérée comme la méthode la plus sûre pour autoriser l'accès à des données et des applications. (ex : AWS Multi-factor Authentification : AWS MFA)

3.6 Sécurité des applications

Pour sécuriser les applications un outil qui est apparu récemment, la solution Docker. C'est un outil open source, fournissant du PaaS né du mouvement DevOps. Il répond à plusieurs problèmes du Cloud computing dont le packaging et le déploiement d'applications.



Le container virtualise l'environnement d'exécution de l'OS de la machine hôte (Linux ou BSD, il n'existe pas à ce jour de container sous Windows). Un container est un ensemble applicatif s'exécutant au sein de l'OS maître de manière virtuellement isolée et contrainte (jails, chroot **). Le container est très performant et léger, car il partage de nombreuses ressources avec l'OS hôte (kernel, devices…). En revanche, bien que s'exécutant de manière isolée, le container ne peut être considéré comme très sécurisé puisque partageant la stack

d'exécution avec l'OS maître. Le container peut au choix démarrer un OS complet ou bien simplement des applications. Docker a pour objectif de ne pas reproduire tout un OS dans un container mais simplement les applications/services souhaités.

Tout de même, niveau sécurité il est possible d'utiliser Docker pour avoir des environnements de développement locaux par projet/client isolés et partageables.

3.7 Sécurité réseau

Chaque environnement est cloisonné et étanche, et l'ensemble des flux entrants et sortants sont filtrés au travers d'un dispositif de sécurité qui est le firewall (pare-feu). En effet, le firewall peut être situé comme le premier niveau de protection des données des serveurs. La matrice de Flux (par gestion de règle) configure les accès web HTTP et HTTPS par défaut, ainsi que les accès d'administration SSH et RDP. Il est de même possible de configurer d'autres ouvertures de flux. Un environnement et son VLAN forment une DMZ. Contrôlez totalement la communication entre la DMZ et l'extérieur grâce au service de Firewalling est devenu un élément incontournable. Le Firewall ainsi que le VLAN sont tous deux des éléments qui permettent d'isoler au mieux une zone on parle alors de DMZ. Cette technique permet l'isolation d'hôte. On peut cité comme technologie de service Firewalling chez Amazone (AWS) sous EC2 (Elastic Compute Cloud), ils utilisent notamment un service nommé Security Group.

3.8 Supervision

La supervision est la « surveillance du bon fonctionnement d'un système ou d'une activité ».

Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques.

Elle répond aux préoccupations suivantes :

- technique : surveillance du réseau, de l'infrastructure et des machines ;
- applicative : surveillance des applications et des processus métiers ;
- contrat de service : surveillance du respect des indicateurs contractuels ;
- métier : surveillance des processus métiers de l'entreprise.

On ajoutera les actions réflexes à cette surveillance du système. Ce sont les réactions automatisées en fonctions d'alertes définies.

En cas de dysfonctionnement, le système de supervision permet d'envoyer des messages sur la console de supervision, ou bien d'envoyer un courriel à l'opérateur. (Source Wikipedia)

Comme solution on peut cité le composant Ceilometer d'Openstack.

3.9 ISO 27001

L'ISO/IEC 27001 est la norme internationale pour le management de la sécurité de l'information (ex : AWS). Elle explique comment mettre en place un système de management de la sécurité de l'information certifié et évalué par un organisme indépendant. Cela permet de sécuriser plus efficacement toutes les données confidentielles, en minimisant ainsi la probabilité d'un accès illégal ou non autorisé.

Avec la norme ISO/IEC 27001 l'entreprise pourra assurer un engagement et une conformité aux meilleures pratiques internationales, prouvant aux clients, aux fournisseurs et aux parties prenantes que la sécurité est un élément essentiel. (*Source : http://www.bsigroup.com/fr-FR/ISOIEC-27001-Securite-de-lInformation/Introduction-a-la-norme-ISOIEC-27001/)*

3.10 Technique d'anonymisation

Technique d'anonymisation : Le G29 publie un avis sur les techniques d'anonymisation

Pour exemple, l'avis rendu par le G29 analyse les garanties offertes et les erreurs communé ment commises des techniques de pseudonymisation telles que les clés de chiffrement, les chiffrements déterministes, les fonctions de hachages ou la tokénisation.

