Journée Cloud LIRIS

CLOUD 2012, IEEE 5th International Conference on Cloud Computing Applications and Experiences Track 5 & 6 - cloud security

PhD Student : W. F. Ouedraogo[1],
Université de Lyon, CNRS INSA-Lyon. LIRIS. UMR5205. F-69621. France,
20 Avenue Albert Einstein 69621 Villeurbanne cedex, France
E-mail: wendpanga-francis@liris.cnrs.fr

21/02/2013

Defining and Implementing Connection Anonymity for SaaS Web Services

Vinícius Pacheco and Ricardo Puttini

Objectif

- Proposer une approche pour protéger l'identité du consommateur Cloud durant les échanges de messages en mode SaaS.
- Proposer un framework d'anonymisation multicouche utilisant différents techniques d'anonymisation.
- Définir deux manières pour générer et gérer les informations d'identification de façon anonyme.

WEB SERVICE CONSUMPTION IN SAAS

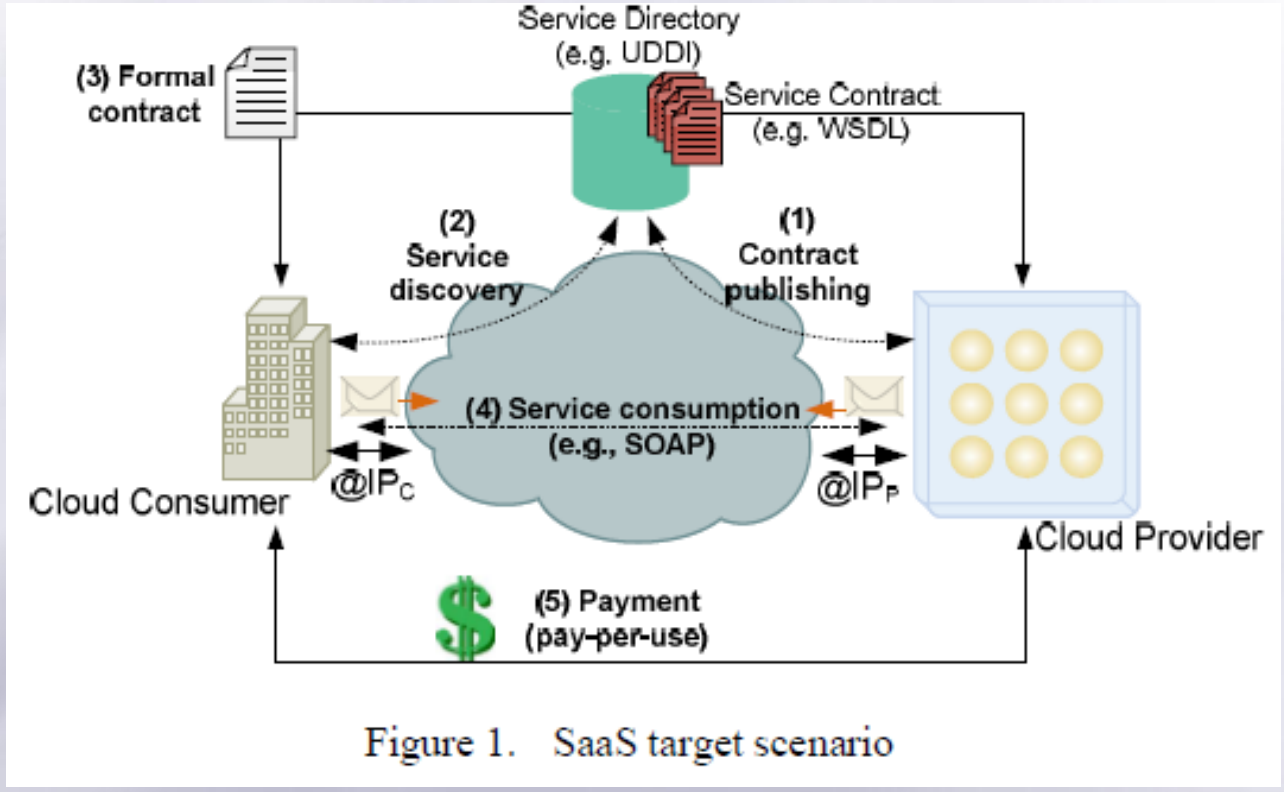


Figure 1. SaaS target scenario

Privacy Assessment

- 3 niveaux d'interactions permettent de reveler la privacy d'un client
  - **Consumer-Provider Contract**
  - **Message Exchanges**
  - **Network-Level**

- Les différents types de privacy :
  - **ID privacy:** cacher ID du sujet.
  - **Location privacy:** ne pas révéler le lieu physique du sujet.
  - **Behavior privacy :** cacher non pas le contenu mais la façon dont ce contenu est manipulé ou utilisé.
  - **Content privacy:** dissimuler les informations du sujet.

