République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'études
en vue de l'obtention du diplôme de Master en Informatique
Spécialité : Administration et Sécurité des Réseux Informatiques

Thème

Détection d'intrusions dans le cloud computing

Présenté par :
Mlle Belkadi Souhila.
Mlle Harfi Hayette.

Proposé et encadré par :
Mme Sellami Lynda.

Devant le jury composé de :

Président : *Mr* Aissani Sofiane.
Examinatrice : *Mme* Benmerbi Samah.

Promotion 2015/2016

Remerciements

Tout d'abord, nous remercions Dieu le tout-puissant qui nous a donné le courage, la force et la volonté pour mener ce travail.

Un grand merci pour nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet.

A nos chères amis qui ont toujours été présents et fidèles.

A notre promotrice ***Mme SELLAMI Lynda*** *pour tout le temps qu'elle nous a consacré, pour ces précieux conseils et pour toute son aide et son appui durant la réalisation.*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement.

Enfin, nous tenons aussi à remercier également tous les membres du jury pour avoir accepté d'évaluer notre travail.

Dédicaces

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce Modeste travail que je dédie :
A Mes très chers parents ;
A Mes frères Nadir et Réda ;
A Mes cousines Radia et Kahina que je considère comme mes sœurs ;
A Mes chères tentes ;
A Mes amis, mes cousins et cousines ;
Harfi Hayette

A l'aide deDIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce Modeste travail que je dédie :
A Mes très chers parents ;
A Mon très cher frère ;
A Mes très chères sœurs Louiza et Kahina ;
A Mes chères tentes ;
A Mes amis, mes cousins et cousines Djamila, Imane ;
A Mon très cher fiancé Rahim qui m'a toujours soutenu ;
A toute ma famille et ma belle famille ;
Belkadi Souhila

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ANN	**A**rtificial **N**ertification **N**etwork
CAPEX	**C**apital **E**xpenditure
CERN	**C**onseil **E**uropéen **R**echerche **N**ucléaire
CPU	**C**entral **P**rocessing **U**nit
DOS	**D**enial **O**f **S**ervice
FTP	**F**ile **T**ransfert **P**rotocol
HTTP	**H** yper **T** text**T**ransfert **P**rotocol
HIDS	**C**isco **C**ertified **I**nternetwork **E**xpert
IAAS	**I**nfrastructure **A**s **A** **S**ervice
IBM	**I**nformation **B**usiness **M**achines
IDS	**I**ntrusion **D**etection **S**ystem
ISN	**I**nitial **S**equence **N**umber
IT	**I**information **T**echnology
JEE	**J**ava **E**ntreprise **E**dition
NIDS	**N**etwork **I**ntrusion **D** etection **S**ystem
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnologie
OPEX	**O**perating **X**xpenses
PAAS	**P**latform **A**s **A** **S**ervice
PDA	**P**ersonal **D**igital **A**ssistant
SAAS	**S**oftware **A**s **AS**ervice
VM	**V**irtuel **M**achine
VPN	**V**irtuel **P**rivate **N**etwork
WWW	**W**orld **W**ide **W**eb

Introduction générale

Vu que la technologie de l'Internet se développe de manière exponentielle depuis sa création, une nouvelle forme de TIC (Technologies de l'information et de la communication) à fait son apparition pour accroitre la productivité des entreprises et répondre à l'évolution des systèmes d'information en termes de ressources et d'espace, il s'agit du Cloud computing.

Le Cloud computing fournit des services extensibles de haute performance et des supports stockage de données évolutives à un nombre important d'utilisateurs. Il élargie le domaine des systèmes informatiques distribués en offrant des services Internet à la demande et par n'importe quel terminal ceci complètent les fonctionnalités de l'informatique distribuée fournies par le Web, les réseaux de grilles et le peer-to-peer. En fait, le Cloud computing offre une infrastructure à grande échelle pour le calcul de haute performance qui s'adapte dynamiquement à l'utilisateur et les besoin de l'application.

Le déploiement, l'accessibilité à l'information et la disponibilité des services expose le cloud à des activités malveillantes et à des attaques. Ce qui rend nécessaire la détection des failles de sécurité quand elles se produisent en utilisant des mécanismes de détection d'intrusion (IDS).

Un Système de détection d'intrusions joue un rôle très important dans la sécurité et la persévérance contre les attaques, c'est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies des intrusions. Afin de détecter les attaques que peut subir un système (réseau informatique), il est nécessaire d'avoir un logiciel spécialisé dont le rôle est de surveiller les données qui transitent sur ce système, et qui est capable de réagir si des activités semblent suspectes.

Dans le cadre de ce mémoire, nous nous intéressons à la détection d'intrusions dans le cloud computing. Pour cela, nous avons organisé notre travail en trois chapitres :

Le premier chapitre intitulé "Généralités sur le Cloud computing", présente les notions

et concepts de base du Cloud computing, ses services, ses types, et ses objectifs.
Le deuxième chapitre intitulé " Les systèmes de détection d'intrusions dans le cloud computing", sera consacré à la description des systèmes de détection d'intrusions(IDSs), ainsi qu'aux IDSs développés dans le cloud computing.

Le troisième chapitre intitulé "Vers un nouvel IDS basé sur le comportement utilisateurs cloud", sera consacrée à la présentation de notre idée qui consiste à développer un IDS basé sur le comportement des utilisateurs.

Enfin en termine par une conclusion générale qui résume les connaissances acquises.

Chapitre 1

Généralités sur les cloud computing

1.1 Introduction

L'informatique a évalué au cours des dernières années, au gré des nouvelles technologies pour répondre à des nouvelles demandes. L'informatique est centralisée avec l'avènement des centres de données. Et surtout, elle se dématérialise et devient "l'informatique dans les nuages", ou Cloud computing. La puissance informatique se virtualité et se consomme de l'endroit et au moment où on en a besoin et devient extensible tout ceci grâce à l'internet. Dans se chapitre nous allons établir un état de cloud computing .

1.2 Historique du Cloud Computing

Bien avant la naissance du terme de Cloud computing, les informaticiens utilisaient déjà des services de Cloud computing comme le webmail2, le stockage de données en ligne (photos, vidéos,...) ou encore le partage d'informations sur les réseaux sociaux. Dans les années 90, un autre concept avait déjà préparé le terrain au Cloud computing. Il s'agit de L'ASP (Application Service Provider) qui permettait au client de louer l'accès à un logiciel installé sur les serveurs distants d'un prestataire, sans installer le logiciel sur ses propres machines. Le Cloud computing ajoute à cette offre la notion d'élasticité avec la possibilité d'ajouter de nouveaux utilisateurs et de nouveaux services d'un simple clic de souris.

Le concept du cloud computing a été initié par Amazon en 2002.Ce dernier avait alors investi dans un parc informatique afin de palier aux surcharges des serveurs dédiés au commerce en ligne constatées durant les fêtes de fin d'année. Mais une fois que les fêtes de fin d'année sont passées les ressources informatiques d'Amazon restait sont peu utilisées.

Amazon a eu l'idée de louer ses capacités informatique le reste de l'année à des clients pour qu'ils stockent les données et qu'ils utilisent les serveurs. Ces services étaient accessibles via Internet et avec une adaptation en temps réel de la capacité de traitement, le tout facturé à la consommation. Cependant, ce n'est qu'en 2006 que Amazon comprit qu'un nouveau mode de consommation de l'informatique et d'Internet faisait son apparition .

Le Cloud computing est enfin apparu avec les différents progrès technologiques réalisés durant ces 50 dernières années, tant que sur le plan matériel, logiciel et conceptuel, qu'aux avancées des mécanismes de sécurité à l'élaboration de réseaux standardisés comme Internet, et à l'expérience dans l'édition et la gestion de logiciels, services, infrastructures et stockage de données [1].

1.3 Définition du Cloud Computing

Le Cloud Computing (l'informatique en nuage en Français) fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (smartphone, PC de bureau, ordinateur portable et tablette). Pour être plus précis, le Cloud Computing permet de partager, chez un fournisseur d'offres Cloud, une infrastructure, une solution applicative ou encore une plateforme à tout utilisateur qui en fait la demande via un simple site internet (aussi appelé portail) en libre-service [2].

Selon la définition du National Institute of Standards and Technology (NIST), le Cloud computing est l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables. Il s'agit donc d'une délocalisation de l'infrastructure informatiqu[3].

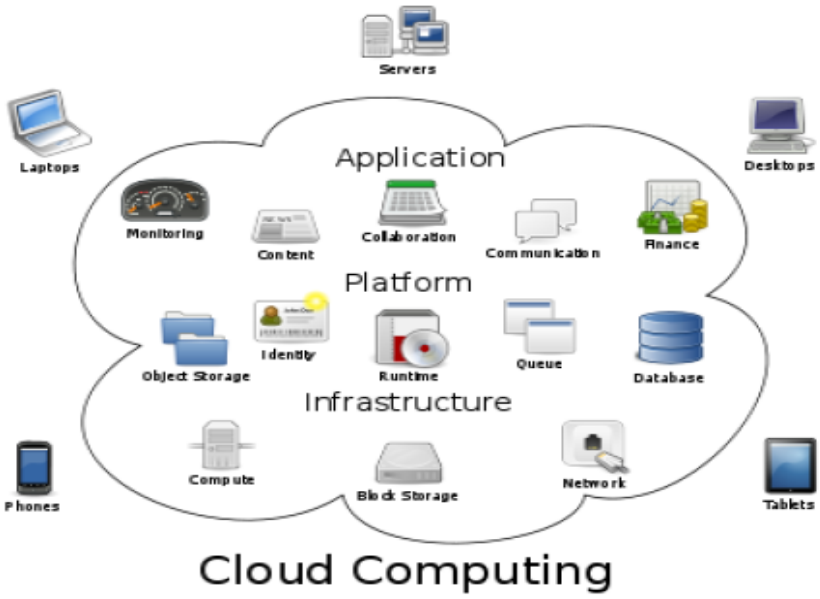


FIG. 1.1 – : exemple d'un cloud computing [4].

1.4 Objectifs du Cloud Computing

Le Cloud Computing est un nouveau modèle informatique qui permet un accès facile et à la demande par le réseau à un ensemble partagé de ressources informatiques configurables qui peuvent être rapidement provisionnées et libérées par un minimum d'effort de gestion ou d'interaction avec le fournisseur de service. L'objectif est de maîtriser les aspects théoriques de ce domaine pour le développement et la mise en œuvre des solutions de services dans un environnement Cloud Computing. Il permet aux entreprises de travailler à distance et de réaliser des économies en matière d'achat de logiciels et de matériels[5].

1.5 Caractéristiques du Cloud Computing

En étudiant divers services disponibles sur le cloud, un ensemble de caractéristiques commun peut être mis en évidence [6] :

1.5.1 Accès instantané

pour utiliser un service Cloud, il suffit généralement de se créer un compte qui sera directement utilisable une fois le mode de paiement est validé. Le service Cloud est accessible lorsque l'utilisateur le souhaite.