En ce sens, la pseudonymisation, qui est un processus consistant à remplacer un certain nombre de champs considérés comme des identifiants potentiels et à les remplacer par d'autres, réduit la corrélation entre des ensembles de données avec l'identité originale de l'individu. (ex : AWS Identity and Access Management :AWS IAM)

Cependant : la corrélation entre différents ensembles de données distincts concernant un in dividu est toujours possible la personne physique est encore susceptible d'être identifiée indi rectement par cet ensemble de données ou à travers différentes bases de données usant du même attribut pseudonymisé pour un même individu.

Ainsi, il est important de retenir que la pseudonymisation d'un ensemble de données : ne constitue pas une anonymisation complète ne constitue pas une technique permettant la réduction de toute corrélation de manière certaine.

Cet avis de la CNIL de nature technique constitue une base d'étude intéressante incontou -nable pour les équipes d'opérationnels présentes au sein des entreprises.

3.11 Contrôle d’accès par adresse MAC, par RBAC, DAC

RBAC : **Role-Based Access Control** (RBAC) ou, en français, **contrôle d'accès à base de rôles** est un modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché. Un rôle découle généralement de la structure d'une entreprise. Les utilisateurs exerçant des fonctions similaires peuvent être regroupés sous le même rôle. Un rôle, déterminé par une autorité centrale, associe à un sujet des autorisations d'accès sur un ensemble objets.

La modification des contrôles d'accès n'est pas nécessaire chaque fois qu'une personne rejoint ou quitte une organisation. Par cette caractéristique, RBAC est considéré comme un système « idéal » pour les entreprises dont la fréquence de changement du personnel est élevée.

Ce modèle est également référencé sous le nom de **nondiscretionary access control** et constitue une nouvelle alternative, entre les systèmes Mandatory Access Control (MAC) et Discretionary Access Control (DAC).

MAC : Le ***Mandatory access control*** (MAC) ou **contrôle d'accès obligatoire** est une méthode de gestion des droits des utilisateurs pour l'usage de systèmes d'information.

Il existe d'autres méthodes telles que :

- le contrôle d'accès discrétionnaire (ou *Discretionary Access Control* - DAC)
- le contrôle d'accès à base de rôles (ou *Role-Based Access Control* - RBAC).

Le contrôle d'accès obligatoire est utilisé lorsque la politique de sécurité des systèmes d’information impose que les décisions de protection **ne doivent pas être prises par le**

propriétaire des objets concernés, et lorsque ces décisions de protection doivent lui être imposées par le dit système. Le contrôle d'accès obligatoire doit permettre d'associer et de gérer des attributs de sécurité relatifs à cette politique, sur les fichiers et processus du système.

Les types de politiques de sécurité possibles pour un système informatique sont pris en compte pour déterminer sa classification en termes de niveau d'assurance selon la méthode « Critères communs », anciennement ITSEC (1991) ou TCSEC américaine de 1985 (DOD 5200.281) ayant défini le niveau « C2 » du Trusted Computer System Evaluation Criteria . Se référer aux profils CAPP (Controlled Access) et LSPP (Labeled Security Protection Profile (en)) du niveau d'assurance EAL3 (ancien ITSEC E2).

DAC : Le **Contrôle d'accès discrétionnaire** (DAC pour *Discretionary access control*) est un genre de contrôle d'accès, défini par le Trusted Computer System Evaluation Criteria(TCSEC) comme « *des moyens de limiter l'accès aux objets basés sur l'identité des sujets ou des groupes auxquels ils appartiennent. Les commandes sont discrétionnaires car un sujet avec une certaine autorisation d'accès est capable de transmettre cette permission (peut-être indirectement) à n'importe quel autre sujet (sauf restriction du contrôle d'accès obligatoire).* »