Proposition : SAAS ANONYMITY FRAMEWORK

- SaaS Contract Connection Anonymity Layer :

  Utilisation d'un third-party broker (TPB) pour :

  - **établir le contrat entre les différents acteurs,**
  - **émettre des informations d'identification anonymes « onetime-usage »,**
  - **agir comme intermédiaire pour la facturation.**
    - *en émettant des informations d'identification anonymes traçables (paiement après usage)*
    - *en émettant des informations d'identification anonymes non traçables (pas de facturation à posteriori, paiement immédiat lors de la consommation –utilisation de monnaie virtuel e-cash)*

- SaaS Message Metadata Connection Anonymity Layer :
  - **Les métadonnées sont représentées par les informations d'identification anonymes, émises par le TPB et incluses dans les messages du consommateur.**

SAAS ANONYMITY FRAMEWORK

- Network Connection Anonymity Layer :
  - **Utiliser les systèmes mix-net actuels (onion-router - tor) à faible latence.**
- Message Data Anonymity Layer :
  - **Utiliser les techniques d'anonymisation de données de type k-anonymat,**
  - **Utiliser des approches basées sur les systèmes de chiffrement homomorphique.**

SAAS ANONYMITY FRAMEWORK : traceable anonymity

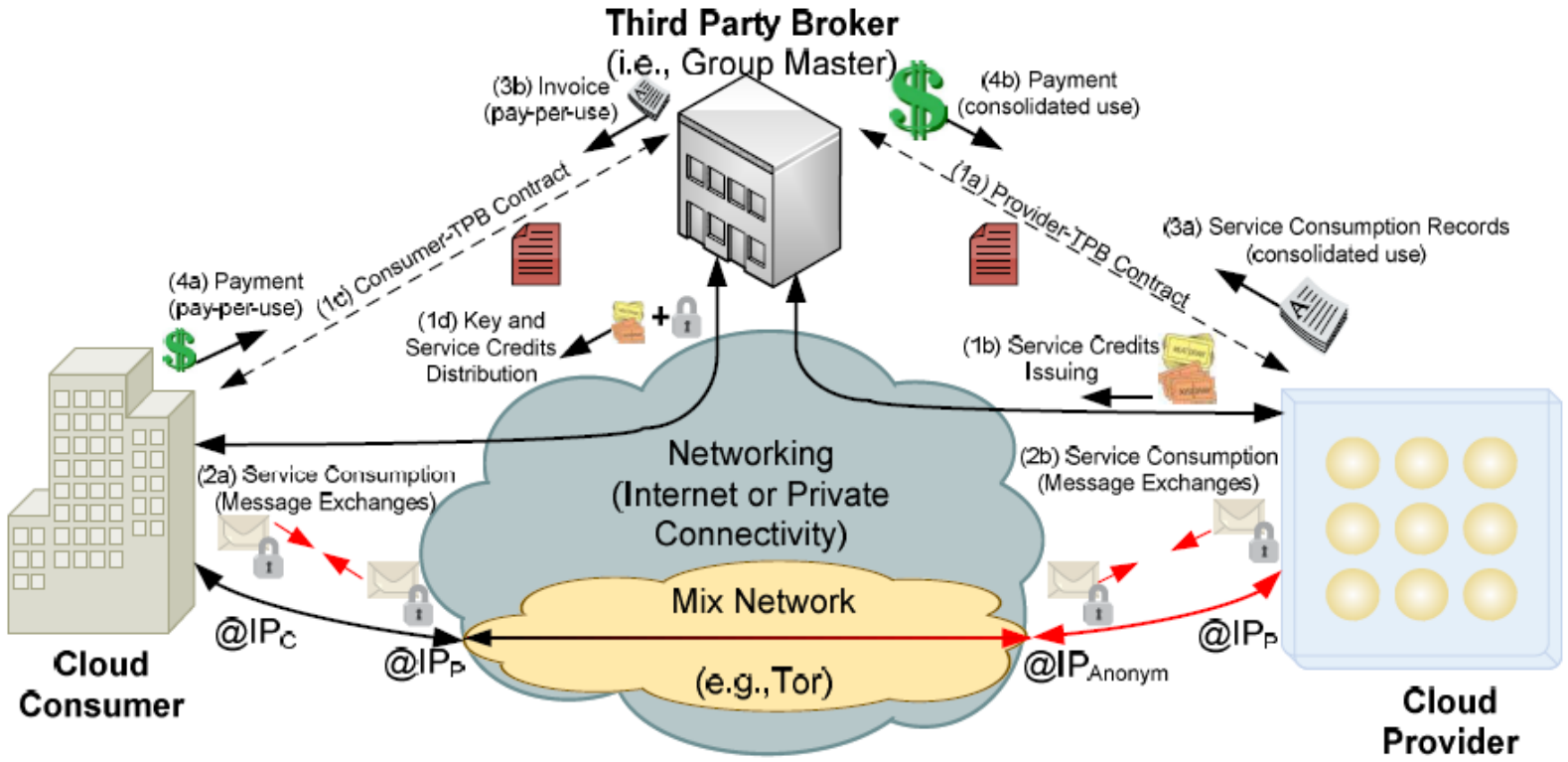


Figure 2. Anonymous Service Consumption – Traceable Anonymity

SAAS ANONYMITY FRAMEWORK : Untraceable anonymity

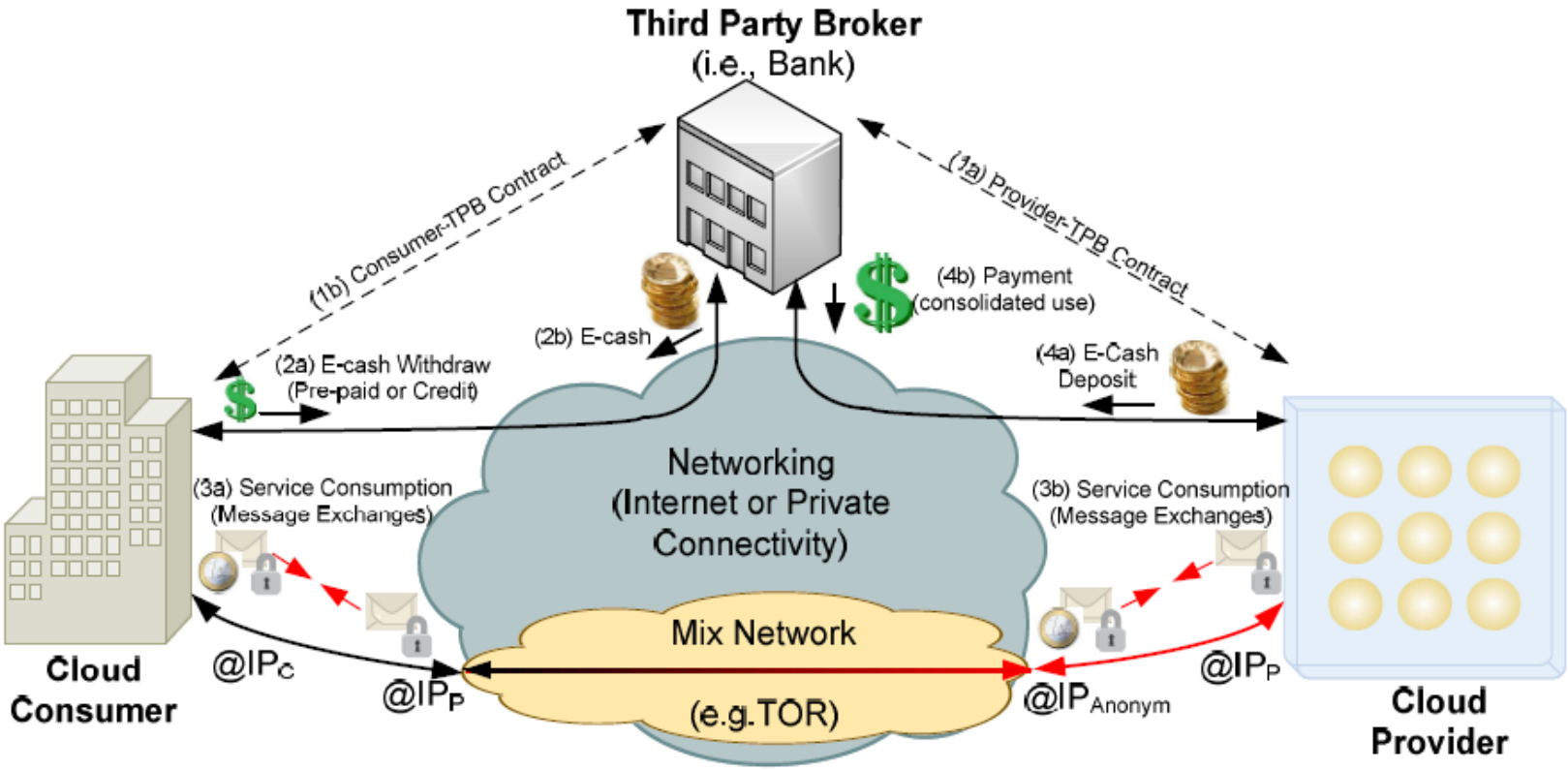


Figure 3: Untraceable Anonymous Service Consumption

Analyse critique

- **+ ++**
  - L'idée du Broker ➔ Permet de préserver l'anonymat en jouant le rôle d'intermédiaire entre le client et le fournisseur de service
  - La solution proposée assure l'anonymat depuis l'établissement du contrat jusqu'à la facturation du client
- **- - -**
  - Réseau de type Tor ➔ environnement non sure pour faire passer des informations confidentielles à moins de privilégier l'anonymat au détriment de la sécurité des informations qui y transitent
  - Anonymat total ne être utilisé que dans des environnements spécifiques ou pour des services spécifiques.

