الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة د. مولاي الطاهر

كلية التكنولوجيا

قسم: الإعلام الآلي

Mémoire de Master

Spécialité : Réseaux Informatiques et Systèmes Répartis

Détection et prédiction des attaques DOS dans l'internet des objets

Présenté par :

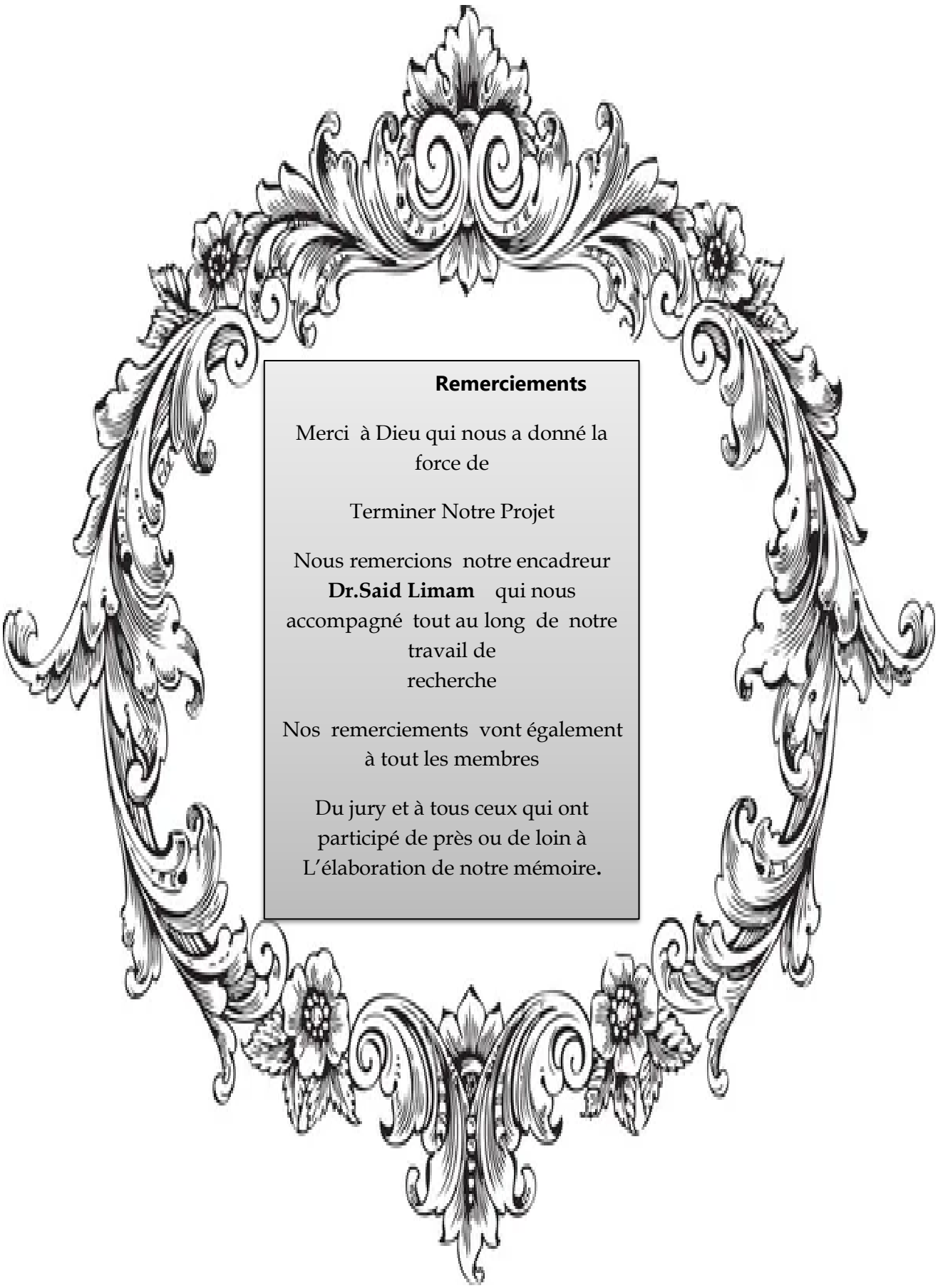
Benyoucef Messaouda

Morsli Amal

Dirigé par :

Dr.Said Limam

Promotion 2021 - 2022



Remerciements

Merci à Dieu qui nous a donné la force de

Terminer Notre Projet

Nous remercions notre encadreur **Dr.Said Limam** qui nous accompagné tout au long de notre travail de recherche

Nos remerciements vont également à tout les membres

Du jury et à tous ceux qui ont participé de près ou de loin à L'élaboration de notre mémoire.

Dédicace

Merci Allah, mon dieu de mavoir donne la capacité d'écrir et de réfléchir, la force de réaliser ce mémoir.

A mes très chers parents, source de vie ,d'amour et d'affection

A mes chers frères et sœurs, source de jion et de bonheur

Ma binôme :Amal

A tout mes amis Rajaa ,Amal, Hanane ,Souhila, Chahinaze source d'espoire et de motivation

Dédicace

Merci Allah ,mon dieu de mavoir donne la capacité d'écrir et de réfléchir ,la force de réaliser ce mémoir .

A ma chère mère source de vie ,d'amour et d'affection

A la mémoire de mon père

A Mon cher frère et mes chères sœurs, source de jion et de bonheur

Ma binôme : Messaouda

A tout mes amis Rajaa, Amal, Hanane ,Souhila ,Chahinaze,Asma source d'espoire et de motivation

TABLE DES MATIÈRES

Introduction générale..... **I**

CHAPITRE I :INTRODUCTION À L'INTERNET DES OBJETS ET AU CLOUD ET FOG COMPUTING

Introduction. **1**

I.1 Internet des objets (IoT):.....**2**

I. 1.1 Définition.....**2**

I. 1. 2 L'objectif d'IoT. **2**

I .1. 3 Domaines applicatifs de l'IoT **3**

I.2 Cloud Computing.....**4**

I. 2.1 Définition:..... .....**4**

I. 2.2 Types de services cloud..... .....**4**

I .2.3 Types de cloud computing:.....**5**

I .2.4 Utilisations du cloud computing:..... ....**5**

I .2.5 principaux avantages du cloud computing..... .....**7**

I .2.5.1 Coût …….....**7**

I.2.5.2 Vitesse …….....……...…….....**7**

I .2.5.3 Mise à l'échelle mondiale ..…….…….....…….…….....……....**8**

I .2.5.4 Productivité …….....……...……...…..**8**

I. 2.5.5 Performances ……. .....……...……...……...**8**

I .2.5.6 Fiabilité …….....……...…….....**8**

I.2.5.7 Sécurité …….....…….....……**8**

I.2.6 Les risques juridiques liés à l'utilisation du cloud computing.…….….....……....**9**

I.2.6.1 La sécurité et la sécurisation des donnée …….....……....**9**

I .2.6.2 Les précautions juridiques nécessaires à la rédaction d'un contrat de cloud computing…….....,,,,.....…**10**

I.2.7 Passer du cloud au Fog……..……..……11

I .3 Fogcomputing…….…….....**11**

I .3.1Définition: ……..……..... **.12**

I .3.2caractéristique…….....…….…..**12**

I .3 .3 Comment fonctionne le fogcomputing :…….....……**13**

I.3.4 Les enjeux du Fog Computing pour les utilisateurs :….....……..……**13**

I .3.5 Les avantages :…….....…..**13**

I .3.6 Les inconvénients du fogcomputing :…….....……..……..**14**

I .3.6.1 Risques liés à la sécurité et à la vie privée :.…….....…..……..…....**14**