3.11. Solution de sécurité au niveau de l'hyperviseur

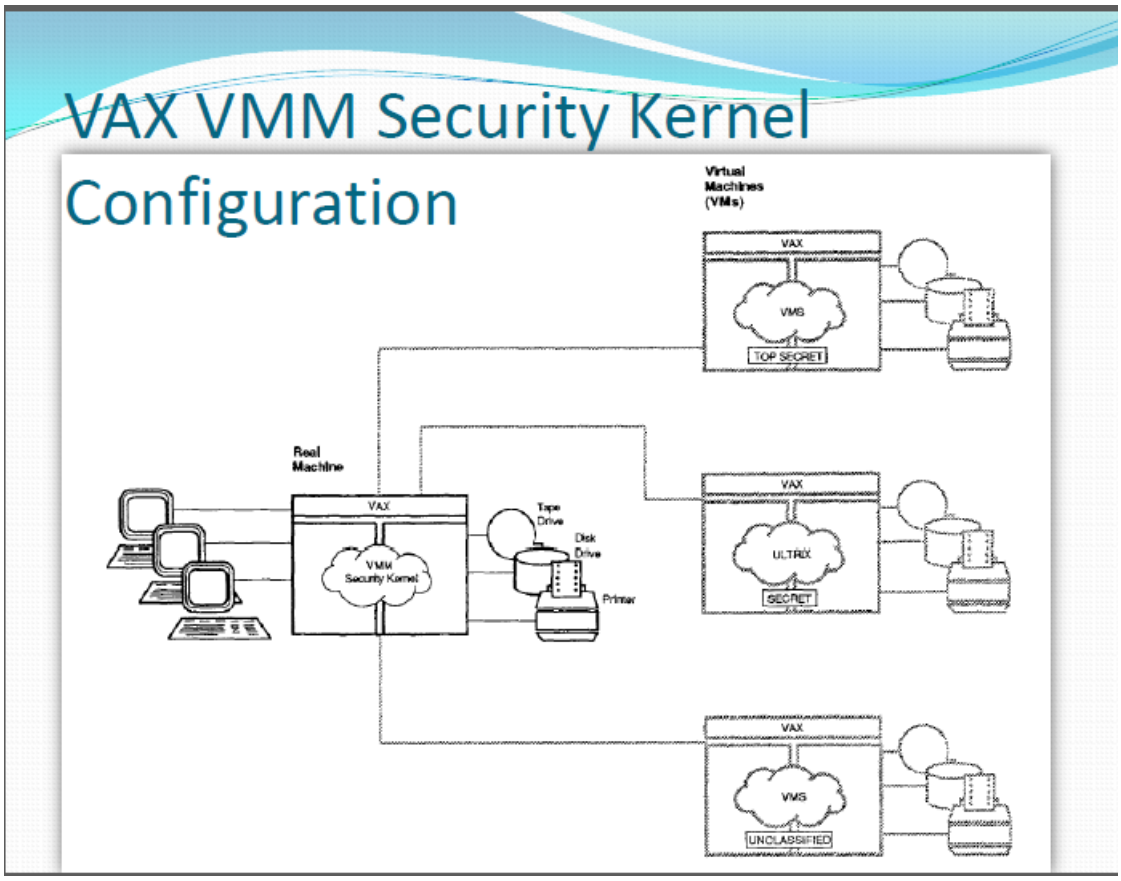
Fonctionnement de Vax VMM :

L'une des premières tentatives pour concevoir un hyperviseur sécurisé est faite par Karger & al lors d'une recherche menée entre 1981 et 1990 sur la production d'un noyau de sécurité Virtual Machine Monitor (VMM). Ce projet de recherche a obtenu le niveau de sécurité A1 par le (NCSC). Il s'agit du niveau de sécurité le plus élevé conformément aux critères d'évaluation du publié par NCSC en 1985 et qui est également connu sous le nom de Livre Orange. Le développement du noyau de sécurité VMM est effectué à partir de l'extension d'adresse virtuelle conçue au cours des années 70. Conformément aux exigences du niveau de sécurité A1, le et de toutes les machines virtuelles. Avec MAC, le VMM VAX utilise le modèle de protection pour la protection de la vie privée et le modèle de protection d'intégrité Biba. Le noyau de sécurité VAX prend en compte et fait fonctionner simultanément et en toute sécurité plusieurs machines virtuelles sur un seul système physique VAX tout en assurant l'isolement et le partage contrôlé des données sensibles. Il est doté d'un système d'authentification sécurisé, avec un niveau de performance élevé et des outils de gestion du système très développés soumettant ainsi les machines virtuelles à des contrôles d'accès et d'audits obligatoires. Ainsi chaque machine virtuelle est dotée d'une classe d'accès composée d'une classe secrète et d'une classe d'intégrité similaire aux classes dans les VMS Security Enhancement Services (VMS SES).