1.5.2 Self service

Les capacités de calcul et les ressources sont misent a disposition des clients ,au besoin sans la nécessite de l'intervention du prestataire du services.

1.5.3 Élasticité

Dans le Cloud l'utilisateur(client)choisit les ressources à consommer ainsi que la quantité. Celle-ci peut varier à tout moment en fonction des besoins.

1.5.4 Paiement à la carte

Les clients du Cloud ont une facture qui ne regroupe le listing des services consommés. Tout ce qui touche à la maintenance, au personnel ou aux infrastructures matérielles n'apparaît pas dans la facture. la facturation se fait généralement à court terme, par exemple, mensuellement.

1.5.5 Service mesuré

possibilité de surveiller, contrôler et mesurer l'utilisation des ressources L'argument en faveur de la valeur, de la flexibilité et de la qualité apportée par ces fonctionnalités est si convaincant que la transition vers le cloud computing va définir le paysage technologique des administrations au cours de la prochaine décennie. Toutefois, la transition vers le cloud computing présente des difficultés pour certaines administrations. Bon nombre d'entre elles sont découragées par la complexité des questions liées à la sécurité des données, aux rôles et aux modèles commerciaux.

1.6 Les différents services du Cloud Computing

Le cloud computing offre trois types de services qui sont : IaaS, PaaS et SaaS [7] :

1.6.1 SaaS (Software as Service)

Le Software as a Service (SaaS) est accessible aux entreprises et il est facturé au nombre d'utilisateurs. L'entreprise loue les applications du fournisseur de services, il n'est Plus besoin d'acheter un logiciel. Ces applications sont accessibles via différentes interfaces, navigateurs Web, clients légers, etc.

1.6.2 PaaS (Platform as a Service)

La Platform as a Service (PaaS) est un service Cloud qui permet à l'entreprise de déployer, d'exécuter et de développer ses propres applications sur des plateformes partagées. L'entreprise loue un environnement middleware avec une infrastructure masquée.

1.6.3 IaaS (Infrastructure as a Service)

L'Infrastructure as a Service (IaaS) est la mise à disposition par l'internet d'infrastructures facilement modifiables et hautement disponible. L'entreprise loue ainsi des capacités de traitement, de stockage et autres infrastructures qu'elle peut structurer et gérer de façon autonome côté logiciel dès le système d'exploitation.

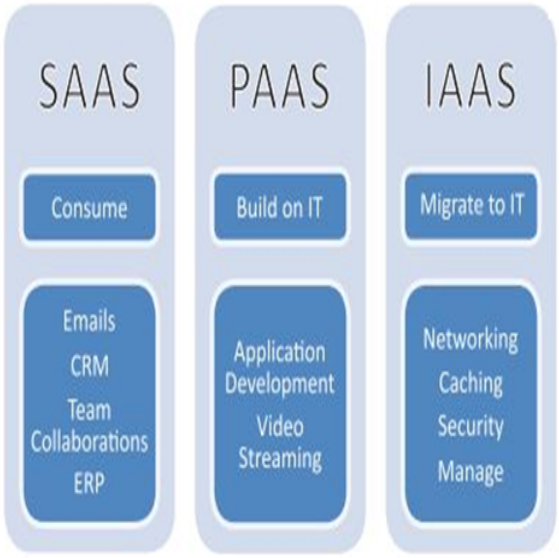


FIG. 1.2 – : Les services du cloud computing [8].

Les services du cloud computing offrent plusieurs avantages aux clients en économisant du temps et de l'argent ,néanmoins des inconvénients sont soulevés qui limite leur utilisations par les clients. Les avantages et inconvénients des services du cloud sont présentés dans le tableau suivant[9] :

- **Avantages et Inconvénients des services**

Types.	Avantages.	Inconvénients .
Saas.	– Pas d'installation . – Plus de licence . – Migration .	– Logiciel limité. – Besoin de sécurité . – Dépendance des prestataire. – Services dédiés.
Paas.	– Ne nécessite pas d'infrastructure. – Pas d'installation . – Environnement hétérogène .	– Limitation des langages . – Pas de personnalisation dans la configuration des machines virtuelles.
Iaas.	– Administration . – Personnalisation . – Flexibilité d'utilisation .	– Besoin de sécurité. – Besoin d'un administrateur Système .

TAB. 1.1 – :Avantages et Inconvénients des services de cloud computing [9].

1.7 Les types de Cloud Computing

Pour le grand public, le cloud computing fait référence globalement à Internet, pour les entreprises il n 'est pas le cas. Pour cela différent modèles de déploiement du cloud existent [10] :

1.7.1 Cloud privé

Les services et ressources cloud sont mise a disposition à une organisation (client/entreprise) unique. Elle peut être gérée par l'organisation elle-même (Cloud Privé interne) ou par un tiers (Cloud Privé externe). Dans ce dernier cas, l'infrastructure est entièrement dédiée à l'entreprise et accessible via réseaux sécurisés de type VPN (Virtual Private Network).

1.7.2 Cloud public

Les services et ressources sont accessible par internet et gérer par un prestataire externe(fournisseur). Ces ressources et servicessont partagées par plusieurs clients et utilisé a la demande. Ces services peuvent être gratuits ou payants.

1.7.3 Cloud hybride

Il s'agit de la conjonction de deux ou plusieurs Cloud (public et privé) amenés à coopérer, à communiquer et à partager entre eux applications et données.

1.7.4 Cloud communautaire

L'infrastructure de Cloud communautaire est partagée par plusieurs organisations qui ont des intérêts communs (par exemple les exigences de sécurité, de conformité ...). Comme le Cloud Privé, il peut être géré par les organisations elles mêmes ou par un tiers.

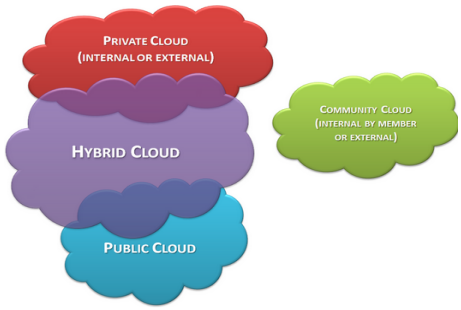


Fig. 1.3 – : Les type de cloud computing[11].

1.8 Avantage du Cloud Computing

Il existe plusieurs avantages du cloud computing [12] :

- **Un démarrage rapide**
  Le Cloud computing permet de tester le plan business rapidement, à coûts réduits et avec facilité.
- **L'agilité pour l'entreprise**
  Résolution des problèmes de gestion informatique simplement sans avoir à s'engager à long terme.
- **Un développement plus rapide des produits**
  Réduisons le temps de recherche pour les développeurs sur le paramétrage des applications.
- **Pas de dépenses de capital**
  Plus besoin des locaux pour élargir vos infrastructures informatiques.

1.9 Limites du Cloud Computing

Le cloud computing présente les inconvénients (limites) suivante[12] :

- **La bande passante**
  Besoin d'une bande passante gigantesque, et les coûts seraient tellement importants qu'il est plus avantageux d'acheter le stockage nous-mêmes plutôt que de le loué.
- **Les performances des applications peuvent être amoindries**
  Un Cloud public n'améliorera définitivement pas les performances des applications.
- **La fiabilité du Cloud**
  Un grand risque lorsqu'on met une application qui donne des avantages compétitifs ou qui contient des informations clients dans le Cloud.
- **Taille de l'entreprise**
  Si votre entreprise est grande alors vos ressources sont grandes, ce qui inclut une grande consommation du Cloud. vous trouverez peut être plus d'intérêt à mettre au point votre propre Cloud plutôt que d'en utiliser un externalisé.

1.10 Les principaux fournisseurs de services cloud computing

Il existe plusieur fourniseurs de services de cloud

1.10.1 Amazon web services

Il s'agit d'une demi-douzaine de services, y compris l'Elastic cloud computing, pour la capacité de calcul et le service de stockage simple, pour la capacité de stockage a la demande.

Amazon est un véritable innovateur en matière de calcul sur le web, offrant du paiement à l'usage sur des services virtuels, et de l'espace de stockage. outre ces offres de base, Amazon offre simple DB(un service web de base de données), le cloudFront (un service web pour la livraison de contenu) net le simple queue service (un service hébergé pour le traitement des messages entre ordinateurs).

1.10.2 Google APPS

Google Apps est un ensemble d'outils de productivité de bureau, création de sites web. App Engine, est une plate-forme qui permet aux développeurs de bâtir et d'héberger des applications sur l'infrastructure de Google.

Le principal objet de Google est l'exploration du web et de fournir de la publicité liée aux résultats de la recherche sur le web, l'incursion de Google dans le logiciel pour les entreprises et accélèrer le mouvement de l'industrie depuis les package logiciels vers les services hébergés sur le web.

1.10.3 Microsoft

Windows Azure, une offre de Windows en tant que plate-forme comprenant le système d'exploitation et les services pour les développeurs qui peuvent être utilisées pour construire et améliorer des applications web hébergées.

1.11 Architecture du cloud computing

1.11.1 Architecture globale du cloud computing

En faisant abstraction de détails de plus haut niveau, l'architecture globale du cloud computing comporte essentiellement[13] :

- **Des clients**
  personne, entreprise,groupe qui accèdent aux différent services offerts par le cloud.
- **Des services**
  Différent niveaux de services et données sont gérer par des fournisseurs afin de les offrir à la demande des clients du cloud.
- **Un réseau**
  Intermédiaire entre le client et le fournisseur,qui permet de transiter les services (chemin que les services entreprend)c'est le reseau Internet.
- **Des fournisseurs**
  Ce sont des entités chez lesquelles on alloue les services cloud.

- **Des serveurs**
  Où sont stocker les services cloud il sont éparpiés partout dans le monde qui constituent le cœur hardware de cloud computing. Les entités citées ci-dessus sont connectées selon le modèle de déploiement du cloud privé et public.

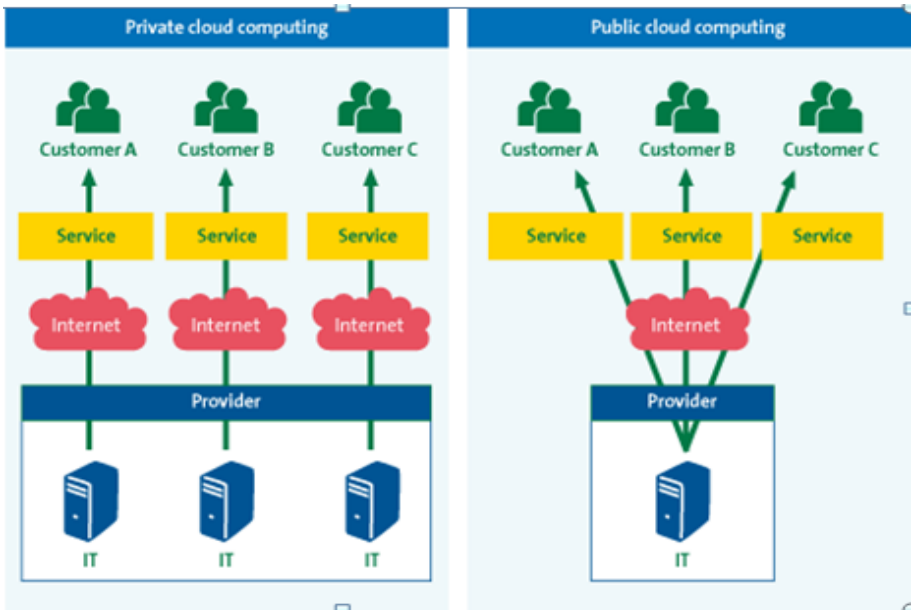


FIG. 1.4 – : Architecture globale et les composants de base du cloud computing [13].