I .3.6.2 Consommation d'énergie :..…….....…….....**14**

I .3.6.3 Emplacement physique dangereux :.....……..….**14**

I. 3.6.4 Complexité du réseau :…….....……..……..…**14**

Conclusion …….....…….....**15**

CHAPITRE II : LES ATTAQUES DOS ET DDOS

Introduction …….....……..……..…….....**16**

II.1 Les attaques DoS /DDOS ……..……..….....**16**

II.1.1 Les attaque Dos :..…….....……..…..**17**

II.1.1.1 Définition Dos :…….....….**17**

II.1.1.2 Historique :…….....…....**17**

II.1.1.3 L'objectif principal d'une attaque DoS :……..….....…..…**18**

II.1.1.4 Les catégories des attaques DoS……..….....……**18**

II.1.1.4.1 Attaques par débordement de tampon :…….....….....**18**

II.1.1.4.2 Attaques par saturation : …….....…..…..**18**

II.1.1.5 Le principe de DoS :…….....……..**19**

II.1.2 Les attaques DDOS ….……..…….....**19**

II.1.2.1 Définition :…….....…**19**

II.1.2.2 Types d'attaques DDoS …….....**20**

II.1.2.3 différence avec une attaque DoS et DDOS……..…….....20

II .2 les articles pour la détection de DoS…….....…….……21

Conclusion …….....……..……24

CHAPITRE III : LE MODULE PROPOSÉ

Introduction……..…….....…….……..25

III.1 Topologie ……..…….....…26

III.2 Le module de détection et de prévention des attaques DoS proposé…….....27

III.2.1L'architecteur de notre proposition de détection…….....28

III.2.2attaque check…….....31

III.2.2 algorithme attaque check…….....…32

III.2.3 misse à jour…….....32

III.2.3 algorithme update…….....33

Conclusion…….....34

CHAPITRE IV :LA SIMULATION

Introduction……..…….....35

IV.1 Langage et l'environnement de notre travail…….…….....35

IV.1.1Langage de programmation Java …….....35

IV.1.1.1 Les avantages de langage Java …….....35

IV.1.2L'environnement de développement …….....…….....…36

IV.2Simulateur IfogSim……...……...…….....36

IV.2.1 Les principales classes d'iFogSim …….....…….....…36

IV.2.2 Les classes modifier…….....…...39

IV .3 modèle d'application……..…….....……....40

IV .4 Diagramme de séquence…….…….....……..…….....41

IV.5 L'interface……..…….....……...……...43

IV.6Résultat exprimentaux.....46

IV.6.1 Expérience 1…….....…….…….**46**

IV.6.1 Expérience 2…….....…….**47**

IV.6.1 Expérience 3…….....…….....**48**

Conclusion …….....**49**

Conclusion général…….…….....**50**

LISTE DES FIGURES

Figure I.1 : le monde avant et après l'internet des objets……**03**

Figure I.2 : Cloud computing…….……**09**

Figure I.3 : Architecture IoT basée sur le Fog Computing……...**12**

Figure II.1 : Daniel de service…….…**16**

Figure II.2 : l'architecture de déni de service……..…...**19**

Figure II.3 : distribuer Daniel de service…….**21**

Figure III.1 : fog computung……...**26**

Figure III.2 : architecteur de notre proposition de détection……...**28**

Figure III.3: l'organigramme de fonctionnement de notre modèle de détection ……**30**

Figure IV.1 : Principales classes d'iFogSim……**37**

Figure IV.2: Modèle d'application d'our app……**40**

Figure IV.3 : diagramme de séquence sans attaque……**41**

Figure IV.4 : diagramme de séquence avec attaque……**42**

Figure IV.5 : interface Fog Divece…….**44**

Figure IV.6: interface mobile……**45**

Figure IV.7 :temps d'exécution avec et sans détection…….**46**

Figure IV.8 :l'utilisation de bande passante avec et sans détection……...**47**

Figure IV.9 :l'énergie de fog avec et sans détection…….….**48**

LISTE DES TABLEAUX

Tableau III.1 : la description de variable……**31**

Tableau IV.1 : temps d'exécution avec et sans détection……..….**46**

Tableau IV.2 : l'utilisation de la bande passante avec et sans détection……..……..…**47**

Tableau IV.3 : l'énergie de fog avec et sans détection……**48**

Introduction générale:

Le Fog Computing est une solution alternative au cloud computing où vous êtes responsable du stockage et du traitement des données des objets connectés. Le Fog Computing se caractérise par la confidentialité du stockage et du traitement des données grâce à l'utilisation d'équipements en périphérie du réseau.

Les "attaques informatiques" ou "cyberattaques" sont des actions volontaires et malveillantes menées au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent. Et tout le monde peut en être la cible : les particuliers, les entreprises, les institutions, les services administratifs et de santé. Parmi ces attaques les attaques DoS.

Ces attaque DoS (Denial of Service en anglais) sont des attaques informatiques ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

Dans notre travail, nous avons proposé un module de détection et de prévention des attaques DoS qui est composé de deux algorithme et nous avons implémenté notre proposition sur le simulateur IfogSim que nous avons étendu.

Organisation du mémoire

Le mémoire est organisé en quatre chapitres :

- **Dans le premier chapitre**, nous présentons les principes des : internet des objets Cloud computing, fog computing.
- **Le deuxième chapitre**, présente les attaques DoS et DDoS.
- **Le troisième chapitre**, décrit et détaille le module de détection et de prévention des attaques DoS que nous avons proposé.
- **Le quatrième chapitre,** présent les résultats de simulation que nous avons effectué pour évaluer notre module de détections, ces résultat de simulation ont été obtenu par le simulateur iFogSim que nous avons étendu.

CHAPITRE

I

Introduction

Internet est un réseau informatique mondial accessible au public. Il s'agit d'un réseau de réseaux, à commutation de paquets, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, gouvernementaux, eux-mêmes regroupés en réseaux autonomes ; il en existe plus de 91 000 en 2019 .

L'information est transmise via Internet grâce à un ensemble standardisé de protocoles de transfert de données, qui permet des applications variées comme le courrier électronique, le World Wide Web, la messagerie instantanée, le partage de fichiers en pair-à-pair, le streaming, le podcasting, la téléconférence.

Dans les années 1990, l'apparition du Web contribue à rendre Internet accessible au grand public. Depuis les années 2010, un nombre croissant de types d'objets divers y sont connectés, formant l'Internet des objets.

Un internaute est une personne qui utilise un accès à Internet. Cet accès peut être obtenu grâce à un fournisseur d'accès via divers moyens de communication électronique : soit filaire (réseau téléphonique commuté à bas débit, ADSL, fibre optique jusqu'au domicile), soit sans fil (WiMAX, par satellite, 1G, 2G, 3G, 3G+, 4G, 4G+ ou 5G)[1].

I.1 Internet des objets (IoT)

Avant de définir les concepts d'IoT, il est important de définir l'objet connecté qui est un objet possédant la capacité d'échanger des données avec d'autres entités physiques ou numériques

I. 1.1 Définition

L'Internet des Objets est un réseau de réseaux qui permet expansion du réseau internet à des objets et/ou des lieux du monde physique , via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant. En anglais, on parle d'IoT (Internet of Things .)

L'Internet des objets (IoT) fait référence au stade évolutif d'Internet, qui constitue une infrastructure de communication globale entre les humains et les machines. L'IoT construit l'infrastructure mondiale qui changera les aspects fondamentaux de nos vies, des services de santé à la fabrication, de l'agriculture à l'exploitation minière. L'IoT offrira les installations nécessaires aux derniers développements en matière d'intelligence artificielle (IA)

I. 1. 2 L'objectif d'IoT [3]

- Evolution naturelle des technologies : lien inévitable entre le monde numérique et le monde physique.
- Assistance à nos activités professionnelles et personnelles.
- Permet une réduction considérable des dépenses dans l'économie d'aujourd'hui (industrie, santé, sécurité, etc.).
- L'IoT est ici et il évolue rapidement ! Il n'y a pas de temps à perdre.
- 50 milliards d'objets en 2020 (estimation)

I .1. 3 Domaines applicatifs de l'IoT [3]

- Ville intelligente : circulation routière intelligente, transports intelligents, collecte des déchets, cartographies diverses (bruit, énergie, etc.).
- Environnements intelligents : prédiction des séismes, détection d'incendies, qualité de l'air, etc.
- Sécurité et gestion des urgences : radiations, attentats, explosions.
- Logistique : aller plus loin que les approches actuelles.
- Contrôle industriel : mesure, pronostic et prédiction des pannes, dépannage à distance.
- Santé : suivi des paramètres biologiques à distance.
- Agriculture intelligente, domotique, applications ludiques etc.

