

Sécurité de cloud computing : approches et solutions

Al Haddad Zayed¹, Hanoune Mostafa², Mamouni Abdelaziz³

Faculté des Sciences Ben M'Sik, Département Mathématiques et Informatique, Université Hassan II de Casablanca

Cdt Driss El Harti, BP 7955 Sidi Othman Casablanca, Maroc

¹Alhaddadtri@gmail.com

²Mhanoune@gmail.com

³Mamouni.abdelaziz@gmail.com

Résumé_ Cloud computing est une révolution économique et technologique, dans lequel les ressources informatiques sont fournies en tant que service via internet. En particulier, ces ressources peuvent être provisionnées de façon dynamique et libérées en fonction de la demande de service et avec un effort minimal de gestion. Il présente une meilleure solution pour gérer les données, les infrastructures, etc. Cependant, la sécurité des données en transit dans un Cloud public reste un challenge pour les fournisseurs de Cloud. En effet, ces données sont la cible de plusieurs attaques réseau, qui ont pour but d'interrompre, d'intercepter, de modifier et de fabriquer des informations. Par conséquent, il est essentiel de faire face à ces attaques en vue d'améliorer l'utilisation et l'adoption de Cloud. A travers cet article nous présentons une étude détaillée sur la sécurité du cloud en fournissant les plus importantes solutions existantes dans ce domaine. Ensuite, nous allons proposer un exemple concret de sécurisation basant sur une méthodologie en couches.

Mots-clés _ Cloud Computing, Sécurité, Vulnérabilité, Authentification.

INTRODUCTION

Cloud computing est devenu incontournable dans la mise en place et la fourniture des services informatiques pour les entreprises. Aujourd'hui, plusieurs entreprises considèrent le cloud computing comme une force majeure à modifier de façon significative l'ensemble de la technologie d'information, la façon dont les centres de données sont construits, la façon dont les logiciels sont déployés, le traitement des mises à jour[1], etc. Il leur permet de remplacer les coûts en capitaux par des coûts variables, de bénéficier d'importantes économies d'échelle, de cesser de deviner la capacité nécessaire, ainsi il offre une vitesse et souplesse accrues[2]. Malgré ces avantages, la

sécurité des données reste un sujet d'inquiétude pour les entreprises et représente un frein majeur pour l'adoption de cette technologie. Pour atténuer ce problème de sécurité, nous présentons à travers cet article un état de l'art sur la sécurité du cloud computing en étudiant les différentes solutions proposées dans ce domaine. Ce papier est organisé comme suit : La section II décrit en détail les travaux connexes. La section III présente les différentes solutions existantes. Dans la section V, on termine cet article avec une conclusion et les perspectives.

LES TRAVAUX CONNEXES SUR LA SECURITE DU CLOUD

La protection de la vie privée et la sécurité des données sont primordiales dans l'utilisation des services cloud. Il existe plusieurs travaux réalisés dans ce domaine[3][4][5]. Des modèles, des approches et des techniques sont proposés afin de protéger les données. M. Singh et S. Singh[6], ont proposé un système d'authentification à plusieurs niveaux visant à renforcer la sécurité dans les transactions financières. Satish et Anita[7], ont proposé une méthode de faux écran pour assurer l'authentification à deux niveaux dans le cloud computing. Tandis que, Arasu et al. [8], ont proposé une méthode utilisant le code d'authentification de message dans laquelle la clé cryptographique, le message et la fonction de hachage sont concaténés ensemble pour assurer l'authentification. Parsi et Sudha [9], ont proposé une méthode utilisant