MANTICORE: Masking All Network Traffic via IP Concealment with OpenVPN Relaying to EC2

Patrick Butler, Adam Rhodes, and Ragib Hasan

Context

- Les chercheurs en Forensic (investigation légale) et les malware communiquent souvent avec des réseaux réputés non sûrs

- ➔ Nécessiter d'utilisation d'un serveur proxy pour dissimuler la véritable origine du trafic réseau.

Objectif

- définir un système qui combine les idées de VPN avec la fonctionnalité d'instanciation du cloud computing afin de masquer dynamiquement et réassigner l'adresse IP du système.

Travaux sur les systèmes de proxy

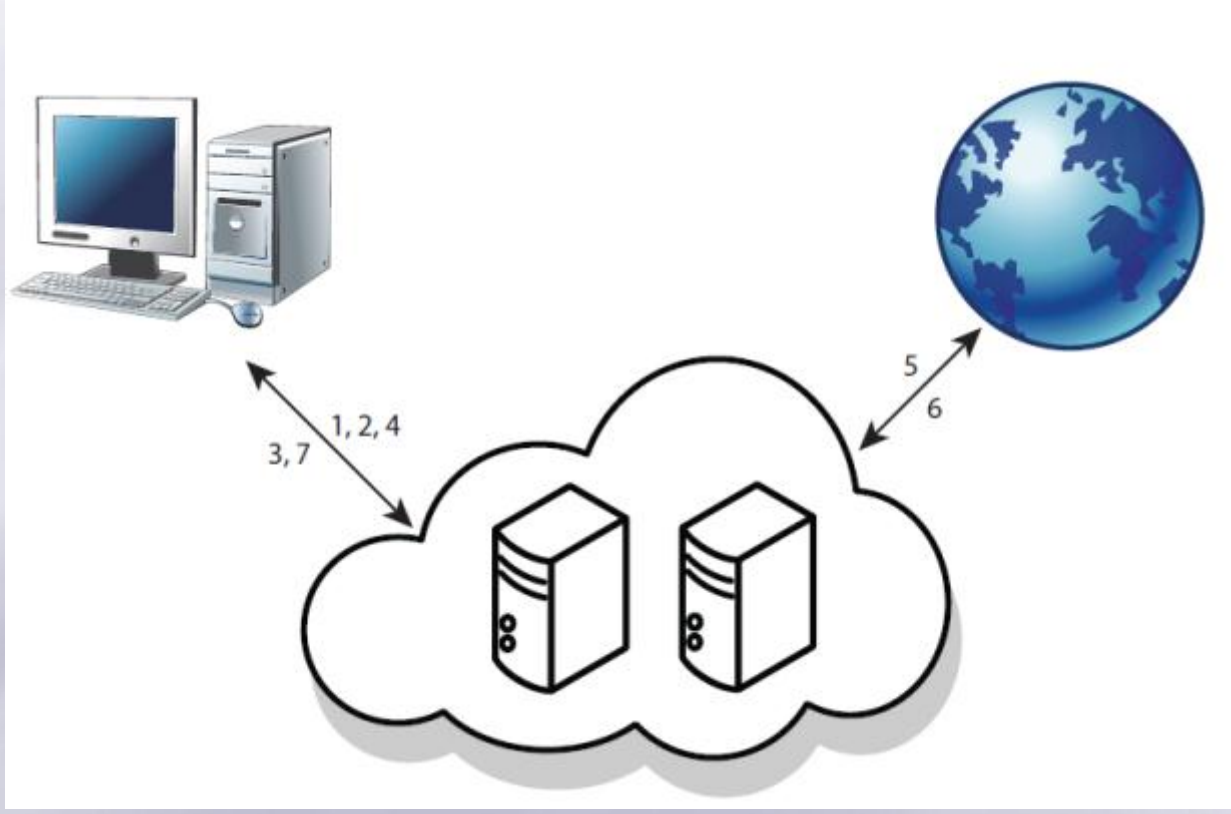
- Anonymat et routage anonyme sur Internet (onion routing tor)
  - **Inconvénient :** nombreux serveurs blacklistent les adresses IP
- Web based proxies and browser based proxies
  - **Inconvenient :**
    - *traffic SSH et FTP non acheminé*
    - *encapsulation des requêtes dans un iframe ➔contraignant*
- VPN based proxy
  - **inconvénient :** Ip statique

Solution proposée : MANTICORE

- extension d'un VPN à base de proxy qui tire partie de la nature élastique du cloud.
- utilise deux systèmes principaux:
  - **Amazon Elastic Compute Cloud (EC2)**
  - **OpenVPN**
- Chaque fois qu'une VM est instanciée, il lui est attribué une adresse IP unique basée sur un algorithme propriétaire d'Amazon.

➔ Solution : redémarrer l'instance qui se verra réattribuer une autre adresse IP.