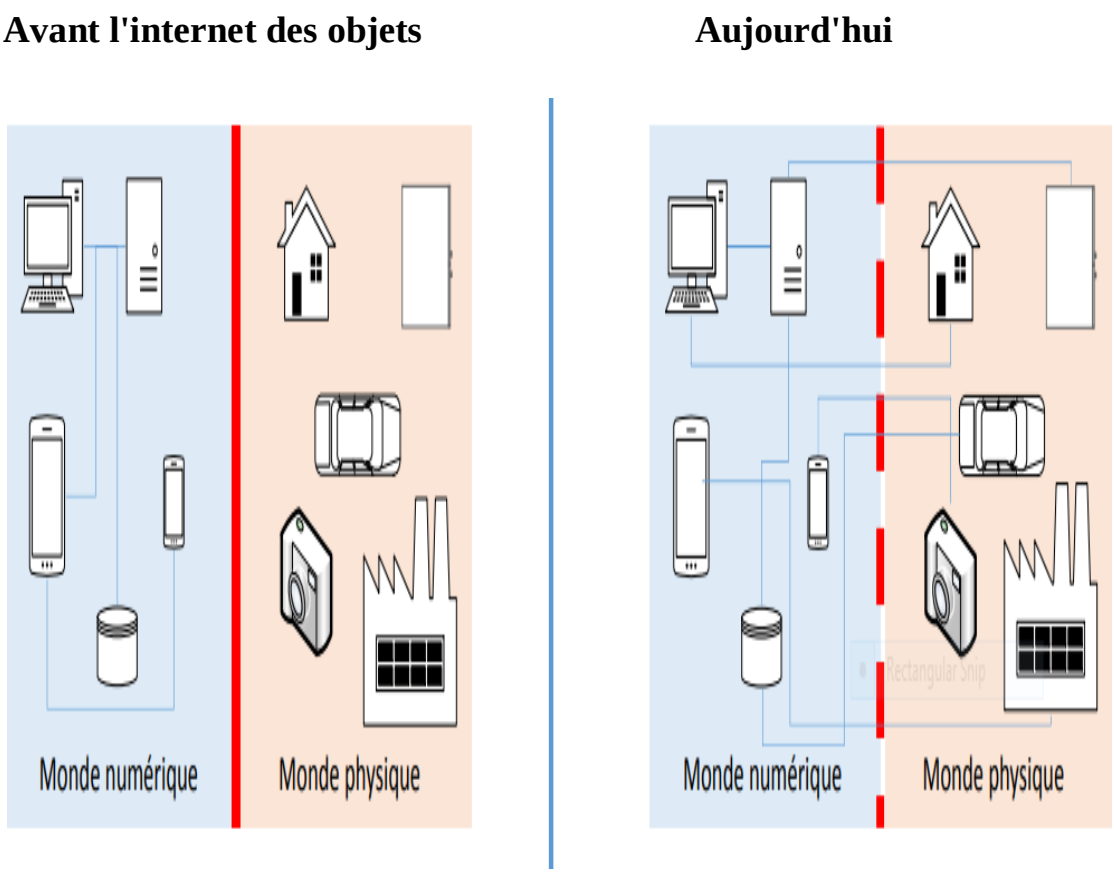


Figure I .1 : le monde avant et après l'internet des objets [4]

I.2 Cloud Computing

I. 2.1 Définition

Le cloud computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. L'ordinateur de bureau ou portable, le téléphone mobile, la tablette tactile et autres objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs. Le cloud se caractérise également par sa souplesse qui permet aux fournisseurs d'adapter automatiquement la capacité de stockage et la puissance de calcul aux besoins des utilisateurs [5]

I . 2.2 Types de services cloud (IaaS, PaaS, SaaS)

La plupart des services de cloud computing peuvent être classés en quatre grandes catégories : IaaS (infrastructure as a service), PaaS (platform as a service), serverless et SaaS (software as a service). On les appelle parfois « pile » de cloud computing, car elles s'empilent les unes sur les autres. Si vous savez en quoi elles consistent et en quoi elles sont différentes, vous pourrez plus facilement atteindre vos objectifs. [5]

I .2.2.1 IaaS (Infrastructure as a Service, en anglais)

Le système d'exploitation et les applications sont installés par les clients sur des serveurs auxquels ils se connectent pour travailler comme s'il s'agissait d'un ordinateur classique.

I. 2.2.2 PaaS (Platform as a Service, en anglais)

Dans ce mode, c'est le fournisseur du service cloud qui administre le système d'exploitation et ses outils. Le client peut installer ses propres applications si besoin.

I .2.2.3 SaaS (Software as a Service,en anglais)

Les applications sont fournies sous forme de services clés en mains auxquels les utilisateurs se connectent via des logiciels dédiés ou un navigateur Internet. Pour le grand public, il s'agit par exemple de messageries électroniques type Gmail, Yahoo, Outlook.com ou de suites bureautiques type Office 365 ou Google Apps

I .2.3 Types de cloud computing

Il Tous les clouds ne sont pas identiques et aucun type de cloud computing ne convient à tout le monde. Plusieurs modèles, types et services différents ont évolué pour vous aider à trouver la solution adaptée à vos besoins.

Vous devez commencer par déterminer le type de déploiement cloud ou d'architecture de cloud computing sur lequel vos services cloud seront implémentés. existe trois modes de déploiement de services cloud : le cloud public, le cloud privé et le cloud hybride. [6]

I .2.3.1 Cloud public

Un cloud public est détenu et exploité par un fournisseur de services cloud tiers, qui propose des ressources de calcul, telles que des serveurs et du stockage, via Internet. Microsoft Azure est un exemple de cloud public. Dans un cloud public, tout le matériel, tous les logiciels et toute l'infrastructure sont la propriété du fournisseur du cloud. Vous accédez à ces services et vous gérez votre compte par l'intermédiaire d'un navigateur web. .

I.2.3.2 Cloud privé

Le cloud privé est l'ensemble des ressources de cloud computing utilisées de façon exclusive par une entreprise ou une organisation. Le cloud privé peut se trouver physiquement dans le centre de données local de l'entreprise. Certaines entreprises paient également des fournisseurs de services pour qu'ils hébergent leur cloud privé. Le cloud privé est un cloud dans lequel les services et l'infrastructure se trouvent sur un réseau privé.

I.2.3.3 Cloud hybride

Le cloud hybride regroupe des clouds publics et privés, liés par une technologie leur permettant de partager des données et des applications. En permettant que les données et applications se déplacent entre des clouds privé et public, un cloud hybride offre à votre entreprise une plus grande flexibilité, davantage d'options de déploiement et une optimisation de votre infrastructure, de votre sécurité et de votre conformité existantes.

I .2.4 Utilisations du cloud computing

Vous utilisez probablement en ce moment même le cloud computing sans le savoir. Si vous utilisez un service en ligne pour envoyer des courriers électroniques, modifier des documents, regarder des films ou regarder la télévision, jouer à des jeux ou stocker des images ou autres fichiers, il est probable que le cloud computing intervienne dans les coulisses. Les premiers services de cloud computing n'ont pas encore dix ans, mais un grand nombre d'organisations, par

exemple des start-ups, des multinationales, des services administratifs ou des ONG, adopte cette technologie pour de nombreuses raisons .[7]

Vous trouverez ici quelques exemples des possibilités d'utilisation des services cloud d'un fournisseur de cloud :

- **Créer des applications cloud natives**

Créez, déployez et mettez à l'échelle rapidement des applications (web, mobiles et API). Tirez parti des technologies et approches cloud natives, telles que les conteneurs, Kubernetes, l'architecture de micro services, la communication pilotée par des API et DevOps.

- **Tester et générer des applications**

Réduisez les coûts et délais de développement d'applications en utilisant des infrastructure cloud dont l'échelle peut être facilement adaptée.

- **Stocker, sauvegarder et récupérer des données**

Protégez vos données à moindre coût et à grande échelle en les transférant via Internet vers un système de stockage cloud hors site, accessible à partir de tout emplacement et appareil.

- **Analyser des données**

Unifiez vos données entre les équipes, les divisions et les emplacements dans le cloud. Utilisez ensuite des services cloud, par exemple de Machine Learning et d'intelligence artificielle, pour extraire des insights qui vous permettent de prendre des décisions éclairées.

- **Diffuser du contenu audio et vidéo**

Communiquez avec votre public en tout lieu, en tout temps et sur tout appareil via un système audio et vidéo haute définition mondialement distribué.

- **Incorporer de intelligence**

Utilisez des modèles intelligents pour interagir avec les clients et fournir des insights à partir des données capturées.

- **Diffuser des logiciels à la demande**

Également appelés logiciel en tant que service (SaaS, Software as a Service), les logiciels à la demande vous permettent d'offrir à vos clients les versions et mises à jour les plus récentes des logiciels, à tout moment et en tout lieu.

I .2.5 principaux avantages du cloud computing

Le cloud computing est radicalement différent de l'approche traditionnelle que les entreprises adoptent en matière de ressources informatiques. Voici sept raisons courantes pour lesquelles les organisations optent pour des services de cloud computing [7] :

I .2.5.1 Coût

Le cloud computing élimine la nécessité d'investir dans du matériel et des logiciels, et de configurer et de gérer des centres de données sur site : racks de serveurs, alimentation électrique permanente pour l'alimentation et le refroidissement, experts informatiques pour la gestion de l'infrastructure. La facture est vite salée.