1.11.2 Architecture de référence du cloud computing selon NIST

L'architecteur de référence définie pas NIST est beaucoup plus complète, elle regroupe tous les acteurs du cloud computing à savoir[14] :

- **Cloud consumer**
  Une personne ou une organisation qui entretient une relation d'affaires et utilise les service des fournisseurs de cloud .
- **Cloud provider**
  Une personne, une organisation ou une entité responsable de fournir des services à des parties intéressées.
- **Cloud auditor**
  C'est partie qui peut procéder à une évaluation indépendante des services fournis par le cloud computing, des opérations des système d'informations, de la vices fournis par le cloud computing, de la performance et de la sécurité de l'implémentation du cloud.
- **Cloud broker**
  C'est l'entité qui gére l'utilisation, la performance et la prestation de services de cloud computing, et qui négocie les relation entre les fournisseurs de services cloud et les client du cloud.
- **cloud carrier**
  C'est l'entité intermédiaire qui fournit la connectivité et le transport des services du fournisseur de cloud au client du cloud. Il existe d'autres architecteur de référence du cloud computing.

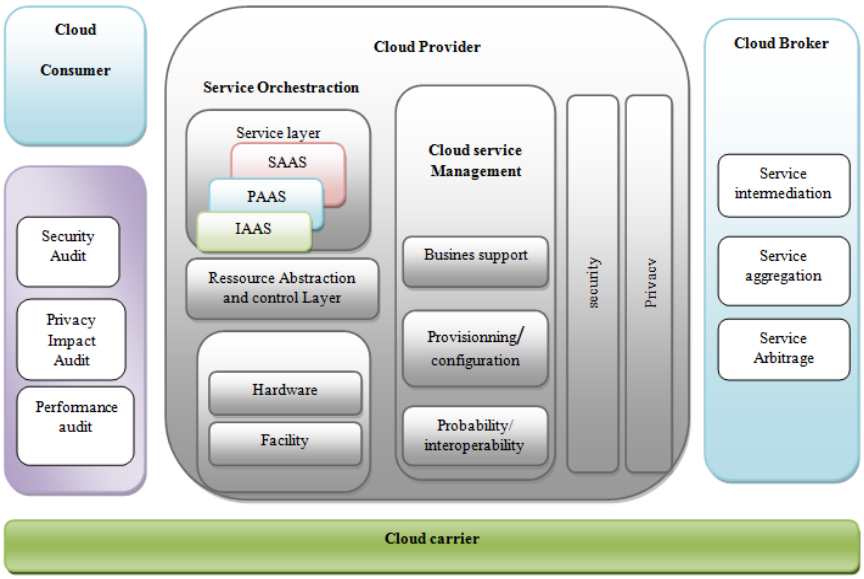


FIG. 1.5 – : l'architecteur de référence du cloud computing [15].

1.12 Conclusion

Au cours de cette première partie, nous avons fourni une base théorique sur le Cloud Computing, en présentant ses types, ses services (IaaS, PaaS, SaaS), ses avantages et inconvénients, afin d'appliquer ses concepts à notre contexte.

L'ouverture du Cloud et sa facilité d'utilisation, sa flexibilité expose les réseaux informatique aux attaques. Donc il est nécessaire de sécurisé les services et ressources cloud en utilisant des mécanismes de sécurité tel que les systèmes de détection d'intrusion(IDS) se qu'il sera l'intérêt du prochain chapitre.

Chapitre 2

Les systèmes de détection d'intrusions dans le Cloud computing

2.1 Introduction

Le Cloud computing, comme tout système informatique réparti, est continuellement exposé à de nombreuses menaces. Ainsi, la sécurité du Cloud est aujourd'hui une préoccupation très importante des fournisseurs et des utilisateurs du cloud. Pour se prémunir des attaques qui se produisent dés l'utilisation des réseaux et des systèmes d'informations, des mécanismes de sécurité sont déployés afin de protéger les données hébergée et partagées dans les infrastructures virtuelles. Les pare-feu sont responsables du filtrage de paquets afin de contrôler l'accès réseau. Néanmoins, le pare-feu ne procure pas une sécurité complète contre les attaques, car il s'intéresse à l'attaque elle-même sans se soucié des attaquants. Les systèmes de détection d'intrusions viennent pour compléter le travail du pare-feu, en s'intéressant au comportement de l'attaquant.

Les systèmes de détection d'intrusions (IDS) détectent les attaques survenant sur le réseau et les systèmes d'informations. L'objectif des administrateurs de sécurité est de prévenir et de détecter les attaques sans perturber le bon fonctionnement du Cloud.

Nous consacrons ce deuxième chapitre à la sécurité, aux mécanismes de sécurité, ainsi qu'aux systèmes de détection d'intrusions.

2.2 Sécurité et mécanismes de sécurité

2.2.1 Définition de la sécurité

La sécurité informatique est l'utilisation de la technologie, des politiques et de l'éducation des personnes pour assurer la confidentialité, l'intégrité et l'accessibilité des données durant leur stockage, leur traitement et leur transmission. La protection des données doit dépendre du système à protéger [15].

2.2.2 Objectifsde la sécurité

La sécurité d'un système informatique a pour mission la protection des informations et des ressources contre toute dévaluation , modification ou destruction.

Les objectifs pris en confédération dans la sécurité sont les suivant [15] :

1. **La confidentialité**
   Permet de garder les informations secrètes de tous sauf des personnes autorisées à les consulter.
2. **L'authentification**
   Permet la confirmation de l'identité d'une entité avant de lui donner l'accès à une ressource.
3. **L'intégrité des informations**
   Permet d'assurer que les informations n'ont pas été altérées par des personnes qui ne sont pas autorisées.
4. **La disponibilité**
   Permet de garantir l'accès à un service ou une donnée.
5. **Non répudiation** Permet d'empêcher le démenti d'engagement ou de l'action précédente.

2.2.3 Mécanismes de défense

Il existe plusieurs mécanismes ou technologies de défense pour faire face aux attaques, nous allons dans ce qui suit citer les principales technologies[16] :

1. **Authentification**
   Permet de vérifier la véracité des utilisateurs, du réseau et des documents .
2. **Cryptographie**
   Permet la confidentialité des informations et la signature électronique .
3. **Contrôle d'accès**
   Permet de vérifie les droits d'accès d'un acteur aux données .

4. **Antivirus**
   C'est un logiciel censé de protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. L'antivirus ne protège pas contre un intrus qui emploie un logiciel légitime, ni contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire .
5. **Le pare-feu**
   C'est un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui traversent le réseau. Il a pour fonction de faire respecter la politique de sécurité du réseau .
6. **Journalisation (logs)**
   Permet l'enregistrement des activités de chaque acteur et de constater que des attaques ont eu lieu, de les analyser et defaire en sorte qu'elles ne se reproduisent pas plus tard .
7. **Analyse des vulnérabilités(Security audit)**
   Permet l'identification des points de vulnérabilité du système qui ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu .
8. **Détection d'intrusion**
   Permet de détection des comportements anormaux d'un utilisateur ou des attaques connues .

2.3 Les systèmes de détection d'intrusion (IDS)

Le concept de système de détection d'intrusions a été introduit en 1980 par James Anderson, mais le sujet n'a pas eu beaucoup de succès. Il a fallu attendre la publication d'un modèle de détection d'intrusions par Denning [17] en 1987 pour marquer réellement le départ du domaine. En 1988, il existait au moins trois prototypes(IDS). La recherche dans le domaine s'est ensuite développée, le nombre de prototypes s'est énormément accru. Le gouvernement des États-Unis a investi des millions de dollars dans ce type de recherches dans le but d'accroître la sécurité de ses machines .

2.3.1 Intrusion

Nous appellerons intrusion toute utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'acquisition de privilèges de façon illégitime. L'intrus est généralement vu comme une personne étrangère au système informatique qui a réussi à en prendre le contrôle, mais les statistiques montrent que les utilisations abusives proviennent le plus fréquemment de personnes internes ayant déjà un accès au système [17].

2.3.2 Détection d'intrusion

Les techniques de détection d'intrusion tentent de faire la différence entre une utilisation normale du système et une tentative d'intrusion et donnent l'alerte. Typiquement, les données d'audit du système sont parcourues à la recherche de signatures connues d'intrusions ou de comportements anormaux. La détection peut être faite en temps réel, dans ce cas, le programme (IDS) peut donner l'alerte, auquel le personnel qualifié pourra tenter de remédier à l'intrusion, en coupant la connexion ou en remontant la piste[17] .

2.3.3 Systèmes de détection d'intrusion

Les IDSs sont des outils permettant de détecter les attaques intrusions des systèmes sur le quel ils sont placés .

Il existe deux types d'IDS : les IDS à base de nœuds et les IDS réseaux [18] :

- **Les IDSs à base de nœud (Host Intrusion Detection System-HIDS** analysent le fonctionnement et l'état des machines sur lesquels ils sont installés afin de détecter les attaques en se basant sur des démons. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées.

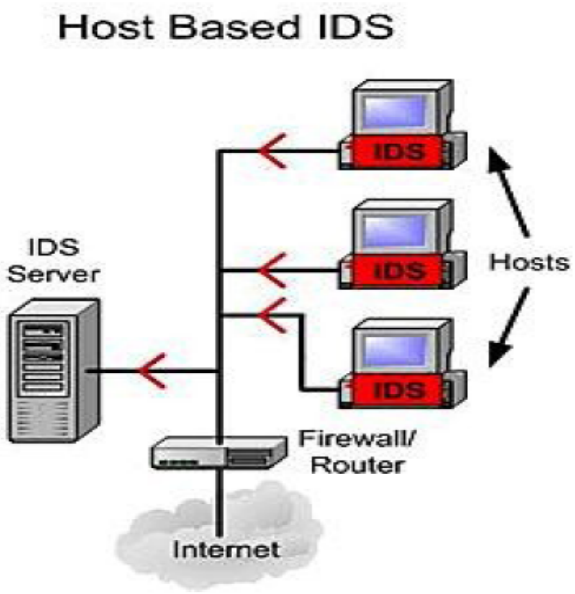


FIG. 2.1 – : Les IDS à base de nœud [18].