l'algorithme RSA pour l'authentification et le transfert sécurisé de données. Cette méthode implique une phase de génération de clé, le chiffrement et le déchiffrement. Dans [3] Il a proposé une technique de sécurité de données dans le cloud par la combinaison des différents mécanismes, à savoir : l'authentification multi-facteur par un mot de passe à usage unique et le code d'authentification d'une empreinte cryptographique de message avec une clé. Dans [10], le concept de signature numérique avec l'algorithme RSA a été proposé, pour crypter les données avant de les transmettre sur le réseau. Cette technique permet de résoudre le problème de l'authentification et de la sécurité en utilisant les techniques d'anonymisation. Balasaraswathi et Manikandan[11], ont proposé une architecture de cloud multiple basée sur le partitionnement de données chiffrées avec une approche dynamique afin de sécuriser l'information en transit ou en reste. Nous avons analysé plusieurs approches de transfert sécurisé de données, ces approches se focalisent principalement sur les paramètres d'authentification. En effet, les données en transit vers le cloud peuvent être attaquées par différents intercepteurs non autorisés. Une méthode particulière ne suffit pas à traiter toutes les questions de sécurité et de confidentialité des données. Par conséquent, différentes techniques et mécanismes intégrés devraient être utilisés [12].

SECURITE DANS LE CLOUD COMPUTING

Le cloud computing basé sur les technologies de la multi-location (voir la figure ci-après) et de la virtualisation ce qui introduit des nouvelles risques et des vulnérabilités de sécurité spécifiques au cloud computing en plus des risques encourus par les environnements traditionnels[13]. Les risques de sécurité dans le cloud peuvent différer des risques de l'infrastructure d'informatique

traditionnelle, soit dans la nature ou de l'intensité ou les deux [14].

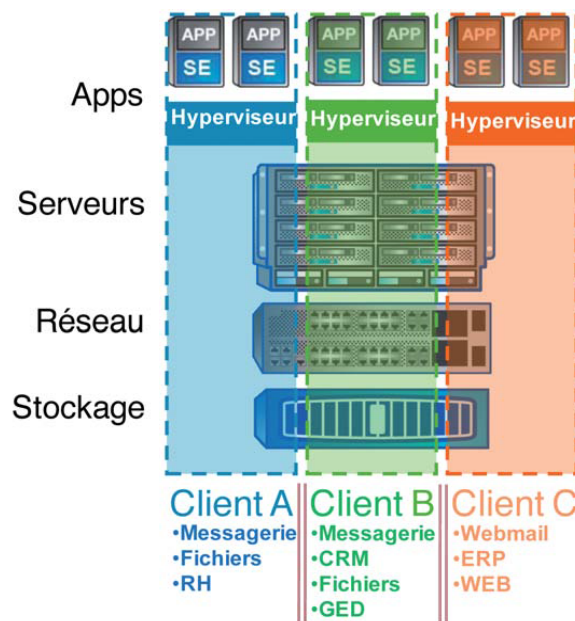


Fig. 13 Multi-location sécurisée

La mutualisation des ressources permet une économie sur les matériels et donc indirectement une diminution de la consommation électrique grâce aux technologies des virtualisation et multi-locations, mais ces technologies introduisent certains risques dans le système. Le partage de l'infrastructure entre plusieurs clients conduit aux risques de la visibilité des données par d'autres utilisateurs. De plus, les utilisateurs de cloud veulent garantir que les données critiques ne sont pas accessibles et utilisées illégalement, même par les fournisseurs du cloud. Le service à la demande est fourni aux clients par des interfaces de gestion basées sur le web qui provoque la probabilité d'un accès non autorisé à l'interface de gestion plus élevé que les systèmes traditionnels. Selon [14], Il existe deux types de communication, à savoir, la communication externe « entre clients et

cloud » et la communication interne « entre l'infrastructure cloud ». Concernant la première, les services du cloud sont accessibles via l'internet en utilisant des mécanismes et des protocoles d'internet standards afin de transmettre des données ou des applications entre les clients et le cloud. Ce type de communication est similaire à celle de toute autre communication sur Internet. En effet, les données en transit peuvent être la cible de plusieurs attaques malveillantes [13][14]. Parmi ces attaques, on peut citer déni de service (DoS), l'écoute, l'usurpation d'identité, l'home de milieu, etc. Concernant la deuxième, c'est -à-dire la communication entre les MVs. Cette communication est cible des attaques malveillants à cause de facteurs suivants, l'infrastructure de communication partagée, le réseau virtuel et la mauvaise configuration de sécurité. Selon [15], la sécurité du Cloud doit être l'affaire de tous, à savoir, les fournisseurs, les prestataires et les utilisateurs. La sécurité du Cloud nécessite une profonde remise en question des politiques de sécurité des entreprises. Elles doivent aller au-delà de la gestion étroite des mots de passe et des privilèges de connexion. Il est nécessaire de passer à l'étape supérieure et de penser la sécurité en termes d'usage et de types des données. Plus elles sont sensibles, plus la sécurité doit être élevée et plus le choix du type de Cloud est critique et crucial. Le niveau de sécurité du Cloud public n'est pas optimisé pour un usage professionnel, mais sa souplesse d'utilisation et son rapport qualité-prix peut le rendre séduisant aux yeux de nombreuses petites structures. Le Cloud Privé quant à lui repose sur le même principe que le Cloud