Solution proposée



Test

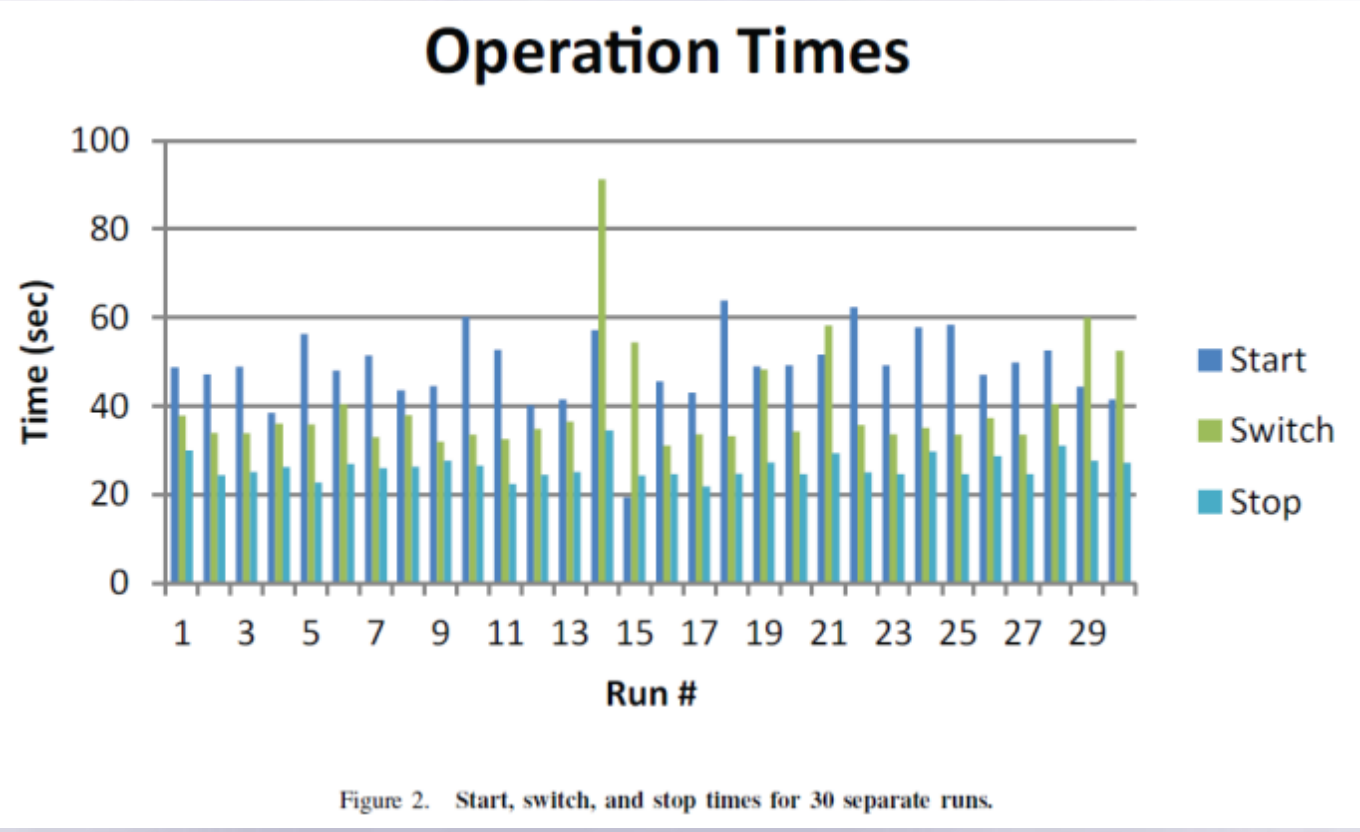


Figure 2. Start, switch, and stop times for 30 separate runs.

Analyse critique

- ++++
  - Solution proposée permet de masquer l'origine du trafic,
  - Mise en œuvre facile
- - - - -
  - Le processus de démarrage d'arrêt et de Switch est contraignant avec un temps d'attente non négligeable

Hatman: Intra-cloud Trust Management for Hadoop

Safwan Mahmud Khan and Kevin W. Hamlen

Context

- Les tâches dans le Cloud sont distribuées en fonction de la charge des nœuds, et non pas de leur réputation
- Compromettre même un seul nœud du Cloud suffit à corrompre l'intégrité d'un grand nombre d'opérations distribuées.

Objectif

- évaluer dynamiquement l'intégrité des nœuds en comparant les sorties des tâches répliquées pour assurer la cohérence.
- Assurer l'intégrité des données et des opérations effectuées ainsi que la sécurité dans un Cloud.