- **Les IDSs réseaux (Network Intrusion Detection System-NIDS)**

  analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode "promiscuous"). Ensuite, les paquets sont décortiqués puis analysés. En cas, de détection d'intrusion, des alertes peuvent être envoyées.

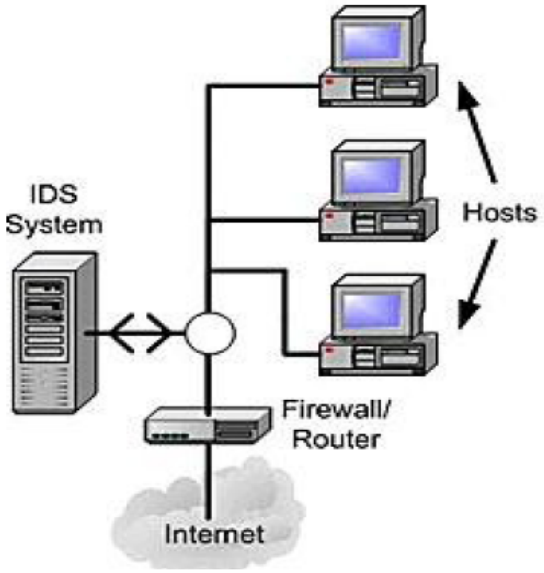


FIG. 2.2 – : Les IDSs réseaux [18].

Les deux types d'IDS possèdent des avantages ainsi que des inconvénients, ces derniers sont illustrer dans le tableau suivant :

Types.	Avantages.	Inconvénients .
IDSs HIDS.	– Permet de constater l'impact d'une attaque et pout donc mieux réagir. – Découverte facile d'un Cheval de Troie puisque les informations sont très étendues. – Observation des activités sur l'hôte avec précision. .	– Ils ont moins de facilité à détecter les scans. – Ils sont plus vulnérables aux attaques de type Dos. – L'analyse des traces d'audit du système est très contraignante en raison de la taille de ces dernières. – Consommation de ressources CPU.
IDSs NIDS.	– Les capteurs peuvent être bien sécurisés puisqu'ils se "contentent" d'observer le trafic . – Détection facile des scans grâce aux signatures . – Peut filtrer le trafic .	– La probabilité de faux négatifs (attaques non détectées comme telles) est élevée et il est difficile de contrôler le réseau entier. – Ils doivent principalement fonctionner de manière cryptée d'où une complication de l'analyse des paquets. – A l'opposé des HIDS, ils ne voient pas les impacts d'une attaque .

TAB. 2.1 – : Les avantages et inconvénients des deux types d'IDSs [18].

2.4 Les critères de classifications des IDSs

Les IDSs peuvent être classifiés en cinq (5) critères de classification qui ont été introduits par Debar et al. dans [19], la figure 2.3 résume les critères de classification des IDSs.

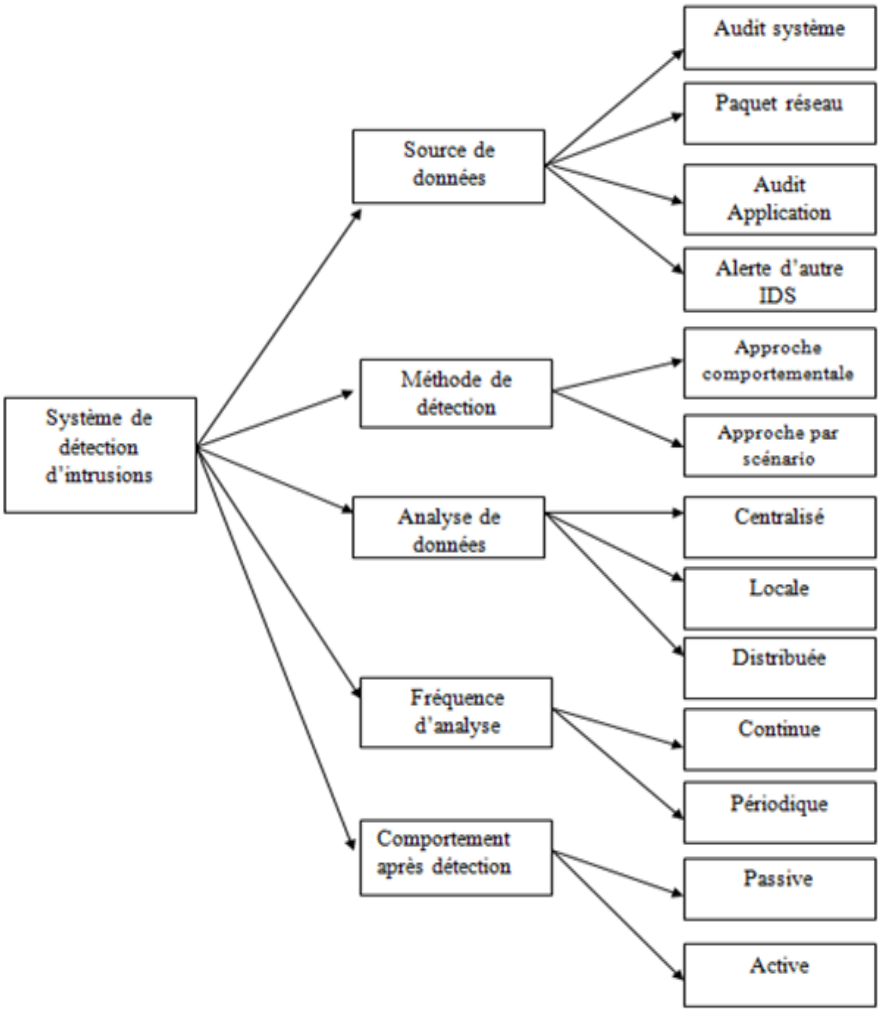


FIG. 2.3 – : Les critères de classification des IDSs [20].

2.4.1 Sources de données :

Les sources des données constituent les informations qu'elles fournissent pour analyser le système pour d'éventuelles intrusions. Il existe quatre sources de données qui sont : l'audit système, le trafic réseau, l'audit applicatif et les alertes d'autres IDSs [20] :

- **Audit système**
  Permet d'enregistrer les actions effectuées sur le système en exploitant l'outil d'administration système. Cette source de données est très pertinente, du fait que la totalité des attaques provoquent une interaction avec le système. Les données d'audit système sont le seul moyen pour recueillir des informations sur les activités des utilisateurs d'une machine donnée.
- **Paquet réseau**
  représente les paquets récupérés du réseau. La plupart des accès aux ordinateurs se font via les réseaux informatiques, alors que la capture des paquets avant qu'ils entrent au serveur est le moyen le plus efficace pour les contrôler. L'analyse des paquets représente le moyen le plus efficace pour détecter les attaques de type déni de service (DOS).
- **Audit application**
  C'est une source d'information de haut niveau, qui représente les services Web tel que le FTP (File Transfert Protocol) et le HTTP (Hyper Text Transfert Protocol). Avec la grande augmentation de l'utilisation des serveurs d'application, les fichiers logs des applications sont devenus une source d'information pour les systèmes de détection d'intrusions.
- **Alerte d'autre IDSs**
  C'est une source d'information basée IDS. Ce sont les alertes remontées par des analyseurs provenant d'un IDS. Chaque alerte synthétise déjà un ou plusieurs événements intéressants du point de vue de la sécurité. La corrélation de ces alertes conduit parfois à la détection d'une intrusion complexe de plus haut niveau.

2.4.2 Méthode de détection

Il existe deux méthodes de détection, la première consiste à utiliser des connaissances accumulées sur les attaques puis les exploiter afin de prouver l'existence d'autres attaques. Le second consiste à créer un modèle basé sur le comportement habituel du système et surveiller toute déviation de ce comportement. La première méthode est appelée approche par scénario et la seconde est l'approche comportementale [20] :

- **L'approche par scénario**

  Elle se base sur des attaques connues préalablement. Cela nécessite une connaissance à priori des attaques à détecter. Elle se base sur les connaissances accumulées sur les attaques spécifiques et les vulnérabilités du système. Le système de détection

d'intrusion contient les informations et cherche toute tentative de les exploiter. Si l'IDS détecte une tentative, une alarme est déclenchée. Par conséquent, la précision des systèmes de détection d'intrusions basée sur l'approche par scénario est bonne. Cependant, cette précision dépend toujours de la mise à jour des connaissances sur les attaques qui doit être régulière.

- **L'approche comportementale**

  Les techniques de détection d'intrusion basée sur l'approche comportementale supposent que l'intrusion peut être détectée par l'observation de la déviation par rapport au comportement normal ou prévu du système ou des utilisateurs. Au début le modèle du comportement normal est extrait à partir des informations de référence recueillies par divers moyens, puis le système de détection d'intrusions compare ce modèle avec l'activité actuelle, si une déviation est détectée, une alerte est déclenchée. D'une manière générale, on peut dire que cette approche considère tout comportement non enregistré précédemment, comme intrusion. Par conséquent, cette approche peut être complète, mais la précision reste son plus grand souci.

2.4.3 Analyse de données

Les données peuvent être analysée en centralisé, en locale ou bien distribué [20] :

1. **Analyse centralisé**
   Consiste à centraliser les alertes et le contrôle au sein d'une seule machine (administrateur réseau).
2. **Analyse locale**
   L'analyse se fait localement, c'est-à-dire sur chaque hôte séparément des autres. Donc, on lance l'analyse sur un hôte seulement, ce qui fait perdre du temps. De plus, il n'y a pas de surveillance entière du réseau en même temps.
3. **Analyse distribué**
   L'analyse se fait de manière distribuée sur le réseau. L'analyse est lancée sur toutes les machines au même temps. Ce qui fait gagner du temps dans l'analyse et permet la surveillance entière du réseau et évite donc d'avoir des attaques au moment de l'analyse.

2.4.4 Fréquence d'analyse

Il existe deux façons dont les systèmes de détection d'intrusions effectuent leurs analyses qui sont : analyse continue et analyse périodique [20] :

- **La surveillance continue**
  une analyse continue et en temps réel par l'acquisition d'informations sur les mesures prises sur l'environnement et analyse ce cliché a la recherche des logiciels vulnérables, des erreurs de configuration, etc.

- **L'analyse périodique**
  Cette analyse revient à surveiller et à analyser le système de manière périodique, c'est-à-dire, à chaque période de temps qui est choisie par l'administrateur (observation périodique dans le temps).

2.4.5 Comportement après détection

Le comportement de l'IDS après une détection d'intrusion peut être passive, active ou bien les deux au même temps [20] :

- **Action passive**
  L'IDS informe directement l'utilisateur ou le manager qu'une intrusion est détectée en déclenchant une alerte.
- **Action active**
  L'IDS en cas d'une attaque l'IDS non seulement il informe le manager ou l'utilisateur mais aussi il réagi contre cette attaque en coupant le courant par exemple.
- **Action passive et active**
  L'IDS peut informer l'utilisateur ou bien le manager qu'une intrusion est détectée et il réagi directement.