I.2.5.2 Vitesse

La plupart des services de cloud computing sont fournis en libre-service et à la demande. D'énormes ressources de calcul peuvent donc être mises en œuvre en quelques minutes et en quelques clics, offrant ainsi aux entreprises un haut niveau de flexibilité et les dégageant de la pression liée à la planification de la capacité.

I .2.5.3 Mise à l'échelle mondiale

La mise à l'échelle élastique est un des avantages des services de cloud computing. En termes de cloud, cela veut dire qu'il est possible de mettre en œuvre la quantité nécessaire de ressources informatiques, par exemple plus ou moins de puissance de calcul, de stockage ou de bande passante, au moment où elles sont nécessaires, là où elles sont nécessaires.

I .2.5.4 Productivité

Les centres de données sur site nécessitent en général la manipulation de matériel, la mise à jour des logiciels et d'autres corvées informatiques qui prennent beaucoup de temps. Le cloud computing supprime la plupart de ces tâches et les équipes informatiques peuvent donc passer plus de temps à travailler à la concrétisation des objectifs de l'entreprise.

I. 2.5.5 Performances

Les plus grands services de cloud computing s'exécutent sur un réseau de centres de données sécurisés, dont le matériel est régulièrement mis à niveau pour assurer des performances rapides et efficaces. Ceci offre plusieurs avantages par rapport à un centre de données classique, y compris un temps de latence réseau réduit pour les applications et de plus grandes économies d'échelle.

I .2.5.6 Fiabilité

Le cloud computing simplifie la sauvegarde des données, la récupération d'urgence et la continuité des activités. Il rend ces activités moins coûteuses, car les données peuvent être mises en miroir sur plusieurs sites redondants au sein du réseau du fournisseur.

I.2.5.7 Sécurité

De nombreux fournisseurs de cloud offrent un vaste éventail de stratégies, technologies et contrôles qui renforcent globalement votre situation de sécurité, contribuant ainsi à protéger vos données, vos applications et votre infrastructure contre des menaces potentielles.

Figure I .2 : Cloud computing [8]

I.2.6 Les risques juridiques liés à l'utilisation du cloud computing

I.2.6.1 La sécurité et la sécurisation des données

L'accès aux données et aux applications est réalisé entre le client et la multiplicité des serveurs distants. Leur mutualisation et la délocalisation de ceux-ci multiplie donc les risques. L'accès aux services induira donc des connexions sécurisées et une authentification des utilisateurs, induisant alors le problème de la gestion des identifiants et celui des responsabilités (accès non autorisé, perte ou vol d'identifiants,etc.).

Pour les mêmes raisons, il existe également un risque de perte de données qu'il conviendra de prendre en considération, d'évaluer et d'anticiper dans le cadre de procédures de sauvegarde adaptées (stockage dans des espaces privés, en local, en environnement public, etc.). De même, il existe également des risques au regard de la confidentialité des données (fuites), vu le nombre de serveurs et la délocalisation de ceux-ci.

De plus, il existe des risques financiers liés aux outils de contrôle servant à évaluer la consommation du cloud computing, et sa facturation. Il conviendra ainsi de définir contractuellement une unité de mesure du stockage, et des ressources informatiques utilisées. [9]

I .2.6.2 Les précautions juridiques nécessaires à la rédaction d'un contrat de cloud computing

Pour pallier les risques précédemment évoqués, il conviendra de conclure une convention de niveau de service, ou SLA (Service Level Agreement) qui pourra comporter des indications quant aux attentes du client, au sujet de la réalisation des obligations du prestataire (malus ou pénalités).

Par ailleurs, pour assurer une pérennité des services de cloud computing, il s'avère primordial de contractualiser un plan de réversibilité permettant d'assurer le transfert des services à d'autres prestataires. Il faudra donc prévoir les facteurs déclencheurs de cette réversibilité (carence du prestataire, libre choix du client après un certain nombre d'années), et ses conditions, ainsi que son coût.

En cas de perte de données, il sera préconisé de prévoir la réplication de celles-ci sur plusieurs sites ou l'obligation de résultat de restauration des données dans des délais contractuels définis. Par ailleurs, le contrat prendra soin de préciser que l'ensemble des traitements ne seront opérés par l'hébergeur que sur instructions et contrôle des utilisateurs, c'est-à-dire sans prise d'initiative sans instructions expresses des utilisateurs considérés comme responsables de traitements.

Enfin, pour ce qui est de l'intégrité et de la confidentialité des données, il pourra être prévu une clause d'audits externes, ainsi qu'une clause de responsabilité dont il faudra s'assurer de la rigueur, pour encadrer tout particulièrement la traçabilité, l'accès frauduleux, l'atteinte à l'intégrité, voire la perte de données sensibles. [10]

I.2.7 Passer du cloud au Fog

Même si le Cloud Computing présente de nombreux avantages, il est sur le point d'être supplanté par une manière de travailler encore plus sophistiquée : le Fog Computing, qui repose sur les mêmes principes que le Cloud Computing, mais avec bien plus de sécurité.

Le Cloud Computing présente néanmoins des inconvénients, le plus grave concernant la sécurité. Si l'intégrité du serveur qui héberge vos outils informatiques est compromise, les données de vos employés et de vos clients pourraient être exposées à des risques. En fonction de la taille de l'entreprise, cela pourrait signifier que les données de milliers voire de millions d'utilisateurs seraient compromises. Heureusement, le Fog Computing offre une solution.

I .3 Fog computing

Même si le Cloud Computing présente de nombreux avantages, il est sur le point d'être supplanté par une manière de travailler encore plus sophistiquée : le Fog Computing, qui repose sur les mêmes principes que le Cloud Computing, mais avec bien plus de sécurité. Le Cloud Computing présente néanmoins des inconvénients, le plus grave concernant la sécurité. Si l'intégrité du serveur qui héberge vos outils informatiques est compromise, les données de vos employés et de vos clients pourraient être exposées à des risques. En fonction de la taille de l'entreprise, cela pourrait signifier que les données de milliers voire de millions d'utilisateurs seraient compromises.[11]

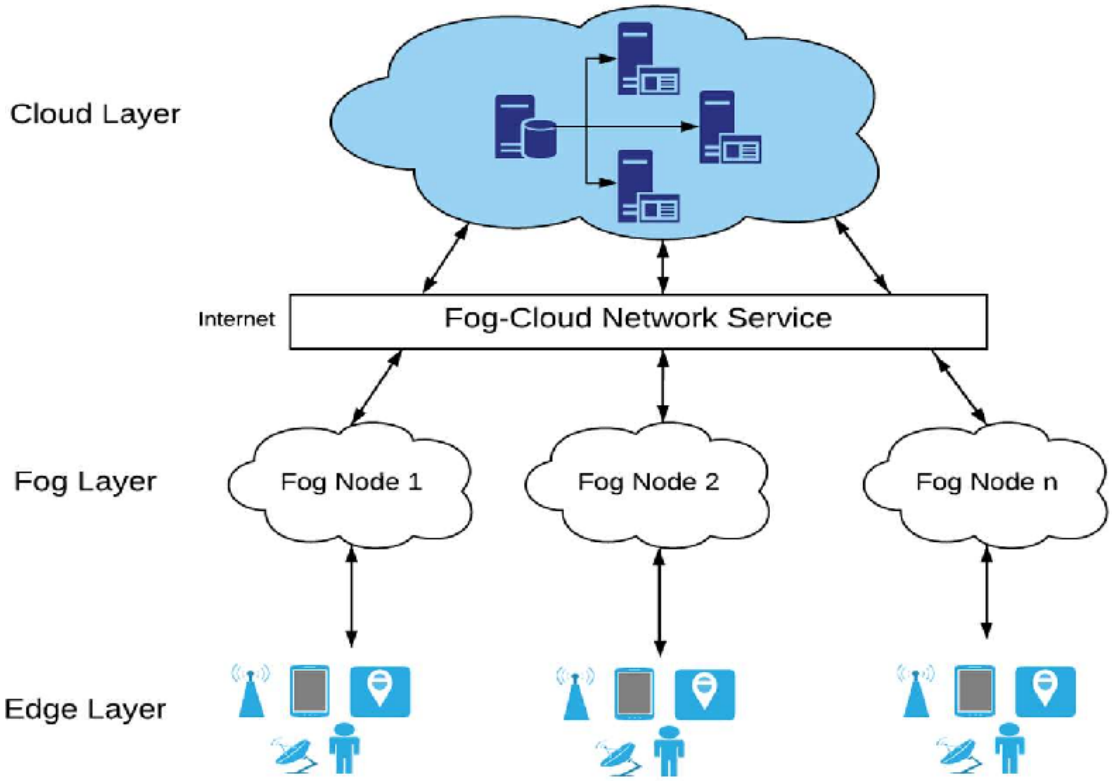


Figure I .3 : Architecture IoT basée sur le Fog Computing [11]