Hatman Architecture

- Hatman (Hadoop Trust Manager) ajoute aux NameNodes de Hadoop une extension de réputation

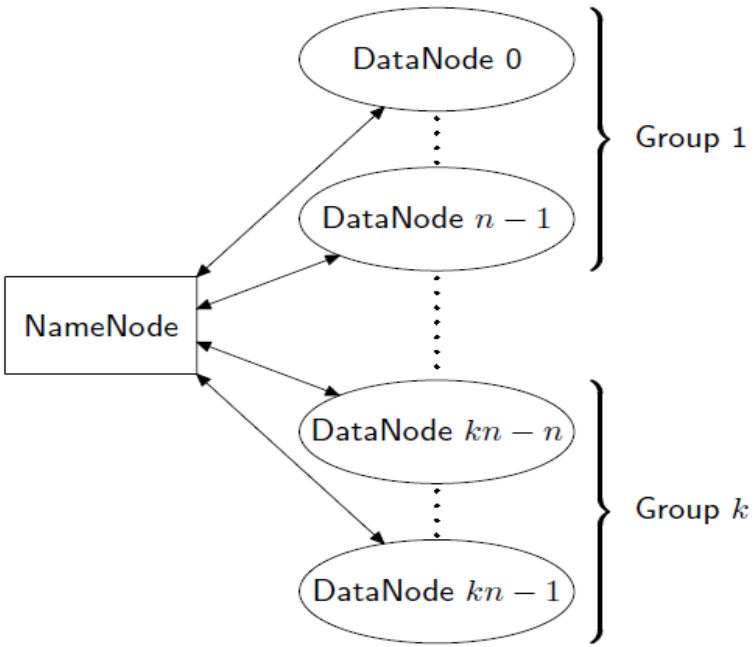


Figure 1. A Hatman job replicated k times and distributed across n data nodes per replica group.

Hatman Architecture

Algorithm 1 Hatman job processing

Input: job J, group size n, replication factor k
Output: job result r

1: Choose k unique groups G_g each of size n
2: **for all** groups G_g **do**
3: $r_g \leftarrow HadoopDispatch(G_g, J)$
4: **end for**
5: **for all** pairs (G_g, G_h) with $g \neq h$ **do**
6: **if** r_g and r_h are small **then**
7: $eq \leftarrow (r_g =? r_h)$
8: **else**
9: $eq \leftarrow HatmanDispatch(r_g =? r_h)$
10: **end if**
11: **for all** $(i, j) \in G_g \times G_h$ with $i \neq j$ **do**
12: $C_{ij} \leftarrow C_{ij} + 1$ (and $C_{ji} = C_{ij}$)
13: **if** $eq = true$ **then**
14: $A_{ij} \leftarrow A_{ij} + 1$ (and $A_{ji} = A_{ji}$)
15: **end if**
16: **end for**
17: **end for**
18: **if** time to update trust vector **then**
19: $T \leftarrow HatmanDispatch(tmatrix(A, C))$
20: $t \leftarrow HatmanDispatch(EigenTrust(T))$
21: **end if**
22: $m \leftarrow \arg\max_g \ eval(G_g)$
23: **return** r_m

Analyse critique

- ++++
  - Permet d'assurer l'intégrité des données et opérations exécutées sur les différents nœuds et de s'assurer de la cohérence
- - - - -
  - Mobilise beaucoup de ressources pour le calcul des tâches répliquées,
  - Algorithme n'est efficace que quand le nombre de réplica est élevé

Programmable Order-Preserving Secure Index for Encrypted Database Query

Dongxi Liu Shenlu Wang

LIRIS UMR 5205 CNRS

Context

- Utilisation des services de BD dans le cloud (Amazon Relational Database Service (RDS) et Microsoft SQL Azure) pour externaliser les BD.
- Préoccupation importante : gestion de la sécurité et de la privacy
- Solution simple: chiffrer la BD ➔ Une BD chiffrée ne peut pas être facilement interrogeable

Objectif

- Proposer une solution préservant l'ordre d'indexation des données chiffrées pour faciliter les requêtes sur la BD cryptées.

Context

- S'intéresse aux requêtes de BD sur un intervalle :

  Select staffs who join the company between 2000 and 2012

- Les requêtes d'égalité ne sont pas difficiles à gérer quand un schéma de chiffrement déterministe (par exemple, AES en mode ECB) est utilisé
- les requêtes d'agrégation ont besoin d'algorithmes de chiffrement homomorphique [11] pour traiter les opérations SQL (de SUM et AVG)

State of art

- Pour traiter les requêtes avec intervalle sur des BD cryptées
  - un schéma de chiffrement préservant l'ordre a été déjà proposé par *R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. « Order preserving encryption for numeric data ».*

  ➔**Pour utiliser ce système, les utilisateurs doivent être en mesure de modéliser les distributions des valeurs dans le plaintext et ciphertext**

- Construire des polynômes préservant l'ordre
  - mécanisme uniquement applicable à un domaine fini de plaintext,
  - les résultats d'évaluation des polynômes préservant l'ordre peut révéler la distribution des plaintext.