public, mais il est bien sûr détenu par une entreprise et à destination d'un nombre plus restreint d'utilisateurs, clients ou partenaires de la société propriétaire. Enfin le Cloud hybride est un mix de Cloud privé et public. Il est constitué de plusieurs partenaires internes et externes. Son intérêt réside dans sa capacité à faire naviguer les données entre la partie publique et privée en fonction de leur sensibilité afin d'optimiser les coûts. Quel que soit son type les fournisseurs de solution Cloud s'appuient sur un mix de code propriétaire et d'open source pour assurer la sécurité et l'intégrité des données qu'ils hébergent et protègent. D'après [16], Quelle que soit la forme du contrat de Cloud Computing, ce contrat doit absolument inclure ces cinq points clés, à savoir, localisation des données, loi et Juridiction, niveaux de service fourni par le prestataire de Cloud Computing, réversibilité et accès aux données et sécurité des données. Par ailleurs, l'ordre d'importance de ces cinq points clés variera selon le service utilisé (IaaS, PaaS, SaaS) et sa finalité (espace de stockage, environnement de développement, outil de facturation). D'après [17], les défis de sécurité du Cloud sont la dispersion des données et lois internationales relatives au respect de la vie privée, besoin de gestion de l'isolation, multi-location, défis de la journalisation, problèmes de propriété de données et garanties de qualité de service, dépendance d'hyperviseurs sécurisés, attraction des hackers (cible intéressante), sécurité des OS virtuels dans le Cloud, possibilité d'interruptions massives de service, besoins de chiffrement pour la sécurité dans le Cloud, sécurité du Cloud public versus sécurité du Cloud privé et le

manque de dispositif public de contrôle de version des versions du SaaS. Et parmi les principales menaces selon CSA/HP on trouve entre autre, abus et utilisation malveillante du Cloud Computing, interfaces et API non sécurisés, malveillances internes, problèmes dus au partage de technologie, perte ou fuite de données, détournement de compte ou de service et enfin profil de risque inconnu. De plus, ENISA a identifiés trente cinq risques de sécurisé, ces risques sont liés aux risques politiques et organisationnels, risques techniques, risques juridiques ainsi aux risques non spécifiques au Cloud. Et parmi les risques les plus élevés selon l'ENISA on trouve, enfermement dans une solution, perte de gouvernance et de contrôle, défis de conformité, échec de l'isolation (multi-location), ordonnance de tribunal, citation, mandat de perquisition, saisie par le gouvernement local, changement de juridictions, protection des données et enfin réseau (congestion, utilisation non optimale...). La colocation sécurisée consiste en l'hébergement sur le Cloud des applications et données de multiples clients (sociétés, organisations, entités métier...) au sein d'une seule et unique infrastructure physique, mutualisée, tout en respectant la sécurité, notamment au sens de la confidentialité. D'après[18], il existe neuf principaux risques, à savoir, la perte de maîtrise et ou de gouvernance, des déficiences au niveau des interfaces et des APIs, conformités et maintien de la conformité, localisation des données, ségrégation ou isolement des environnement et des données, perte et destruction maîtrisée de données, récupération des données, malveillance dans l'utilisation et enfin usurpation. Parmi

les responsabilités juridiques de la sécurité et de la confidentialité des données dans le Cloud selon[18], on trouve que le Client est juridiquement responsable de ses données et de leur utilisation, notamment de tout ce qui concerne leur conformité aux obligations juridiques. Alors que, le Prestataire est soumis à des obligations techniques et organisationnelles. Il s'engage à préserver l'intégrité et la confidentialité des données, à protéger et récupérer des données, à chiffrer les données, etc.