À chaque fois qu'un utilisateur veut accéder à une machine virtuelle, il doit d'abord s'authentifier au VMM VAX. À cet effet, le VAX hyperviseur offre un processus de confiance en cours d'exécution dans le noyau. Ce processus ne s'exécute qu'après validation de

l'Authentification de l'utilisateur. Puis, le VAX hyperviseur crée un chemin de confiance entre le processus serveur et l'utilisateur. Le serveur fournit des commandes permettant à l'utilisateur de se connecter à une machine virtuelle en fonction de ses droits d'accès. Dans le cas où l'utilisateur a les droits nécessaires pour se connecter à une machine virtuelle une autre voie de sécurité est établie entre l'utilisateur et la machine virtuelle, lui permettant d'interagir avec le système d'exploitation en cours d'exécution dans la machine virtuelle. En résumé, le VMM VAX offre un niveau de sécurité élevé en répondant aux niveaux d'exigence de sécurité A1 avec non seulement la mise en oeuvre des modèles de sécurité formels, DAC, MAC, de l'analyse des canaux cachés mais aussi aux exigences du monde réel avec une distribution sécurisée des ressources finales et un niveau élevé de confiance à l'utilisateur.

En résumé, le VMM VAX offre un niveau de sécurité élevé en répondant aux niveaux d'exigence de sécurité A1 avec non seulement la mise en oeuvre des modèles de sécurité formels, DAC, MAC, de l'analyse des canaux cachés mais aussi aux exigences du monde réel avec une distribution sécurisée des ressources finales et un niveau élevé de confiance à l'utilisateur.



Terra (TVMM) :

En 2003, Tal Garfinkel et al ont écrit un article présentant une Machine virtuelle basée sur une plateforme de confiance appelée Terra. L'architecture Terra est basée sur un moniteur de

machine virtuelle qui permet à plusieurs machines virtuelles d'être multiplexées sur une seule machine physique. Terra utilise le moniteur de machine virtuelle sécurisée appelée Trusted Virtual Monitor Machine (TVMM). L'architecture TVMM propose des services variés avec des mécanismes de protection avancés.

Les avantages de Terra se situe comme la plupart des VMM sur l'isolement, l'extensibilité, la compatibilité et la sécurité dont Terra propose des fonctionnalité supplémentaire :

b. Attestation (voir schéma ci-contre) : cette fonction permet à une application qui s'exécute dans une boîte fermée de s'identifier cryptographiquement à un tiers distant, c'est-à-dire d'informer la partie distante de ce qui est exécuté à l'intérieur de la boîte fermée. Ce qui permet à la partie distante de faire confiance à la demande et de savoir que l'application se comportera comme souhaité. Le processus de certification comporte les 3 étapes pour chaque composant :

b1. Le composant qui veut être certifié doit fournir sa paire de clé publique/clé privée

b2. Ensuite le composant remet sa clé publique et les données d'application supplémentaires du composant de niveau inférieur qu'il veut valider en utilisant la norme "ENDORSE" API.

b3. Le composant de niveau inférieur utilise sa clé privée pour signer le certificat qui contient la clé publique et les données d'application supplémentaires qu'il a reçu ainsi que le hachage des parties attestables du composant de niveau supérieur.

c. Chemin de confiance : TVMM fournit un trajet sécurisé entre l'utilisateur et l'application. Ce chemin de confiance est essentiel pour bâtir des applications sécurisées. La voie de sécurité proposée par TVMM permet à un utilisateur de déterminer quelles sont les machines virtuelles qui tournent tout en permettant à une machine virtuelle de s'assurer qu'il communique avec un utilisateur humain. Le chemin de confiance proposé assure également la protection des renseignements personnels et l'intégrité des communications entre les utilisateurs et les machines virtuelles, ce qui empêche l'altération par des programmes malveillants.