Solution

- un schéma d'indexation préservant l'ordre construit sur des expressions linéaires simples de la forme : **a * x + b + noise**
- La forme des expressions est publique, mais les coefficients a et b sont gardés secrets.
- Le noise est soigneusement sélectionné, de telle sorte que l'ordre des données d'entrée est préservé.

Solution : architecture

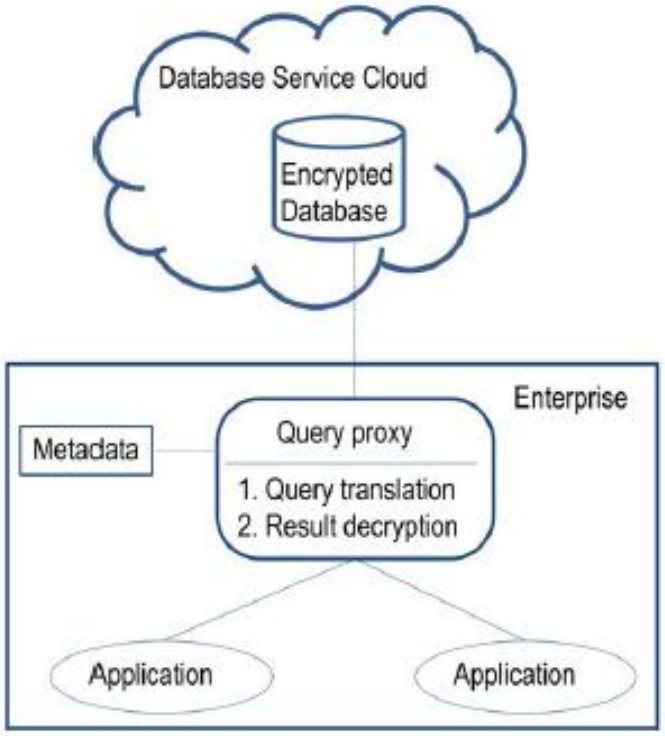


Figure 1. Architecture of Querying Encrypted Databases

Analyse critique

- ++++
  - Leur système d'indexation permet de programmer des expressions d'indexation basiques qui traitent différentes valeurs d'entrée avec différents expressions d'indexation.
  - Schéma d'indexation proposé ne dépend que des expressions linéaires,
  - Système plus facile à implémenter,
  - Le système n'est pas un système de cryptage, il peut donc être utilisé en association avec des algorithmes de chiffrement existantes (ex AES).
- - - - -
  - Ne traite seulement que les requêtes par intervalle

Maitland: Lighter-Weight VM Introspection to Support Cyber-Security in the Cloud

Chris Benninger, Stephen W. Neville,
Yagiz Onat Yazir, Chris Matthews, Yvonne Coady

Context

- Les environnements de cloud computing sont des cibles attrayants pour les logiciels malveillants car la structure des Clouds permet :
  - l'exécution de code à distance
  - Offre une possibilité de s'affranchir du confinement imposé par les (VM)
- L'introspection de VM fournit l'un des principaux outils de la cyber-sécurité pour analyser les comportements du code des utilisateurs à l'exécution.
  - Traditionnellement, les outils d'introspection exigent une intégration étroite avec les hyperviseurs sous-jacentes
  - Et une importante re-engineering lors de l'application des mises à jours et patches des OS.

State of art

- Moyens traditionnels pour répondre aux logiciels malveillants
  - **L'analyse statique : analyse du code avant son exécution**
  - **L'analyse dynamique : analyse du code à l'exécution**
- L'analyse statique échoue assez facilement lorsque :
  - les séquences d'instructions malveillantes sont chiffrées
  - Le code est packagé cachant ainsi les signatures malveillants connus.
    - *Le package multi-couche peut également être utilisé pour vaincre les tentatives défensives.*
- Obfuscation ou « assombrissement » du code

State of art

- Les techniques standards de détection dynamiques sont en grande partie limitées à l'analyse des informations contenues dans les codes exécutées ➔ **détecte pas les codes dormants**

Solution

- L'introspection des VM fournit un moyen intéressant de combiner des techniques de détection dynamiques et statiques
  - **fournir un ensemble d'informations disponibles dans n'importe quelles pages mémoires exécutables ainsi que les sous-ensembles d'instructions exécutées**