METHODOLOGIE EN COUCHES

A. Modèle de sécurité des données proposé dans le cloud

L'approche en couches a été donnée dans la figure 1, où la première couche est responsable de l'authentification de l'utilisateur. La deuxième couche est responsable de l'anonymisation des données et de la protection de la vie privée des utilisateurs et la troisième couche est responsable de la récupération des données et du déchiffrement[19][20].

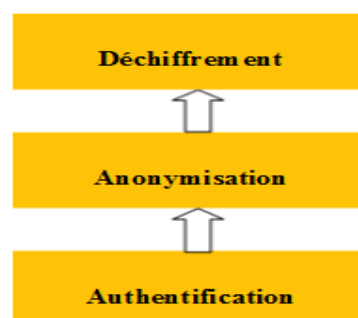


Fig. 14 Modèle de sécurité de données dans le cloud

B. Mécanisme OTP

Mécanisme one time password (OTP) ou le mot de passe à usage unique est un mot de passe qui n'est valable que pour une

session ou une transaction. L'utilisation d'une authentification multi facteur avec OTP réduit les risques associés avec la connexion au système depuis un poste de travail non sécurisé[21]. OTP est comme un système de validation qui fournit une couche supplémentaire de sécurité pour les données et les informations sensibles en demandant un mot de passe qui est uniquement valable pour une seule connexion. De plus, ce mot de passe n'est plus choisi par l'utilisateur, mais généré automatiquement par une méthode de précalculé, ce qui va éliminer certaines lacunes associées aux mots de passe statiques telles que les lacunes de longévité du mot de passe, de simplicité du mot de passe et d'attaque par force brute. OTPs sont générés du côté du serveur et envoyés à l'utilisateur en utilisant un canal de télécommunication. Ils ne sont pas susceptible aux utilisateurs malveillants de trouver le nom d'utilisateur et mot de passe pour accéder à la ressource. On ne peut rien faire pour obtenir dans le cloud sans la bonne combinaison de nom d'utilisateur, le mot de passe et le mot de passe à usage unique. Afin de sécuriser le système d'une manière plus efficace, l'OTP généré doit être difficile à estimer, retrouver, ou tracer par les pirates. Par conséquent, il est très important de développer des algorithmes de génération d'OTP sécurisé[22]. Plusieurs éléments peuvent être utilisés pour générer un mot de passe à usage unique difficile à deviner[23], à savoir, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), nom d'utilisateur, PIN, minute, heure, etc.

C. Techniques de chiffrements

La mutualisation des ressources est l'une des principales caractéristiques du cloud computing, où ces ressources sont partagées entre plusieurs utilisateurs du service. Ce partage rend l'emplacement exact des données des utilisateurs impossible à déterminer, ce qui peut poser des problèmes liés notamment à la localisation des données, à leur sécurité, à leur accessibilité, etc[19]. Pour cela, des techniques devraient être utilisés afin d'assurer la vie privée et la confidentialité de données en transit et en repos. Pour augmenter le niveau de sécurité des données dans le cloud public, il est important de les chiffrer en utilisant l'anonymisation avec des sauvegardes et des audits[20]. L'anonymisation peut être définie comme l'opération de suppression de l'ensemble des informations permettant d'identifier directement ou indirectement un individu[24], contenues dans un document ou une base de données et ce qui va rendre très difficile de ré-identifier les personnes ou les entités concernées. L'anonymisation de données peut être utilisées pour répondre à la question de la confidentialité des données tout en permettant aux données d'être analysées et utilisées efficacement. Les données anonymes peuvent être transmises et traitées sans la préoccupation de leurs propriétaires. Ensuite, elles peuvent être mises en correspondance avec les données d'origine dans un endroit sécurisé et fiable.