I .3.1 Définition

Le fog computing, aussi appelé "informatique dans le brouillard", définit une infrastructure chargée de stocker et de traiter des données issues d'objets connectés. Concurrent direct, alternative ou solution complémentaire au cloud computing, le fog computing a comme particularité de stocker et de traiter les données via le recours à des équipements implantés à la périphérie du réseau. Il permet donc de réaliser ces deux actions en local, sans avoir à solliciter un datacenter situé à plusieurs centaines de kilomètres ou un cloud. Dans ce domaine du stockage et du traitement des données et de l'IoT, le fog computing crée une interface supplémentaire que l'on peut situer entre le Edge Computing et le Cloud Computing. [12]

I .3.2 caractéristiques

La norme IEEE définit le « fog computing » comme « une architecture horizontale au niveau du système qui distribue les ressources et les services de calcul, de stockage, de contrôle et de mise en réseau à travers tout le continuum cloud-objets » .

Cette informatique géo distribuée se caractérise en général par:[13]

- la mise en œuvre d'un grand nombre de capteurs intelligents ou d'objets connectés.
- l'utilisation de l'informatique en nuage.
- des volumes de données importants à traiter.
- une sensibilité à la latence des communications dans le réseau.
- une large distribution géographique des objets connectés et/ou la prise en compte de leur localisation.
- une hétérogénéité des équipements.
- l'utilisation de réseaux sans-fils et/ou d'équipements mobiles.

I .3 .3 Comment fonctionne le fog computing ?

L'Open Fog a défini une infrastructure pour mettre en œuvre une solution de FaaS (Fog as a Service). Celle-ci se décline en plusieurs couches calquées sur la logique d'empilement du cloud (IaaS, PaaS et SaaS). Une architecture à laquelle s'ajoutent des éléments spécifiques au fog computing : des services d'interconnexion réseau, de collecte de données à partir des objets connectés, ou encore des applications de traitement plus spécifiques. Le principe de fonctionnement est ainsi le même que celui du cloud avec quelques particularités [14]

I.3.4 Les enjeux du Fog Computing pour les utilisateurs

- Le Fog Computing est un marché encore relativement nouveau, mais qui va croître en même temps que celui, déjà beaucoup plus connu, des objets connectés[15]
- Le Fog Computing offre des services déjà existants avec plus de fluidité, de stabilité et de rapidité, tout en bénéficiant d'une sécurité accrue, mais aussi de nouveaux services qui représentent le monde de demain[15]

I .3.5 Les avantages

La technologie Fog Computing présente des avantages considérables par rapport au cloud Computing. De nombreuses plates-formes IoT tirent plus d'avantages du Fog que du cloud [15] :

- .Quantité minimale de données envoyée au cloud.
- Économiser la bande passante
- Réduire la latence des données

- Améliorer la sécurité des données
- Traitement immédiat des données

I .3.6 Les inconvénients du fog computing

Comme toute technologie, les applications de fog Computing présentent également des inconvénients. Voici quelques-unes des limitations que vous devez prendre en compte avant de vous lancer [16] :

I .3.6.1 Risques liés à la sécurité et à la vie privée

Les grandes entreprises utilisent plusieurs appareils et il est presque impossible de tous les authentifier. Cela les rend vulnérables à diverses formes de cyberattaques si des protections adéquates ne sont pas en place. En fait, des personnes malveillantes peuvent accéder à vos nœuds en utilisant vos propres appareils contre vous.

Le fog computing soulève également des inquiétudes concernant la confidentialité des utilisateurs finaux. En fait, les nœuds collectent des informations sensibles à partir des appareils.

I .3.6.2 Consommation d'énergie

Les nœuds consomment beaucoup d'énergie pour fonctionner. Par conséquent, plus l'entreprise dispose de nœuds, plus la consommation d'énergie est importante. Cela peut être un défi à gérer pour certaines organisations.

I .3.6.3 Emplacement physique dangereux

L'emplacement est également l'un des points faibles du fog computing. En effet, en raison de la nature dispersée des nœuds, certains d'entre eux peuvent très probablement se situer dans des environnements moins sécurisés. Par conséquent, des acteurs malveillants peuvent facilement y accéder, ce qui augmente le risque d'attaques.

I. 3.6.4 Complexité du réseau

Le Fog Computing s'utilise généralement en tandem avec les ressources de réseautage et de cloud computing traditionnelles. La combinaison de ces technologies peut devenir très complexe à gérer. Cette architecture réseau complexe doit être maintenue et sécurisée contre les cyberattaques. Par conséquent, plus l'organisation est grande, plus la tâche devient difficile.

Conclusion

l'Internet des objets (IoT) est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution

Le cloud computing est un concept qui consiste à accéder à des données et services sur un serveur distant.

Le fog computing définit une infrastructure chargée de stocker et de traiter des données issues d'objets connectés. Concurrent direct, alternative ou solution complémentaire au cloud computing. Il a comme particularité de stocker et de traiter les données via le recours à des équipements implantés à la périphérie du réseau.

Les risques liés à la sécurité du cloud et fog sont nombreux y compris les attaques DoS nous présenterons ces attaques dans le chapitre suivant.

CHAPITRE

II

Introduction

La sécurité informatique est un terme générique qui s'applique aux réseaux, à Internet, aux points de terminaison, aux API, au cloud, aux applications, aux conteneurs, etc. Elle consiste à établir un ensemble de stratégies de sécurité qui fonctionnent conjointement pour vous aider à protéger vos données numériques.[17]

Le but de la sécurité informatique est de garantir la sécurité des accès et des utilisations des informations enregistrées dans les équipements informatiques, ainsi que du système lui-même, en se protégeant contre d'éventuelles attaques, en identifiant les vulnérabilités et en appliquant des systèmes de cryptage aux.[18]

le réseau sans fil présente de nombreux avantages, malgré de cela peut également conduire a de nombreux problèmes de sécurité. L'ouverture du support sans fil incite l'attaquant à obtenir l'accèsdes appareils du réseau. L'IoT n'a pas été sécurisé cardes normes 802.11 présente de graves vulnérabilités couche, cryptage et authentification en raison de la nature de la diffusion en communication.[19]

II.1 Les attaques DoS /DDOS

Figure II.1 : Daniel de service

[20]

II.1.1 Les attaque Dos

II.1.1.1 Définition Dos

Une attaque par déni de service (abr. DoS attack pour Denial of Service attack en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. [21]

II.1.1.2 Historique

Les attaques par déni de service ont commencé dans les années 1980, ce n'est qu'en Aout 1992 qu'aurait eu lieu la première attaque de déni de service distribué dirigée contre les serveurs de l'Université du Minnesota, à la suite de quoi l'accès Internet de l'Université est resté bloqué pendant plus de 2 jours. Historique des attaques de déni de service : En décembre 1996 a eu lieu l'attaque Ping de la mort (Ping Of Death).[22]

En juillet 1997, a eu lieu l'attaque Smurf qui, grâce à un serveur de diffusion (« broadcast »), duplique et envoie sur l'ensemble du réseau le message qu'il aura reçu de la machine attaquante. Par la suite, les machines du réseau répondent au serveur de diffusion qui redirigera ces réponses sur la machine cible.

Cette attaque fut suivie par l'attaque WinNuke qui provoquait un « blue screen » ou un « reboot » sur les postes Windows 95 et NT. En octobre de la même année a eu lieu l'attaque Land dont le principe est l'usurpation d'adresse IP dans le but d'exploiter une faille du protocole TCP/IP dans les systèmes visés. Cette attaque consiste donc à envoyer dans les champs sources et destination des paquets IP exactement la même adresse et le même numéro de port ce qui avait pour conséquence de déstabiliser ou de faire tomber les systèmes vulnérables tels que les systèmes Windows 95, 98, NT 4.O, Free BSD etc. ...