Solution : Maitland Architecture

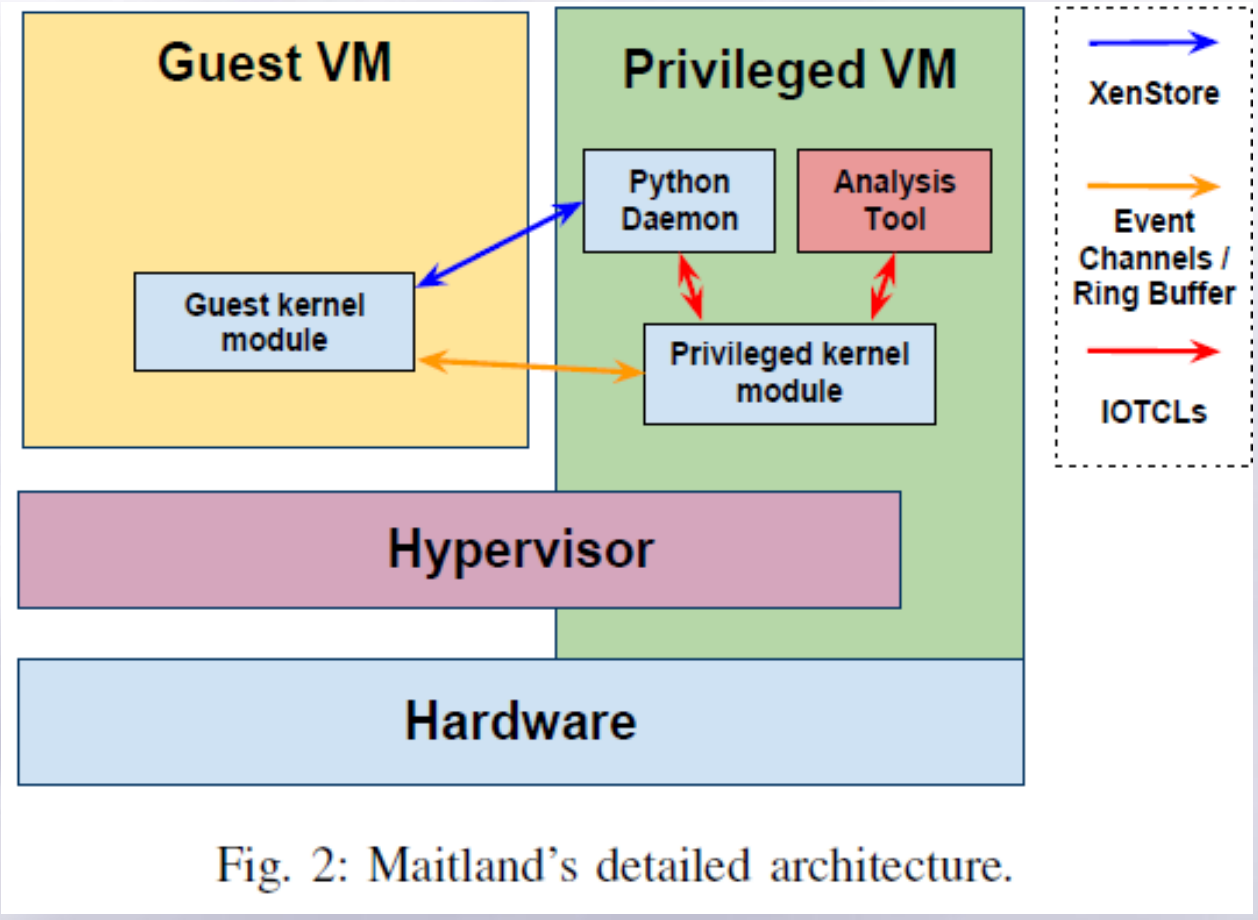


Fig. 2: Maitland's detailed architecture.

Solution: processus d'introspection

- Detecting Memory Page Unpacking and Decryption
  - Les pages mémoires qui passe d'un état de page de donnée à page exécutable sont repérés car les codes malveillants packagés ou chiffrés pour être exécutable ont besoin d'effectuer cette opération
- Accessing a Process' Memory Snapshot
  - Une fois détecté, le processus à l'origine de l'opération est supprimé de l'ordonnanceur de l'OS, et toutes les pages manipulées par ce processus sont ensuite copiées ver le « privilège VM ».
- Accessing a Process' Memory Snapshot
  - Tout outil d'analyse en cours d'exécution dans la machine virtuelle privilégiée peut alors voir et évaluer la mémoire capturer du processus suspecté
- Responding to a Perceived Threat
  - Si une activité suspect est détectée,
    - *On met fin au processus à l'origine de l'action suspect*
    - *Une analyse approfondi peut être faite*
    - *On laisse l'opération se poursuivre, mais on ne « commitee » pas les résultats jusqu'à avoir la preuve de la non dangerosité des actions effectuées*

Analyse critique

- ++++
  - fournit des moyens d'introspection complète de VM sans modifier ou personnaliser les hyperviseurs,
  - Fournit un mécanisme de détection de code malveillant multi-couche packagés ou chiffrés indépendamment de l'algorithme de chiffrement et du mode de packaging,
  - Pourrait être facilement intégré dans des plateformes cloud commerciales,
  - facile à installer, déployer, modifier et étendre tout en conservant les qualités des précédents solutions traditionnel d'introspection VM.
- - - - -
  - L'implémentation actuelle ne supporte que Maitland Linux VM invité dû à un mauvais soutien de la para virtualisation Xen par les plateformes Windows.

Merci de votre attention