2.4.6 Les limites actuelles de la détection d'intrusions

Il existe des limites spécifiques pour la détection d'abus ainsi que des limites pour la détection d'anomalies qui sont les suivant [21] :

2.4.6.1 Limites spécifiques à la détection d'abus

Les principaux défis actuels de cette technique sont les suivants :

- **Base de signature d'attaques délicate à construire.**
- **Seules les attaques contenues dans la base sont détectées.**
- **Nécessite la mise à jour de la base de signature d'attaques comme les Antivirus.**
- **Incapables de détecter certains types d'attaque.**
- **Ils sont eux-mêmes vulnérables aux attaques.**
- **Problème des faux négatifs qui sont le fait que les nouvelles attaques passent l'IDS sans être détectées.**

2.4.6.2 Limites spécifiques à la détection d'anomalie

Cette technique comporte elle-aussi de nombreux problèmes complexes à résoudre ; voici les plus couramment évoqués :

- **Choix délicat des mesures à retenir pour un système cible donné.**

- **Pour un utilisateur au comportement erratique, toute activité est " normale ".**
- **En cas de profonde modification de l'environnement du système cible, déclenchement d'un flot ininterrompu d'alarmes (faux positifs).**
- **Utilisateur pouvant changer lentement de comportement dans le but d'habituer le système à un comportement intrusif (faux négatifs).**

2.5 Les IDS dans le Cloud computing :

Au cours des dernières années, plusieurs travaux de recherche ont été faits dans le but de proposer des solutions d'IDS dans l'environnement du cloud computing. Nous allons citer dans cette partie les travaux les plus connus [22] :

1. **Architecture IDS de l'environnement cloud computing**

   Une interaction entre les services est offerte dans [23], l'IDS fournit des services et des services de stockage pris en charge par chaque nœud de l'environnement Cloud. Le système de service IDS est composé en deux éléments : l'analyseur et le système d'alerte. Les données provenant de diverses ressources sont capturé par le vérificateur (auditeur) de l'événement. Le système de service IDS reçoit des données dl'auditeur de l'événement. Ces données sont utilisées pour détecter les intrusions en utilisant une technique basée sur la basée du comportement. Dans cette approche, le réseau neuronal artificiel (ANN) est utilisé pour détecter les attaques inconnues. Le système d'alerte informe les autres nœuds lorsqu'une attaque ou intrusion est détectée.

2. **Approche basé sur les statistiques et la théorie des probabilités**

   L'approche CP (Co-variante Probability) est basée sur les statistiques et la théorie des probabilités [24]. Les statistiques se basent sur des ensembles mutuellement exclusifs et ils sont utiliser pour décomposer cet ensemble. La détection d'intrusion est construite en utilisant les sous-ensembles générés à partir des espaces de l'échantillon considéré .

3. **IDS associe à une machine virtuelle (VM)**

   Cette approche se compose de deux éléments [25] : Unité de gestion IDS et capteur IDS. Unité de gestion IDS se compose d'un rassembleur d'événement, d'une base de données d'événements, du composant d'analyse et d'un contrôleur à distance. Le capteur IDS identifie les comportements malveillants. Le rassembleur d'événements collecte les comportements et les stocke dans la base de données d'événements. Le composant d'analyse accède à la base de données d'événements et d'analyser les événements qui sont configurés par les utilisateurs. Le contrôleur d'IDS gère l'IDS-VM (machines virtuelles) et peut communiquer avec l'IDS-VM et le capteur IDS.

4. **Approche basé sur agent mobile**

Pour détecter l'intrusion dans des applications Cloud Dastjerdi et al. [26] ont proposé une méthode évolutive, flexible et rentable en utilisant les agents mobiles. Cette méthode est utilisée pour protéger les machines virtuelles qui se trouvent à l'extérieur de l'organisation. L'ensemble des attaques sont collectées par l'agent mobile. Une analyse plus poussée et une vérification sont appliquées sur cette preuve.

2.6 Les Caractéristiques et les limites des différentes approches proposées :

Dans le tableau suivant, une comparaison des différentes approches, qui ont été proposé, est présentée [22] :

IDS .	Inconvénients .
Architecture IDS de l'environnement cloud computing	– Nécessite plus de temps de formation et d'exemples pour la précision de la détection. – Il ne peut pas détecter toutes intrusions internes en cours d'exécution sur les machines virtuelles.
Approche basé sur les statistiques et la théorie des probabilités	– Utilisé pour détecter tous les types d'attaques. – Limitation du temps de calcul.
IDS associe à une machine virtuelle	– La VM peut être attaqué. – Méthode très complexe. – Ne peut pas détecter les attaques sur les machines virtuelles.
Approche basé sur agent mobile	– Produit la charge du réseau avec une augmentation de VM attaché. – Fournit un IDS pour l'application cloud indépendamment de leur emplacement.

TAB. 2.2 – : Les limites des différentes approches proposées [22].

2.7 Conclusion

De manière générale, l'efficacité d'un système de détection d'intrusion dépend de sa "configurabilité" (possibilité de définir et d'ajouter de nouvelles spécifications d'attaque), de sa robustesse (résistance aux défaillances) et de la faible quantité de faux positifs

(fausses alertes) et de faux négatifs (attaques non détectées) qu'il génère. Dans ce chapitre, nous avons présenté la sécurité, ses objectifs et les mécanismes de défense, les systèmes de détection d'intrusions ainsi que quelques travaux de recherche qui ont été proposées par les chercheurs.

La détection d'intrusion est devenue une industrie mature et une technologie éprouvée. Néanmoins, quelques voies restent cependant relativement inexplorées : les mécanismes de réponse aux attaques, les architectures pour les systèmes de détection d'intrusions distribués. les standards d'interopérabilité entre différents systèmes de détection d'intrusion, et la recherche de nouveaux paradigmes pour effectuer la détection d'intrusion.

Dans le chapitre suivant, nous allons proposer notre idée qui est le développement d'un IDS à base de comportement des clients du cloud.

Chapitre 3

Vers un nouvel IDS basé sur le comportement utilisateurs cloud

3.1 Introduction

Dans ce chapitre, nous allons proposer un IDS à base du comportements des clients pour assurer la sécurité dans un cloud computing. Nous allons présenté, dans un premier temps, l'environnement de travail et passer ensuite aux étapes du développement de notre application.

3.2 Problématique et objectifs

Face à des problèmes : de grand volume de trafic réseau, de distribution des données très déséquilibrée, de difficulté de prendre une décision sur un comportement normale ou anormale, et de l'exigence d'une adaptation permanente pour des environnements évolutionnaire, on est ainsi conduit à utiliser des techniques pour créer les noyaux des modèles de détection d'intrusion.
Notre objectif est de développer un IDS basé sur le comportement des clients. Notre IDS sera de détecter des intrusions qui circulent dans le réseau dans le cloud computing.

3.3 Description de l'application

Notre application a pour but le développement d'un IDS basé sur le comportement des clients (utilisateurs) cloud, nous allons essayer de placer l'IDS dans chaque nœud connecté au Cloud computing, nous avons choisi l'IDS à base de comportement ce qui va nous permettre de poursuivre le comportement des clients durant leurs connexion au cloud, cette période va nous donner une idée générale sur le comportement du client (utilisateur) : les

services consulté ,les logiciels télécharger, Les ressources disponibles, etc.

Notre IDS va se basée sur la comparaison du comportement du client lors de l'analyse et son comportement habituelle (profil normale), si le résultat obtenu confirme qu'il n'y a pas de changement de comportement alors il n'y a pas d'intrusion. Dans le cas d'un changement de comportement un message est afficher pour informer qu'une intrusion est détectée.

3.3.1 Les étapes de la détection d'intrusion

Afin de développer notre IDS, nous avons besoin de données à analyser qui proviennent de l'audit système des utilisateurs, ces données sont analysées en distribuée. L'approche de détection entretenue dans notre IDS est l'approche comportementale avec une fréquence d'utilisation continue qui nous permet de surveiller les activités des clients en permanence. En cas d'attaques détectées, un comportement vis-à-vis l'attaque est appliqué.

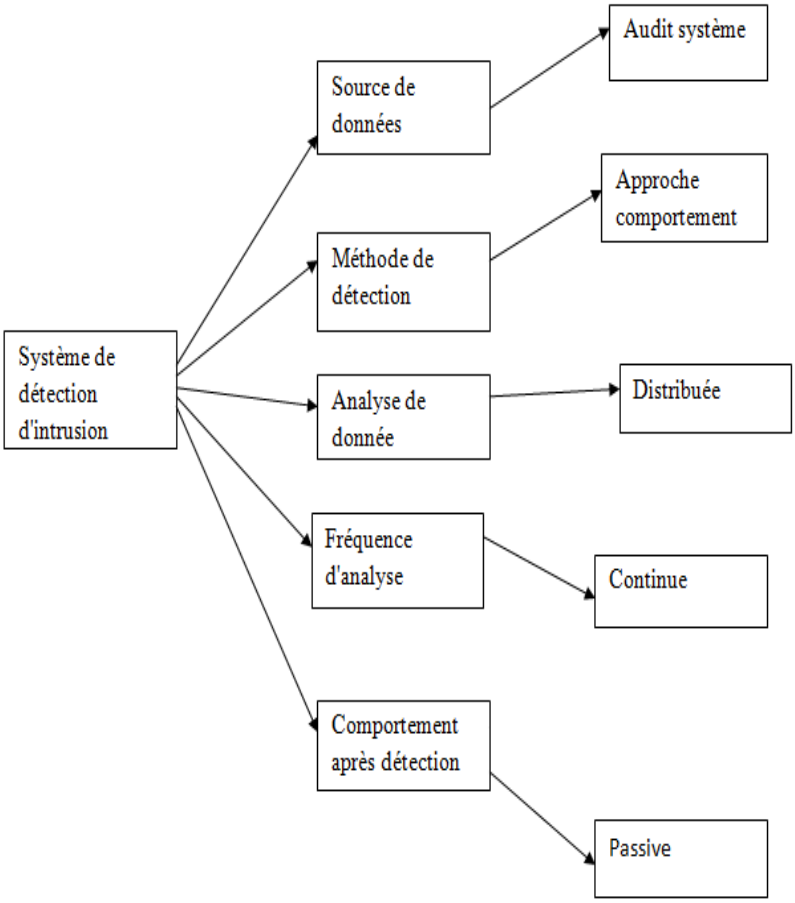


FIG. 3.1 – : La Classification de l'IDS Choisi.

3.3.2 Le schéma de sécurité

Nous rappelons que notre objectif est de détecter les intrusions qui peuvent se produire dans le cloud computing. L'idée principale est de comparer entre un profil normal prédéfini et le comportement réel de l'utilisateur. Pour ce faire, nous avons décomposé notre schéma de sécurité comme suit (voir Fig.3.2).