Les mécanismes Terra :

Pour atteindre ces objectifs en matière de sécurité le TVMM offre une interface pour le maintien de l'application en sécurité. À cet effet, Terra fournit plusieurs classes de disques virtuels qui sont utilisés pour assurer la les données d'une VM au nom de cette VM assurant ainsi l'intimité du stockage et de l'intégrité. Le TVMM utilise la technique de pour empêcher toute manipulation des disques dont l'intégrité reste importante bien qu'ils n'exigent pas de vie privée.

Pour la mise en oeuvre de l'attestation, le TVMM utilise une table de hachage et s'assure que les données chargées correspondent effectivement à ses hachages. Si les paragraphes d'une

entité hachée doivent être vérifiés de façon indépendante, Terra divise les paragraphes en bloc de taille fixe et chaque bloc est haché séparément.

Pour l'attestation d'interface, le TVMM fournit une interface étroite à coffret fermé pour soutenir l'attestation. Cette interface fournit les opérations suivantes

En conclusion, Terra présente une architecture très flexible qui fournit certaines fonctions de sécurité très importantes dont l'attestation. Toutefois, pour pouvoir utiliser toutes les fonctions de sécurité offertes par Terra, le système doit être exécuté sur du matériel inviolable. Ce qui n'est pas le cas pour les puces matérielles pour PC. Ceci étant, cela peut changer dans un proche avenir avec le Module implémenté dans les PC depuis 2010.

sHype :

La sécurité proposée par le sHype repose sur l'isolement fourni par le noyau qu'il complète par la supervision du partage des ressource entre les machines virtuelles. Le sHype agit en tant que médiateur à l'intérieur de l'hyperviseur et entre les machines virtuelles dans la gestion des ressources en fonction de la politique de sécurité active et du contrôle d'accès dans les communications inter-virtuelles. Tout ceci concourt à une grande flexibilité de l'architecture sHype avec des politiques de sécurité mesurées et indépendantes de la mise en oeuvre technique.

HyperWall :

Une autre approche pour assurer la sécurité est proposée avec l'architecture HyperW all. Il s'agit de protéger les machines virtuelles invitées à partir d'un hyperviseur non fiable. Avec HyperW all, l'hyperviseur gère librement la mémoire, les coeurs de processeur et d'autres ressources d'une plateforme. Une fois les machines virtuelles créées, (Confidentiality and Integrity Protection) protège la mémoire des machines virtuelles invitées à partir de l'hyperviseur ou par le DMA(Direct Memory Access) selon les spécifications du client. Le client peut spécifier que certaines plages de mémoire soient protégées contre les accès par l'hyperviseur ou par le DMA. L'HyperW all est l'élément clé qui assure la protection de la confidentialité et de l'intégrité des objets qui ne sont accessibles que par le matériel. Ils protègent tout ou partie de la mémoire d'une machine virtuelle basée sur les spécifications du client.

Hypersafe :

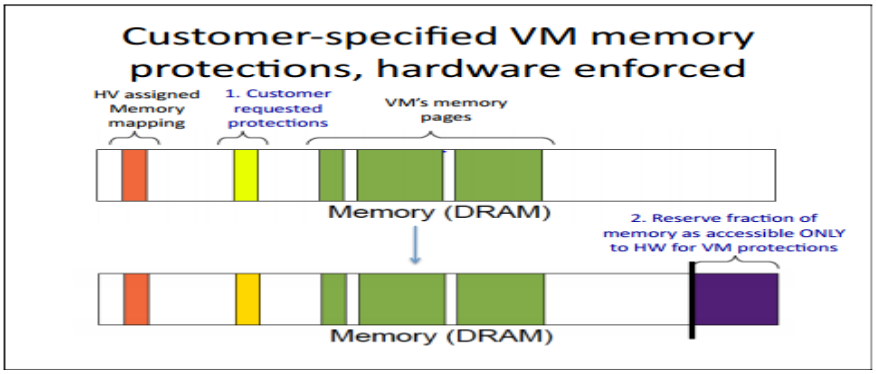
L'architecture de hyperwall , qui prévoit des protections de machines virtuelles invitées contre les attaques par un hyperviseur malveillant . Les IaaS le plus populaires (Infrastructure-as- aservice) modèle de cloud computing, tels que le service Amazon EC2, maintient les serveurs physiques et loue des machines virtuelles pour les clients . Bien que le fournisseur d'infrastructure fournit le matériel et le logiciel de virtualisation , les clients