Enfin, en décembre 1997, a été appliquée l'attaque Teardrop / Over drop dont le principe est d'exploiter la fragmentation effectuée par le protocole IP (fragmentation des paquets, de taille trop importante, en plus petits paquets possédant tous un numéro d'identification et de séquence, à la réception, ils sont réassemblés grâce aux valeurs de décalage). On insère dans les paquets fragmentés de fausses informations de décalage qui, lors du réassemblage provoquaient des vides ou recoupements qui avaient pour conséquence une instabilité sur les stations Linux, Windows NT et 95. En janvier 1998, l'attaque Bonk/Boink qui visait les stations Windows 95 et NT 4.0. Le principe est d'émettre une grande quantité de paquets UDP corrompus provoquant des blocages ou des plantages du système d'exploitation

qui a été visé, suivie par l'attaque Fraggle qui inondait la cible de paquets UDP en utilisant une variante amplifiée de l'attaque Smurf. Suivit en juin 1998 de l'attaque Syndrop basée sur le Teardrop en TCP avec le bit SYN et possédant des champs invalides tels que le numéro de séquence par exemple. L'impact de cette attaque est le blocage les postes Windows NT4 SP3 par un Freeze (gèles, blocage). Le lundi 21 octobre 2002, une attaque de type Ping Flood bloque 9 des 13 serveurs DNS qui ont pour but le routage des requêtes de résolution de nom de domaine, rendant ainsi impossible l'accès à leurs ressources pendant trois heures. Les pirates ont pu grâce à un parc important de machines de générer un nombre de requêtes entre deux et trois fois supérieur à la capacité des treize serveurs visés.[23]

II.1.1.3 L'objectif principal d'une attaque DoS

L'attaque par déni de service, ou DoS (en anglais Denial of Service), vise à perturber, ou paralyser totalement, le fonctionnement d'un serveur informatique en le bombardant à outrance de requêtes erronées.[24]

II.1.1.4 Les attaques DoS appartiennent généralement à deux catégories

II.1.1.4.1 Attaques par débordement de tampon (buffer overflow)

Type d'attaque par débordement de tampon (Buffer overflow) débordement de tampon mémoire peut amener une machine à consommer tout l'espace disque dur, la mémoire ou le temps CPU disponibles. Cette forme d'exploitation se traduit souvent par un comportement lent, des pannes de système ou d'autres comportements délétères du serveur, entraînant un déni de service.[25]

II.1.1.4.2 Attaques par saturation (flood attacks)

En saturant un serveur ciblé avec une quantité énorme de paquets, un acteur malveillant est capable de sursaturer la capacité du serveur, ce qui entraîne un déni de service. Pour que la plupart des attaques par saturation DoS réussissent, l'acteur malveillant doit avoir plus de bande passante disponible que la cible[25]

II.1.1.5 Le principe de DoS

Envoyer une très grande quantité de paquets, dont la taille est relativement importante, en même temps, voire sur une longue période [26]

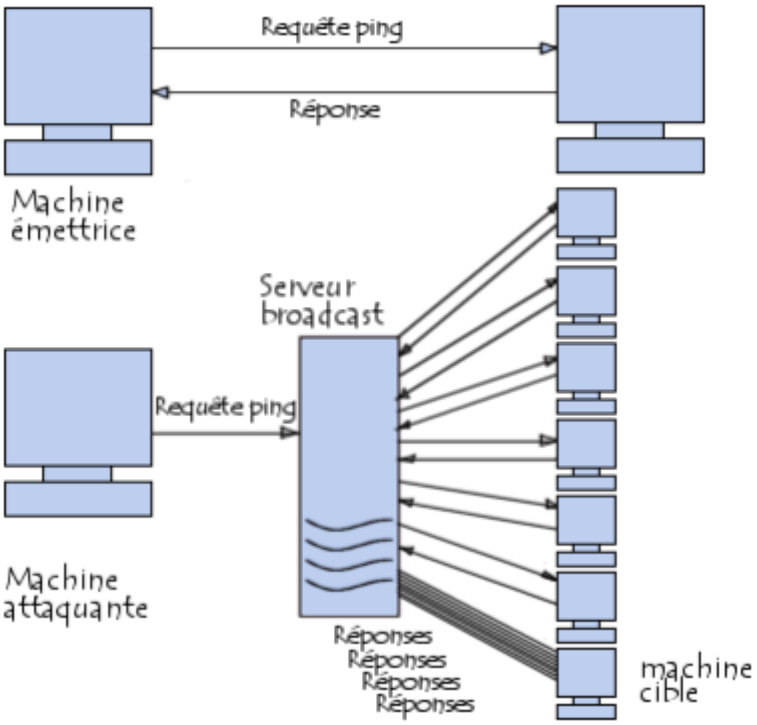


Figure II.2 : déni de service [23]

II.1.2 Les attaques DDOS

II.1.2.1 Définition

Une attaque par déni de service distribué (DDoS) est une tentative malveillante de perturber le trafic normal d'un serveur, service ou réseau ciblé en submergeant la cible ou son infrastructure environnante avec un flot de trafic Internet.

L'efficacité des attaques DDoS réside dans l'utilisation de plusieurs systèmes informatiques compromis comme sources de trafic hostile. Les machines exploitées peuvent être des ordinateurs et d'autres ressources situées sur le réseau, comme des appareils IdO.

En généralisant, une attaque DDoS ressemble à un embouteillage inattendu qui bloque une autoroute et empêche le trafic normal d'arriver à destination. [27]

II.1.2.2 Types d'attaques DDoS

Il existe de nombreux types d'attaques DDoS différents. On dénombre toutefois trois catégories principales**.**

II.1.2.2.1 Les attaques de trafic

Sont les plus courantes. Elles consistent à envoyer un immense volume de paquets TCP, UDP et ICPM à la cible. Ainsi, les requêtes légitimes sont perdues. Ces attaques peuvent être effectuées via l'exploitation de malwares. .[28]

II.1.2.2.2 Les attaques de bande-passante

Consistent à surcharger la cible de données inutiles. Ceci provoque une perte de bande-passante et des ressources nécessaires à son fonctionnement, provoquant un déni de service. [28]

II.1.2.2.3 les attaques d'application

consistent à envoyer des messages en grand nombre à l'application ciblée pour consommer ses ressources, rendant indisponibles les ressources du système cible. [28]

II.1.2.3 différence avec une attaque DoS et DDOS

Une attaque DoS (déni de service) est différente d'une attaque DDoS. Dans le cas d'une attaque DoS, en règle générale**,** un seul ordinateur et une seule connexion internet servent à inonder un système ou une ressource prise pour cible.

De son côté, l'attaque Distributed Denial of Service implique de nombreux ordinateurs **et** connexions internet pour inonder la source. Bien souvent, les attaques DDoS sont des attaques d'envergure mondiale, distribuées par le biais de botnets.[29]

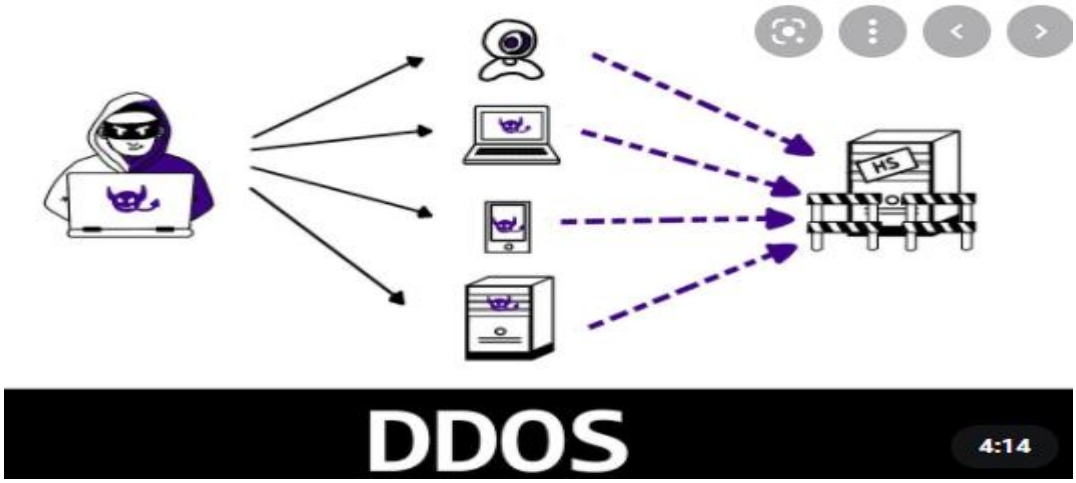


Figure II.3 : distribuer Daniel de service [30]

Dans notre travail, nous nous sommes appuyés sur les articles et suggestions d'autres chercheurs et avons essayé de les améliorer afin de détecter les attaques DoS

II .2 les articles pour la détection de DoS/DDoS

II.2.1 Détection des attaques DDOS dans le Cloud Computing

Le cloud computing est une technologie florissante et adoptée par de nombreuses entreprises. Cependant, cette évolution a rendu le système du cloud computing hautement vulnérable à plusieurs menaces de sécurité. Le cloud Computing l'un des techniques les plus évolué il prend de plus en plus sa place dans le monde car il fournit à un grand nombre d'utilisateurs des services performants et stockage de données évolutif.