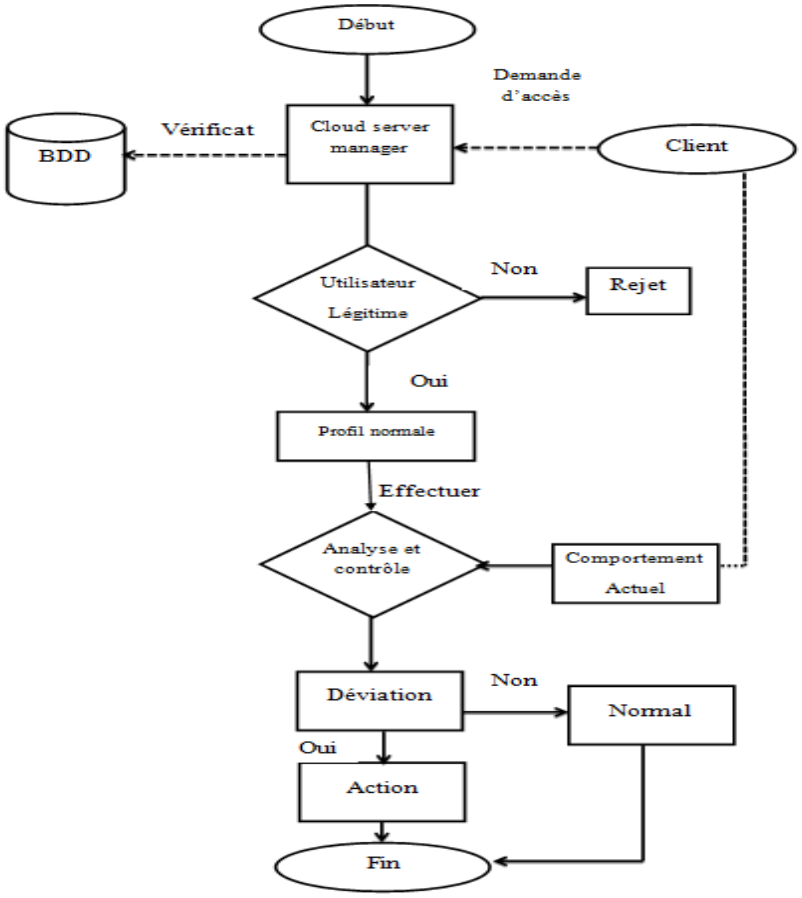


FIG. 3.2 – : Diagramme du schéma de sécurité de notre IDS.

- **Lorsqu'un client veut accéder à l'un des services du cloud computing, il demande d'accès au serveur provider manager. Une vérification de l'authentification du client est effectuée, par le fournisseur des services cloud, pour garantir l'identité et la légitimité du demandeur (client)**

- **Après que authentification du client est assurée, le profil normale du client est créé à base de l'authentification (les entrées reçue par le client). Nous notons que le profil du client est déterminé en fonction du login et le mot de passe fourni par l'utilisateur lors de l'accès au réseau. Le profil de l'utilisateur peut être considéré comme une combinaison des privilèges et restrictions. Un privilège est une action autorisée tandis qu'une restriction est l'interdiction de l'action.**

- **Le comportement du client est construit à partir du flux de données. Dans cette phase, deux tâches sont principalement effectuées. Tout d'abord, nous recueillir des informations sur le comportement de l'utilisateur afin de construire le comportement actuel du client, puis on compare le comportement actuel du client au profil normal.**

- **Lorsqu'une anomalie est est détectée, une alarme est envoyée au fournisseur et au client dans le but de résoudre le problème détecté.**

3.4 Réalisation de l'application

Dans ce qui suit, une réalisation de l'IDS proposé est présenté.

3.4.1 Environnement de développement

Dans la réalisation de ce projet, nous avons employé plusieurs techniques (langages, outils, environnements, etc.). Dans les sections suivantes, nous allons présenter ces différentes techniques.

- **Java**
  est un langage de programmation orienté objet développé par Sun Microsystems. Les premières versions datent de 1995, il a réussi à intéresser et intriguer beaucoup de développeurs à travers le monde.Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris). Java donne aussi la possibilité de développer des programmes pour téléphones portables et assistants personnels
- **Eclipse**
  est un IDE(Integrated Development Environment) qui est un logiciel qui simplifie

la programmation en proposant un certain nombre de raccourcis et d'aide à la programmation. Il est développé par IBM(Information Business Machines), gratuit et disponible pour la plupart des systèmes d'exploitation. Eclipse compile automatiquement le code que vous écrivez, en soulignant en rouge ou jaune les problème qu'il décèle.

3.5 Les interface de l'application

Dans ce qui suit nous allons présenter quelques interfaces réalisées pour notre application :

- **La page Authentification**
  Cette page permet au client de s'authentifier en insérant un mot de passe et un login.

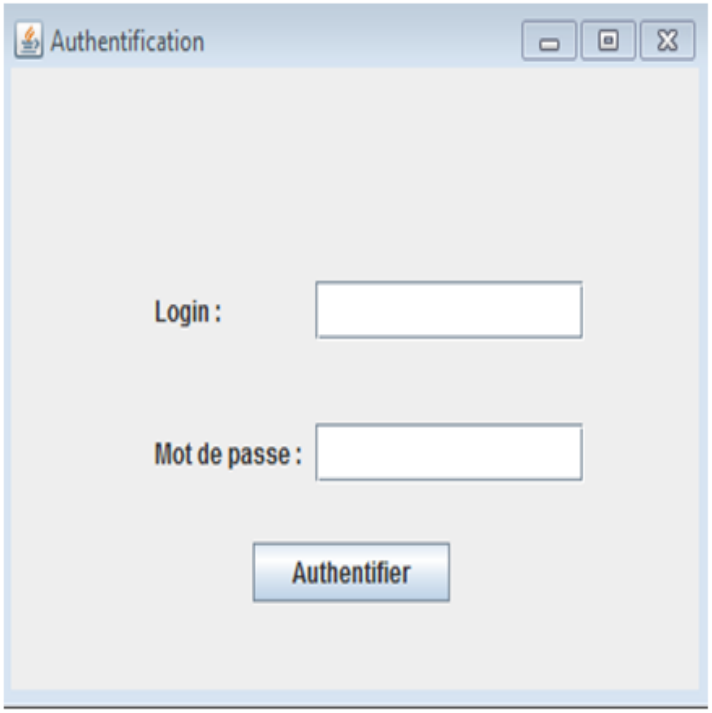


FIG. 3.3 – : La fenêtre Authentification.

Si l'un des deux champs est vide un message d'erreur sera affiché comme illustrer dans cette interface :

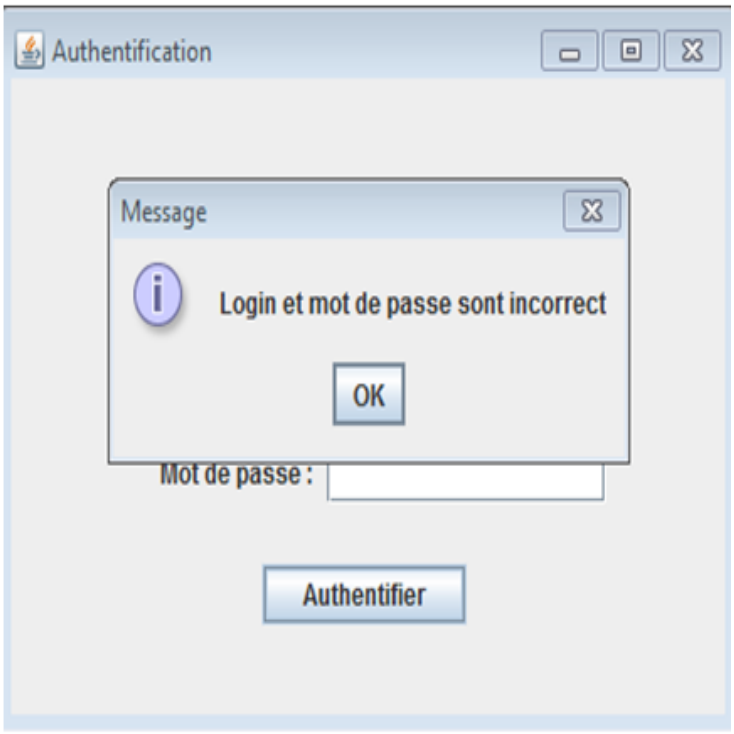


FIG. 3.4 – : La fenêtre Authentification.

- **Interface de détection d'intrusion**

Une fois l'authentification du client est effectuée, l'interface suivante est affichée :

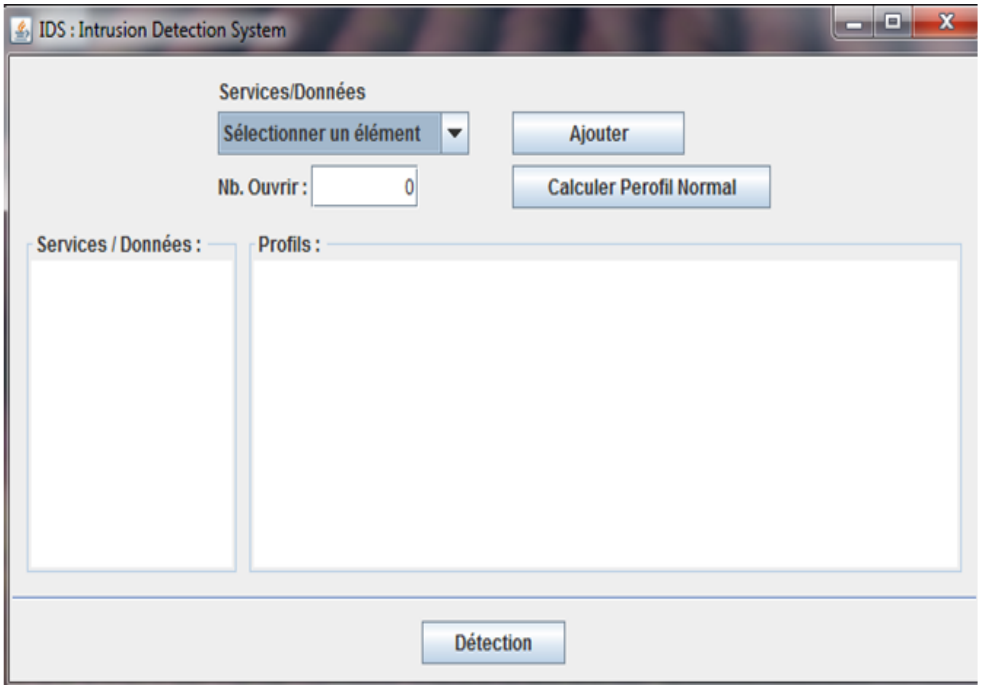


FIG. 3.5 – : Interface de détection (a)