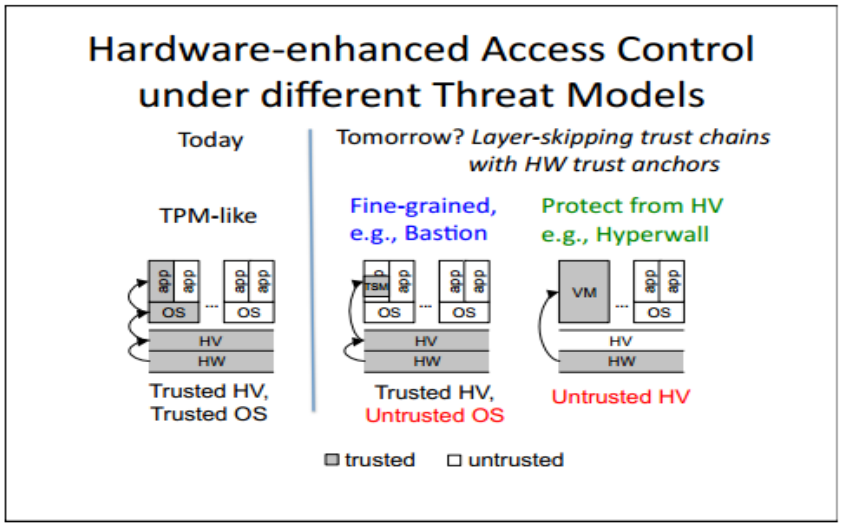
fournir leur propre système d'exploitation invité (OS) et des applications afin de fonctionner à l'intérieur de la VM loué .

D’autres clés telles que Kenc et Khash sont utilisées par le matériel HyperW all et sont stockées dans la mémoire protégée. Les clés sont générées au cours de chaque cycle d'amorçage. Elles sont utilisés chaque fois qu'une machine virtuelle est interrompue. Les clés sont stockées dans des endroits protégés de la mémoire partagée DRAM.

Une autre clé privée unique PKvm est introduite dans chaque machine virtuelle. Cette clé est stockée à l'intérieur de la zone de mémoire qui est spécifiée comme privée et interdite d’accès à l’hyperviseur et au **DMA**.

Avec HyperWall, l'hyperviseur est capable de gérer entièrement la plateforme, pour démarrer, mettre en pause ou en arrêt les machines virtuelles ou de modifier l'affectation de la mémoire, de vérifier que l'hyperviseur n’a pas un comportement contraire à ce qui est attendu. Pour ce faire, l’HyperWall fournit des données de hachage pour attester que l'image du client VM initiale et les protections spécifiées étaient instanciées lors du lancement de la machine virtuelle. En outre, les preuves de confiance peuvent être générées pendant la durée de vie de la machine virtuelle pour vérifier que ses protections spécifiées ne sont pas corrompues. Lorsque la machine virtuelle est interrompue, sa mémoire protégée est mis à zéro par le matériel pour prévenir la fuite de données ou de code. Ainsi l'hyperviseur et le DMA retrouvent les droits d'accès à la mémoire de la machine virtuelle.





CipherCloud pour securisé le SaaS :

Le produit de la startup est une **appliance** virtuelle, à déployer sur un serveur de l'entreprise, qui va transformer à la volée et en toute transparence les informations sensibles émises et reçues depuis l'application hébergée dans les nuages, et ainsi rendre celles-ci inutilisables en dehors des "murs" de l'organisation. Pour prendre un exemple, lorsqu'un utilisateur saisit le nom d'un client dans l'application (via son navigateur web), il est converti par l'appliance en une chaîne de caractères dénuée de sens avant d'être transmis aux serveurs et, inversement, lorsque l'utilisateur accède à ce client (toujours dans son navigateur), la conversion inverse est appliquée pour lui restituer le nom d'origine.