Cependant cette évolution a rendu le système de cloud computing avec une sécurité très vulnérable surtout qu'il y a les menaces des attaques ddos. L'attaque DDoS est l'une des techniques de piratage les plus puissantes sur cloud. L'arme de base que le pirate utilise ces types d'attaques essentiellement pour consommer les ressources du cloud.

Ce travail effectué dans le cadre de ce mémoire vient répondre aux problèmes des attaques ddos dans le cloud computing et a pour objectif d'implémenter une solution intelligente de détection des attaques ddos via les différentes modèles du machine learning.

Ils ont pris l'initiative de présenter les différents concepts du cloud computing, pui son s'est concentrée sur les problèmes et les solutions de ces attaques. Dans ce contexte on a utilisé la dernière data set ddos pour faire un systéme de détection des attaques ddosa base machine learning où on à utiliser plusieurs algorithmes tell que l'arbre

de décision ,l'algorithme des K plus proches voisins, régression Logistique, gaussienne NB etc..[31]

II.2.2 Détection d'attaques sur les équipements d'accès à Internet

Les anomalies réseaux, et en particulier les attaques par déni de service distribuées, restent une menace considérable pour les acteurs de l'Internet. La détection de ces anomalies requiert des outils adaptés, capables non seulement d'opérer une détection correcte, mais aussi de répondre aux nombreuses contraintes liées à un fonctionnement dans un contexte industriel. Entre autres, la capacité d'un détecteur à opérer de manière autonome, ainsi qu'à fonctionner sur du trafic échantillonné sont des critères importants.

Au contraire des approches supervisées ou par signatures, la détection non-supervisée des attaques ne requiert aucune forme de connaissance préalable sur les propriétés du trafic ou des anomalies. Cette approche repose sur une caractérisation autonome du trafic en production, et ne nécessite l'intervention de l'administrateur qu'à postériori, lorsque une déviation du trafic habituel est détectée. Le problème avec de telle approches reste que construire une telle caractérisation est algorithmiquement complexe, et peut donc nécessiter des ressources de calculs conséquentes. Cette exigence, notamment lorsque la détection doit fonctionner sur des équipements réseaux aux charges fonctionnelles déjà lourdes, est dissuasive quant à l'adoption de telles approches.

Ce constat ils amène à proposer un nouvel algorithme de détection non-supervisé plus économe en ressources de calcul, visant en priorité les attaques par déni de service distribuées. Sa détection repose sur la création à intervalles réguliers d'instantanés du trafic,et produit des résultats simples à interpréter, aidant le diagnostic de l'administrateur. Ilsévaluent les performances de son algorithme sur deux jeux de données pour vérifier àla fois sa capacité à détecter correctement les anomalies sans lever de faux-positifs et sacapacité à fonctionner en temps réel avec des ressources de calcul limitées, ainsi que sur dutrafic échantillonné. Les résultats obtenus sont comparés à ceux de deux autres détecteurs,FastNetMon et UNADA.[32]

II.2.3 Détection d'intrusions dans le cloud computing

Le concept de système de détection d'intrusions a été introduit en 1980 par JamesAnderson, mais le sujet n'a pas eu beaucoup de succès. Il a fallu attendre la publication d'un modèle de d′détection d'intrusions par Denning [17] en 1987 pour marquer réellement led′épart 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 Etats-Unis a investi des millions de dollars dans ce type de recherches dans le but d'accroitre la sécurité de ses machines .Leur application a pour but le développement d'un IDS basé sur le comportement des clients (utilisateurs) cloud, ils vont essayer de placer l'IDS dans chaque nœud connectéau Cloud computing, ils ont 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. Son 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. Afin de développer son IDS, ils ont 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.[33]

Conclusion:

Le déni de service ou DoS (Denial of Service) est une attaque réseau qui empêche l'utilisation légitime des ressources d'un serveur en surchargeant celui-ci de requêtes. Les ordinateurs disposent de ressources limitées.

Les attaqueDDoS (Distributed Denial of Service) est une attaque informatique consistant à prendre pour cible un système informatique en l'inondant de messages entrants ou de requêtes de connexion afin de provoquer un déni de service. Découvrez tout ce que vous devez savoir à ce sujet

Dans notre travail, nous nous sommes appuyés sur des articles d'autres développeurs pour détecter les attaques DoS.

Nous avons proposons notre module de détection d'attaque DoS que nous présenterons dans le chapitre suivant .

CHAPITRE

III

Introduction

Actuellement, l'Internet des objets (IoT) a pour but d'interconnecter tout objet et toute personne via l'Internet. Selon l'estimation de Cisco. Avec une telle quantité de dispositifs finaux capables de détecter/agir sur l'environnement physique, l'IoT façonne les interactions futures entre l'homme et le monde. Cependant, ces objets génèrent aussi un volume de données important à traiter, ce qui nous incite à exploiter l'ensemble des ressources du réseau pas seulement ceux des objets.Le Fog computing étend les fonctionnalités du cloud computing à l'extrémité du réseau, plus rapproché des capteurs, des actionneurs et des périphériques IoT. Composé de périphériques variés dotés de différentes capacités de ressources, le fog permet de traiter les données localement (c'est-à-dire dans des périphériques plus proches des capteurs et des objets que le cloud), ce qui permet de réduire le temps de réponse des applications. De plus, les données volumineuses récoltées par des capteurs, peuvent être filtrées et agrégées via des analyses locales.

III.1Topologie

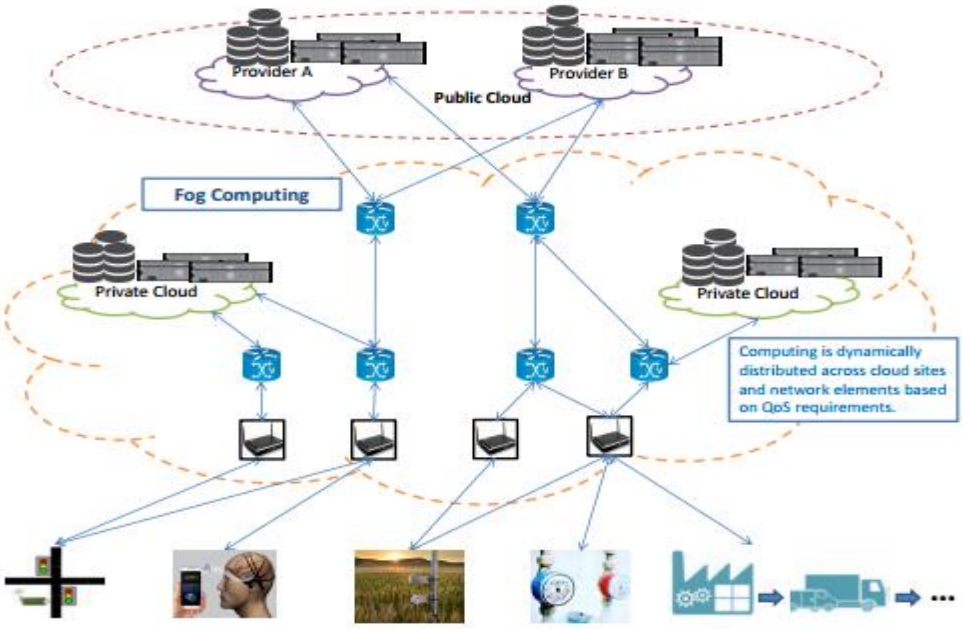


Figure III.1 : fog computung

Le fog computing, aussi appelé "informatique dans le brouillard", définit une infrastructure chargée de stocker et de traiter des données issues d'objets connectés. Concurrent direct, alternative ou solution complémentaire au cloud computing, le fog computing a comme particularité de stocker et de traiter les données via le recours à des équipements implantés à la périphérie du réseau. Il permet donc de réaliser ces deux actions en local, sans avoir à solliciter un datacenter situé à plusieurs centaines de kilomètres ou un cloud. Dans ce domaine du stockage et du traitement des données et de l'IoT, le fog computing crée une interface supplémentaire que l'on peut situer entre l'Edge Computing et le Cloud Computing. [34]