- **Quand on clique pour choisir un service parmi la liste des services et données, si le client n'effectue aucun choix, un message sera afficher dans cette interface indiquant qu'il faut choisir un service ou donnée.**
- **Sion a sélectionné un service parmi la liste mais nous n'avons pas saisie la quantité qu'on veut, et un message sera afficher dans cette interface indiquant qu'il faut saisir un nombre (quantité) après le choix de service ou de donnée.**
- **Quand on clique sur le bouton calcul profile normal, les services et données déjà consulter par le client seront affichés ainsi que le nombre de fois qui sont ouvert ou consulter, ces derniers sont enregistrer dans la base de données.**

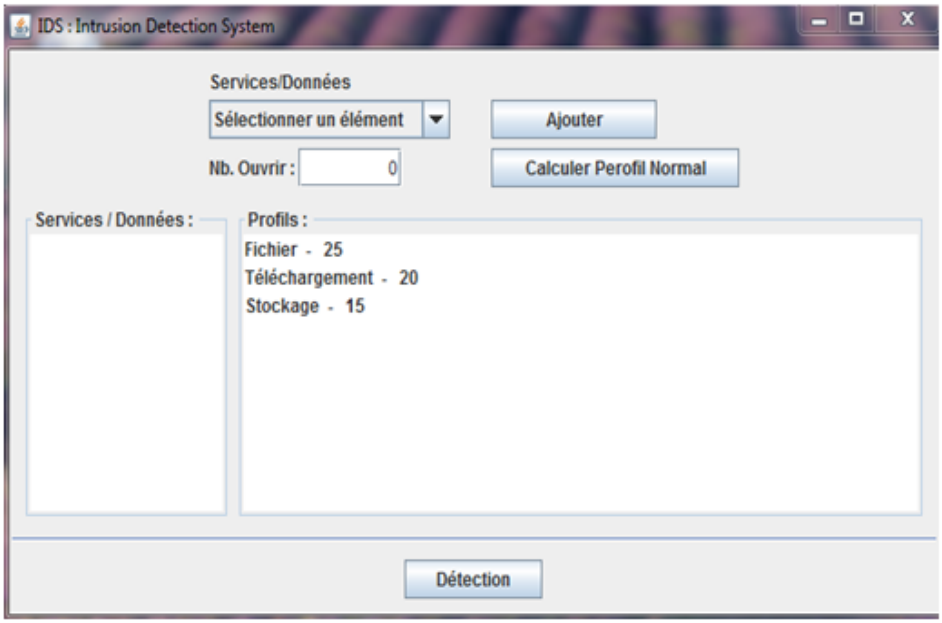


FIG. 3.6 – : Interface de détection (b)

- **message d'alerte est afficher indiquant qu'une intrusion est détectée dans le cas où une déviation du comportement du client est remarquée.**

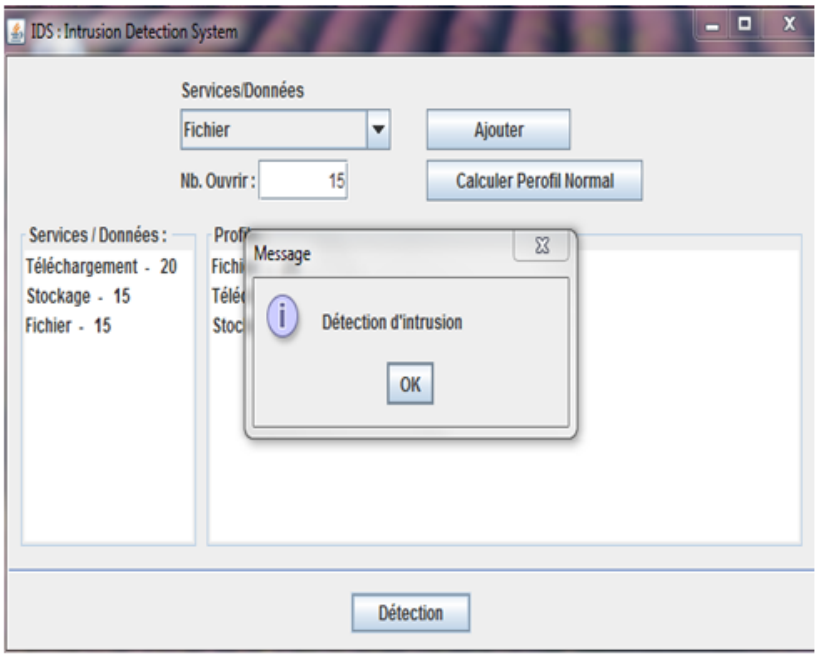


FIG. 3.7 – : Interface de détection (c)

3.6 Conclusion

La détection d'intrusion est l'un des mécanismes de défense et une détection des comportements anormaux d'un utilisateur ou des attaques. Nous avons développé un IDS qui permet de détecter et d'informer qu'une attaque est effectuée.

Conclusion générale

Le cloud computing est une révolution dans le domaine informatique attirant de nouvelles technologies ainsi qu'il offre beaucoup d'avantages en termes de puissance de calcul, de temps de réponse et de réduction des coûts. L'utilisation de plus en plus fréquente du cloud computing fait apparaître de nouveaux risques de sécurité.Pour faire face à ces risques de sécurité, les intervenants du cloud fond recoure aux systèmes de détection et de

préventiond'intrusions qui permettent de repérer et d'empêcher l'intrusion d'un utilisateur (client) malveillant.Les systèmes de détection d'intrusion (IDS) ont pour fonction la surveillance d'événements se produisant dansun système informatique ou dans un réseau.

Tout au long de ce travail, nous avons tenté de palier au problème de la détection d'intrusions dans le Cloud computing, nous avons développé un IDS basé sur les comportements des utilisateurs du clouds (clients). L'objectif été de détecter des intrusions qui se produisait dans le cloud computing, l'idée principale est de comparer lecomportement des utilisateurs accédant aux ressources du cloud avec le comportement habituel (profil normale), lorsqu'uneanomalie est détectée, une alarme est envoyée au fournisseur et au client dans le but de résoudre le problème détecté.

Notre IDS identifie des anomalies et détecte des attaques provenant soit de l'intérieur ou de l'extérieur du réseau. Il répond à toutes les attaques car il se base sur le comportement normal du cloud computing donc, toutes déviation à ce comportement est identifiée comme attaque. Pour les fausses attaques (faux positif), notre IDS peut les réduire grâce à l'intervalle de confiance associé aux données cloud, qui permet de tolérer et réduire les alarmes déclenchées dès qu'une déviation (changement) du comportement des utilisateurs est détectée.

Notre IDS est un bon outil pour la détection d'intrusions connues et inconnues qui est l'objectif des IDSs. Il tire profit de l'approche comportemental. L'approche comportementale est utilisée pour la détection d'intrusions en comparant le comportement actuel de

l'utilisateur cloud à son comportement normal déjà calculé et enregistré et toute déviation à celui-ci est considérée une attaque. Notre système n'a pas besoin de période d'apprentissage pour la construction du profil normale, car il se base sur l'authentification.

En perspective, l'implémentation de tous les concepts étudiés théoriquement comme l'audit du système d'exploitation et le scannage de trafic réseau ou la réponse active reste à compléter, ainsi qu'il serai intéressant de tester notre IDS sur environnement Cloud computing réel.

Bibliographie

[1] J-F Pépin, S. Bouteiller, A-S. Boissard, J. Watrinel, Fondamentaux du Cloud computing- le point de vue des grandes entreprise. Réseau de Grandes Entreprises (CIGREF). Mars 2013. http ://www.eurocloud.fr/doc/cigref2.pdf.(Derniére consultation avril 2016)

[2] N. Degroodt. L'élasticité des bases de données sur le cloud computing. mémoire de master en sciences informatiques. Université libre de bruxelles. Université d'Europe, 2010.

[3] P. Mell, T. Grance, The NIST Definition of Cloud Computing, Recommendation of NIST. Special Publication 800-145, 2011. http ://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[4] B. AZRIA, J. CHERKI, L'impact du Cloud Computing dans les PME, mémoire, Ecole supérieure de génie informatique ESGI, 2014.

[5] S.Lanani. Une approche BPM (Business Process Managment) par composition d'applications dans le cloud computing. Mémoire de magister, Université Mohamed Khider de Biskra. 2010.

[6] A.A.Y. Elwessabi. Une approche basée agent mobile pour le cloud computing. Mémoire de magister. Université HADJ LAKHDAR - BATNA, 2014.

[7] P.P. Codo. Conception d'Une Solution de Cloud Computing Privé Basée sur un Algorithme de Supervision Distribué : Application aux Services IAAS. Ecole Polytechnique d'Abomey-Calavi (EPAC), 2012.

[8] K. Maioua, A. Mansouri. Approche basée Agents Mobiles intelligents dans un environnement de cloud Computing. Mémoire de master. Université Kasdi Merbah

Ouargla, 2014.

[9] H. Saouli. Découverte de services web via le Cloudcomputing à base d'agents mobiles. Thèse de doctorat. Université Mohamed Khider de Biskra, 2015.

[10] D. Yuanshun, X. Yanping, Z.Gewei. Self-healing and Hybrid Diagnosis in Cloud Computing. Proceedings CloudCom of 1st International Conference on CloudComputing. Beijing, China, pp. 45-56, 2009.

[11] AE. Youssef, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[12] http ://www.renaudvenet.com/cloud-computing-avantages-et-inconvenients-2011-01-26.html(Derniére consultation mai 2016)

[13] L.F. Noumsl. Etude et mise en place d'une solution "cloud computing " privée dans une entreprise moderne : cas de CAMTEL. Ecole nationale supérieure des postes et télécommunications, 2012.

[14] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and D, NIST SP 500-292, NIST Cloud Computing Reference Architecture, Leaf, 2011.

[15] O.Markowitch, cours de " cryptologie distribuée et protocoles ", computer science department, université libre de Bruxelles, Belgium, 2009.

[16] W.Stallings, Network security Essentials, 2ndedition, prentice Hall, 2003.

[17] D.E Denning. "An intrusion-dection model".In :proccedings of the IEEE Transactions on software engineering, Septembre 1987 .

[18] H. GUILLAUME, Détection d'intrusions paramétrée par la politique de sécurité, soupélec, campus de rennes, équipe SSIR, 7 février 2005.

[19] H.Debar, M.Dacier, A.Wespi, a revised taxonomy for intrusion detection systems, annals des telecommunications, vol 55, 2000, NO 7-8,PP 361-378.

[20] Ludovic Mé. " Détection des intrusions dans les systèmes d'information : la nécessaire prise en compte des caractéristique du système surveillé ". Habilitation à diriger des

recherches, université de Rennes 1 l'institut de formation Supérieure en informatique et en Communication de Rennes1, 2003.