Deux types de transformation sont proposés : soit le chiffrement des données (en utilisant des "clés" qui restent confinées sur les serveurs internes), soit la "tokenisation", qui consiste à gérer des tables de correspondance entre les données "réelles" (qui restent donc à l'intérieur de l'entreprise) et celles qui sont effectivement enregistrées dans l'application. Ce dernier mode, plus lourd à gérer, permet non seulement de protéger les informations sensibles mais également de respecter les réglementations en vigueur dans certains secteurs, qui interdisent leur "export" hors des frontières. Le principe de la solution de CipherCloud n'est pas aussi simple qu'il y parait car il doit fonctionner sans aucune modification dans les applications, et c'est là que réside toute l'expertise de la société. Par exemple, les fonctions de tri, de recherche ou de sélection disponibles dans la plupart des logiciels doivent être préservées, même sur les données chiffrées ou "**tokenisées**".

En conclusion, il Garantie de la protection de vos données, empêchement de tout accès non autorisé et préservation des fonctionnalités applicatives, et, garantie la conformité au moyen d'un suivi continu du contenu, de l'activité des utilisateurs et de la détection des anomalies. Il permet d 'effectuer le suivi des interactions entre utilisateurs sur de multiples applications Cloud, garantit la conformité et identifie des anomalies à l'aide de tableaux de bord et de rapports détaillés sur la sécurité.

DaaS :

Le DaaS permet de fournir rapidement des postes de travail virtuels avec des applications standards et une intégration limitée avec le SI de l'entreprise, sans oublier une visibilité nette sur les coûts qu'il engage. Une phase pilote permettra de valider de manière concrète le fonctionnement du service et la qualité de l'expérience utilisateur.

Bien sûr, pour les entreprises qui souhaitent aller plus loin, se posent *in fine* les questions liées à l'intégration des applications sur un poste virtuel hébergé dans le *Cloud* et de la sécurité associée. De manière générale, les applications Web ou SaaS facilitent la mise en œuvre du *Desktop as a Service*. Les entreprises peuvent néanmoins toujours se tourner vers des solutions DaaS en mode *Cloud* privé, qui permettent de concilier avantages du *Cloud* et

besoins de sécurité. Certains fournisseurs comme *Orange Business Services* avec *Flexible Workspace* proposent déjà des solutions « sur étagère » qui vont dans ce sens.

Cloud Gate Intercloud :

Les fonctionnalités proposées par CloudGate portent sur la sécurité de l'accès aux applications hébergées et sur la correction des défauts éventuels de performance. Pour renforcer la sécurité des données qui transitent sur le réseau… elles ne le quittent pas !

Même si elles transitent vers un cloud public, de type AWS ou Salesforce.com, Internet n'est pas sollicité et les données demeurent sur le réseau privé. Les interconnexions des clouds privés et publics sont également protégées.

Le traitement du signal de bout en bout de la connexion est également essentiel. Le choix par InterCloud de mettre en place un VLAN pour cloisonner un service transporté et en assurer l'étanchéité est intéressant et mérite d'être signalé.

InterCloud rappel tout de même le rôle essentiel des opérateurs, alors que c'est généralement le fournisseur du service hébergé qui figure sous le feu de la rampe.

Conclusion

En conclusion, le cloud computing est souvent mal perçu par les entreprises en générales. En réponse à cette problématique nous pouvons dire qu'il ne faut pas se fié aux mythes et légendes envers le cloud computing. Le cloud computing est tout simplement une autre façon de mettre à disposition des services en utilisant un autre réseau qui est Internet. Celui ci est donc exposé à des risques tant au niveau technique qu'au niveau administratif (contrat de cloud et réversibilité). Le cloud compunting sera dans tout les cas plus fiable et plus sécuritaire comparé à l'infogérance classique. Car, Le cloud computing met l'accent sur la sécurité de l'infrastructure, des applications, et, sur des mesures de sécurité pour protéger les données. Des fournisseurs plus sensibles à la sécurité réconfortent les clients grâce aux certifications (ISO 27001) et normes (NCSC, SAS 70 Type II, PCI DSS Niveau 1, etc) puisqu'elles appliquent les meilleures procédures de sécurité au sein du S.I.. Le choix du modèle de cloud sera déterminant notamment en rapport avec le souhait du client sur l'organisation.