CONCLUSION

Le Cloud computing est une technologie très prometteuse permettant à ses clients de réduire les coûts d'exploitation, d'administration etc. Tout en augmentant l'efficacité, toutefois, l'adoption de cette

technologie reste faible, et cela revient aux problèmes de sécurité en particulier la sécurité des données échangées sur le réseau internet. Afin de résoudre ces problèmes et d'améliorer l'adoption et l'utilisation de cette technologie. Nous avons étudié les aspects de sécurité du cloud, ensuite nous avons présenté les différentes solutions existantes, par la suite nous allons présenter en détaille une solution basant sur une architecture de cloud multiple. Cette solution permet un accès sécurisé au cloud en utilisant le mot de passe à usage unique (OTP) et permet également d'assurer la sécurité des données en transit en utilisant l'anonymisation des identités ce qui permet aux données d'être analysées et utilisées efficacement et sans se soucier de leurs sécurité.

Références

- [1] "5 Tendances pour transformer le Cloud Computing | Tunisie Cloud Computing - Cloud Computing, Système d'information en Tunisie."
- [2] "AWS | Qu'est-ce que le cloud computing – Les avantages du cloud," *Amazon Web Services, Inc.* [Online]. Available: [//aws.amazon.com/fr/what-is-cloud-computing/](https://aws.amazon.com/fr/what-is-cloud-computing/). [Accessed: 07-Jul-2015].
- [3] P. Pankaj and C. Inderveer, "A Secure Data Transfer Technique for Cloud Computing," THAPAR UNIVERSITY, August 2014, 2014.
- [4] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, Jan. 2013.
- [5] K. Arjun, G. L. Byung, L. HoonJae, and K. Anu, "Secure Storage and Access of Data in Cloud," *International Conference on ICT Convergence (ICTC)*, 15-Oct-2012.
- [6] S. Maninder and S. Sarbjeet, "Design and Implementation of Multi-tier Authentication Scheme in Cloud," *IJCSI Int. J. Comput. Sci.*, vol. 9, no. 2.
- [7] K. Satish and G. Anita, "Multi-Authentication for Cloud Security: A Framework," *Int. J. Comput. Sci. Eng. Technol. IJCSET*, vol. 5, no. 04, Apr. 2014.
- [8] A. S.Ezhil, G. B, and A. S, "Privacy -Preserving Public Auditing In Cloud Using HMAC Algorithm," *Int. J. Recent Technol. Eng. IJRTE*, vol. 2, Mar. 2013.
- [9] P. Kalpana and S. Singaraju, "Data security in cloud computing using RSA algorithm," *IJRCCCT*, vol. 1, no. 4, pp. 143–146, 2012.
- [10] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," 2010, pp. 211–216.
- [11] V. R. Balasaraswathi and S. Manikandan, "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach," in *Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on*, 2014, pp. 1190–1194.
- [12] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," 2009, p. 127.
- [13] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, Apr. 2014.
- [14] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci.*, vol. 305, pp. 357–383, Jun. 2015.
- [15] B.-H. CARINE, "Cloud computing, la sécurité en question."
- [16] J. Guillaume, "securite-des-donnees-5-points-a-verifier-avant-de-signer-son-contrat-de-cloud-computing," Sep-2014.
- [17] S. Pascal, "Cloud Computing et Sécurité, Cycle de conférences sur cloud computing et virtualisation, Sécurité de la Virtualisation et du Cloud Computing," Paris, 2010.
- [18] K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilité des données entreposées dans les nuages," in *9ème atelier Fouille de données complexes (EGC-FDC 2012)*, 2012.
- [19] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in *Informatics and Systems (INFOS), 2012 8th International Conference on*, 2012, pp. CC–12.
- [20] Institute of Electrical and Electronics Engineers, Ed., "Enhancing Data Security during Transit in Public Cloud," *Int. J. Eng. Innov. Technol. IJEIT*, vol. 3, Jul. 2013.
- [21] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012, pp. 647–651.
- [22] Balakrishnan.S, Saranya.G, Shobana.S, and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud," *Int. J. Comput. Sci Ence Technol.*, vol. 2, Jun. 2011.
- [23] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009, pp. 641–644.
- [24] "La protection des données personnelles dans l'open data : une exigence et une opportunité." [Online]. Available: <http://www.senat.fr/rap/r13-469/r13-4697.html>. [Accessed: 08-Jul-2015].