[21] Nathalie Dagorn, "Détection et prévention d'intrusion : présentation et limites", Rapport de recherche, 2006. https ://hal.archives-ouvertes.fr/inria-00084202/document

[22] L. Sellami, D. Idoughi, PF. Tiako, An Intrusion Detection System Based on Nodes in Cloud Computing Environments. In : P. Iványi, B.H.V. Topping, (Editors), Proceedings of the Fourth International Conference on Parallel, Distributed, Grid and Cloud Computing for Engineering : Civil-Comp Press. Stirlingshire : UK. Paper 22, (2015). doi :10.4203/ccp.107.22.

[23] K.Vieira, A.Schulter, C.Westphall, C.Westphall ,Intrusion detection techniques in grid and cloud computing environment. IEEE IT Professional Magazine, pp.38-43 (2010).

[24] Y. Guan, J. Bao, "A CP Intrusion Detection Strategy on Cloud Computing," In International Symposium on Web Information Systemsand Applications (WISA), pp. 84-87, 2009.

[25] S. Roschke, C. Feng, C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," Fifth International Conference on Information Assurance and Security, vol. 2, 2009, pp.130-134.

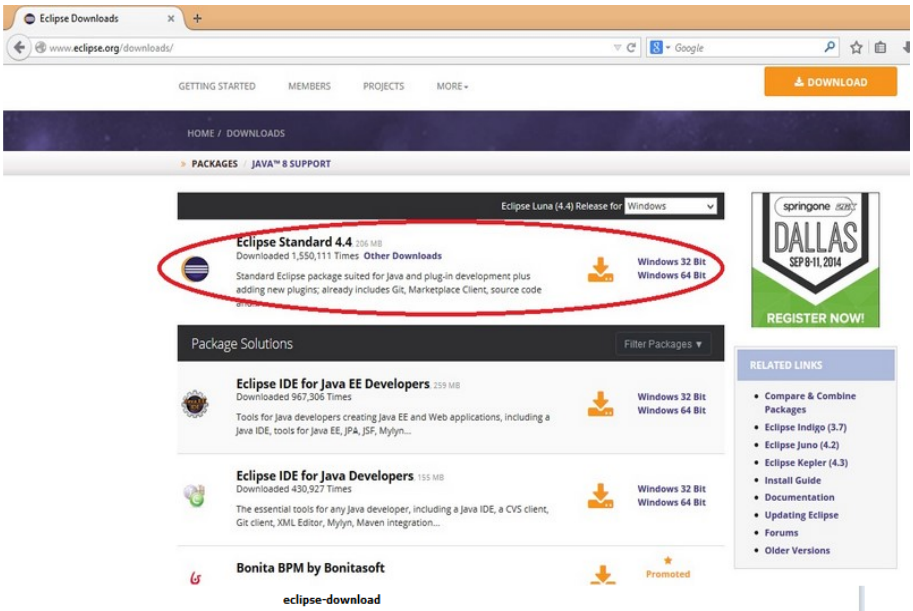
[26] K. A. B. A. V. Dastjerdi, S. G. H. Tabatabaei, "Distributed intrusiondetection in clouds using mobile agents," in Third International Conference on Advanced Engineering Computing and Applications inScinces, 2009. ADVCOMP '09, 2009, pp. 175 - 180.

ANNEXE

1 Téléchargement

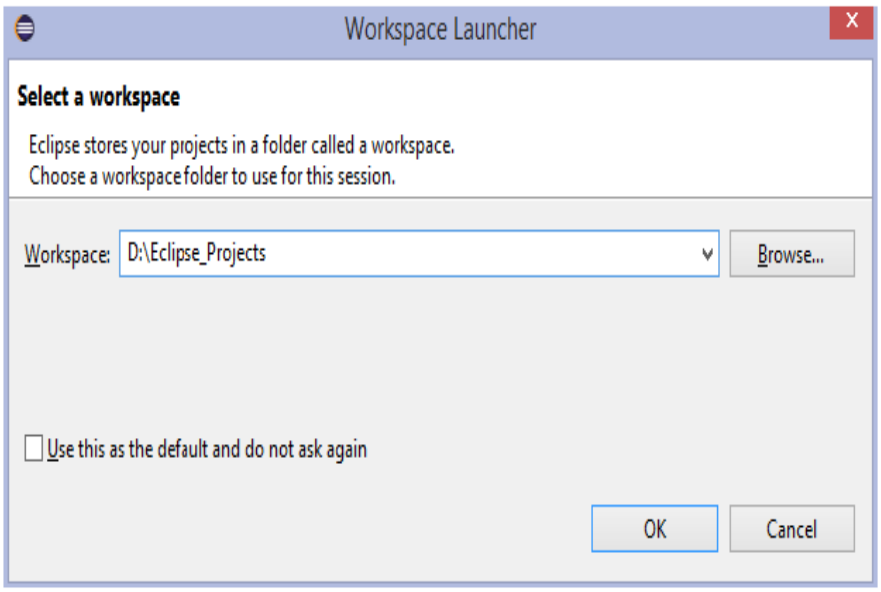
Allez sur le site de la fondation eclipse : http ://www.eclipse.org/

Vous entrez dans l'univers Eclipse... Cliquez sur le bouton 'DOWNLOAD' (bouton orange) à droite. L'écran suivant apparaît, mettant en évidence plusieurs 'eclipse' : La plus imposante est la version dédiée aux développeurs d'applications java qui s'exécuteront dans un serveur (JEE pour Java Enterprise Editon). Celle qui nous intéresse est la version dédiée aux développeurs d'applications Java s'exécutant dans un ordinateur de bureau (JSE pour java Standard Edition) la moins imposante est celle qui permet de développer avec d'autres langages que java : C/C++ ou encore PHP.



2 LANCEMENT

Au premier lancement, Eclipse demande d'indiquer où doit être créé le Workspace . Le Workspace est l'emplacement où seront enregistrés les informations de configuration, les projets et les ressources associées (packages, fichiers sources, fichiers binaires, documentation, etc.). Sur Windows, Eclipse propose, par défaut, de créer cet environnement dans le répertoire ce qui n'est pas forcément l'emplacement idéal (il est souvent préférable de regrouper les projets Java dans un répertoire d'un disque de données). Sélectionner un répertoire vide en utilisant le bouton Browse... et compléter éventuellement le chemin d'accès (le répertoire sera automatiquement créé si nécessaire),

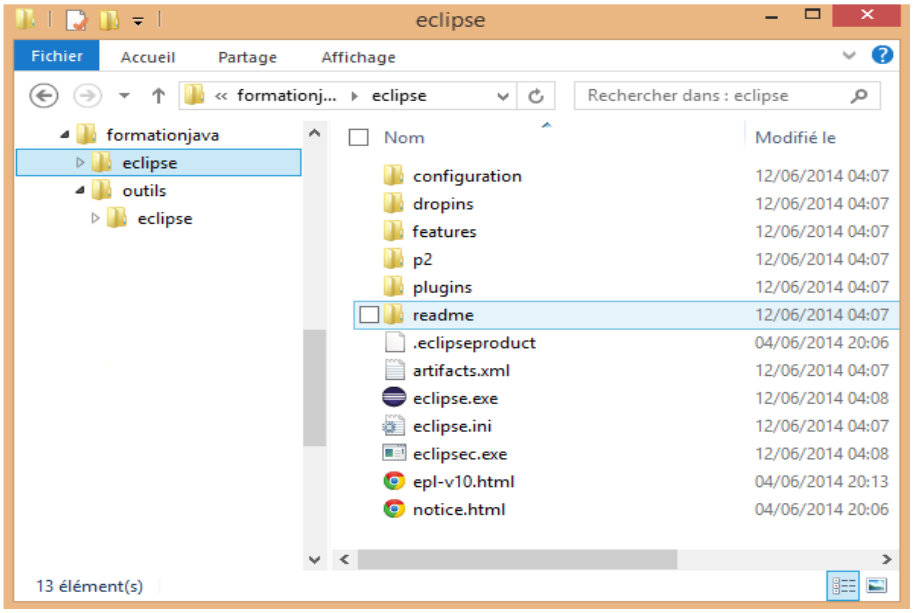


Après avoir, si nécessaire, créé le Workspace, Eclipse affiche un écran de bienvenue qui permet de découvrir différents aspects de l'environnement de développement (vue d'ensemble des différents composants, didacticiels, exemples, nouveautés, etc.).

Le lancement de l'environnement de développement proprement dit s'effectue en cliquant sur l'icône représentant une flèche à droite de l'écran (Workbench) ou en fermant l'onglet Welcome.

3 Installation

Dézippez le fichier eclipse-standard-luna-R-win32. Vous obtenez une arborescence comme celle-ci.



ça y est. Eclipse est installé. Reste à le lancer...

RÉSUMÉ

Avec l'avènement du Cloud computing comme nouveau modèle de déploiement des systèmes informatiques, les grandes entreprises, les communautés scientifiques et même privés profitent des avantages de ce paradigme pour déporter leurs ressources et données. Dans ce contexte il devient nécessaire de mettre en œuvre une solution pour éviter les attaques qui se produisent en utilisant ses ressources ou données. En conséquence nous proposant dans ce travail, une façon de réduire le nombre d'attaques qui se produisent dans le Cloud computing lors de l'utilisation de ses ressources et données. Nous exploitons le comportement enregistré d'un client lors de l'utilisation des ressources disponible dans le Cloud computing afin de le comparer avec un autre comportement qui se passe aprèsce dernier, cette comparaison va nous permettre de détecter des intrusions si le comportement n'est pas le même sinon il y'aura pas d'intrusions cette façon est l'implémentation d'un IDS a base de comportement. Ce manuscrit contient des généralités sur le Cloud computing, les systèmes de détection d'intrusions, et une analyse sur les différentes approches proposées pour pallier le problème de sécurité et des intrusions dans le Cloud computing. Une partie du manuscrit est consacrée à notre proposition de notre solution suivi d'une partie consacrée a sa validation. Nous avons utilisé le langage JAVA pour l'implémentation de notre application ainsi que le PhpMyAdmin pour la création d'une base de données.

Mots clés : CLOUD COMPUTING,INTRUSION,JAVA, IDS.

ABSTRACT

With the advent of cloud computing as new deployment model computer systems, large enterprises, scientists and even private communities enjoy the benefits of this paradigm to deport their resources and data. In this context it becomes necessary to implement a solution to prevent attacks that occur by using its resources or data. Accordingly offering us in this work, a way to reduce the number of attacks that occur in cloud computing during the use of its resources and data. We operate the recorded behavior of a customer in the use of available resources in the cloud computing in order to compare it with another behavior happens after it, this comparison will allow us to detect intrusions if the behavior does is not the same if it y 'will not trespassing this way is the implementation of an SDI baseline behavior.This manuscript contains general information on cloud computing, intrusion detection systems, and analysis of the various approaches proposed to overcome the security problem and intrusions into cloud computing. Part of the manuscript is dedicated to our proposal to our solution followed by a devoted party validation. We used the Java language to implement our application and the phpMyAdmin to create a database.

Key words : CLOUD COMPUTING,INTUSION,JAVA,IDS..