Les clouds fournissent généralement une partie de l'infrastructure réseau nécessaire à la connexion des objets IoT à Internet. Un équipement périphérique doit se connecter à un réseau pour simplifier la communication bidirectionnelle avec une base de données centralisée [35]

Avec le cloud computing, les données sont traitées et accessibles via Internet plutôt que sur un disque dur ou un serveur local. Cette technologie se caractérise par sa grande souplesse et des

coûts réduits en s'adaptant à la demande. Elle permet également aux utilisateurs d'accéder aux documents depuis n'importe quel endroit, à condition qu'ils aient accès au réseau via Internet

Avec le Fog Computing, toutefois, les données sont transmises du point de collecte à une passerelle pour y être traitées, puis renvoyées à la périphérie le Fog Computing agit comme un pont, réunissant le cloud et la périphérie.[36]

III.2Le module de détection et de prévention des attaques DoS proposé

Les attaque DoS sont des attaques qui ont pour but rendre une machine ou un réseau indisponible durant une certaine période. Elles peuvent paraitre sans danger si elles visent un réseau, mais peut s'avérer redoutable lorsqu'elles visent un serveur ou des ressources matérielles appartenant à une grande société dépendant de son infrastructure réseau. Le principe général des attaques DoS, implique l'envoie des donnes ou des paquets de taille ou de contenu inhabituel, ceci a pour but de provoquer des réactions inattendues du réseau, pouvant aller jusqu'à interruption du service.Pour détecter une attaque, il est indispensable de disposer de moyens de supervision de l'infrastructure, tant au niveau du réseau que des services opérés. La supervision permet de suivre l'évolution de la consommation des ressources, comme la bande passante et l'utilisation du processeur, mémoire ou encore l'espace disque. Des variations significatives constatées au niveau de la consommation au niveau de ces ressources peuvent indiquer un problème, et probablement un déni de service. Par exemple, Le trafic réseau peut être supervisé afin d'obtenir des informations sur les échanges réseau sous forme de flux décrits par les adresses IP source ou destination, les ports source ou destination et le protocole de transport utilisé ainsi que d'autres éléments caractéristiques du trafic. L'analyse des données collectées peut permettre de détecter des variations significatives de trafic et éventuellement des attaques.

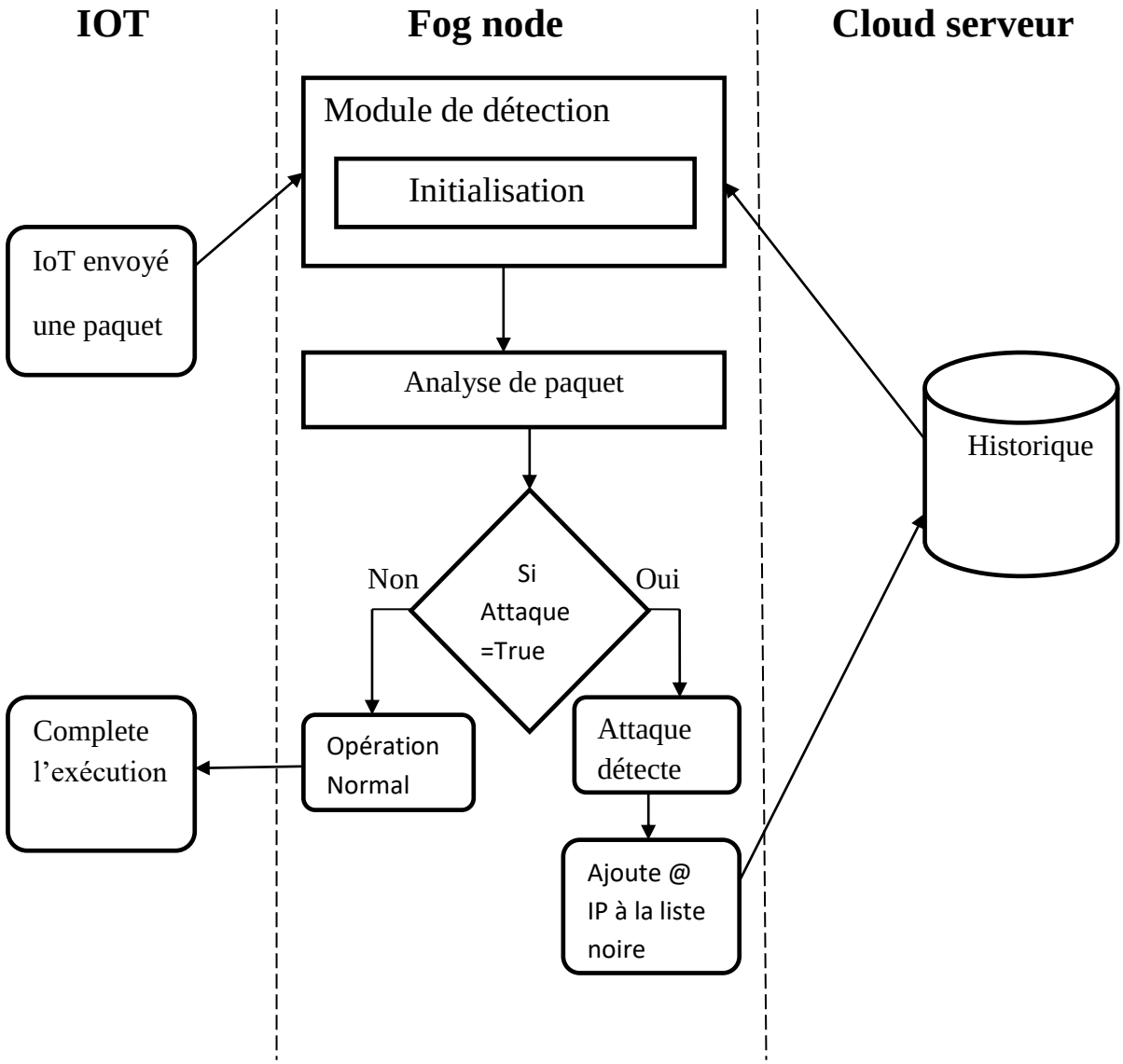


Figure III.2 : architecteur de notre proposition de détection

. La figure III.2 représente l'architecteur de notre module détection et de prévention des attaques DoS. Le module de détection et de prévention proposé sera mis en place dans la couche fog computing pour protéger le système contre les attaques externes. Le module proposé analyse les paquets du protocole TCP/IP arrivant sur la couche fog. Chaque fog dispose une liste qu'on a appelé une liste noire qui contient les adresses IPs des machines qui ont été bloqué. Quand un fog détecte une nouvelle attaque, il ajoute l'adresse IP de la machine source dans la liste noire et il informe la couche Cloud de cette attaque. Afin de prédire le blocage de ces attaquants, la couche Cloud, diffusent la nouvelle liste noire à tous les autres fog.

Dans l'IoT, les appareils sont plus vulnérables à diverses attaques, fournir un accès sécurisé est une tâche difficile. Surtout assurer la disponibilité du nœud et des services ont les plus

difficiles. L'attaque DoS est l'une des attaques dominantes pour contester la disponibilité des services au niveau de fog computing et cloud computing. Le principe général des attaques DoS, implique l'envoie des données ou des paquets de taille ou de contenu inhabituel, ceci a pour but de provoquer des réactions inattendues du réseau, pouvantaller jusqu'à interruption du service. La figure III.3 décrit le fonctionnement de notre modèle de détection des attaques DoS. Nous avons proposé deux algorithmes, le premier algorithme permet de détecter les attaques et le second pour mettre à jour la liste des adresses IP bloquées. Pour identifier l'attaque, l'analyseur de paquets enregistre l'adresse IP source dans une table temporaire et effectue une surveillance du nombre de paquets reçus. Nous avons défini une limite maximale (Un seuil) de paquets par intervalle de temps pour être considéré comme une attaque. Ainsi, un attaquant sera bloqué s'il atteint la limite imposée de paquets envoyés. Les adresses IP des attaquants sont bloquées au niveau du Fog et stockées dans une table contenant les adresses IP bloquées, appelée liste noire. La liste noire est mise à jour chaque fois que l'intervalle de temps défini se termine, cela permet de bloquer les IP qui tentent d'envoyer un grand nombre de paquets dans un petit intervalle de temps et aussi d'éviter qu'une machine victime d'usurpation d'IP soit bloqué définitivement. Nous avons défini aussi une taille de paquet maximale en octets, pouvant être reçu. Ainsi, si la taille des paquets reçus dépasse la limite établie, le paquet doit être rejeté et l'IP de la machine sera bloqué.

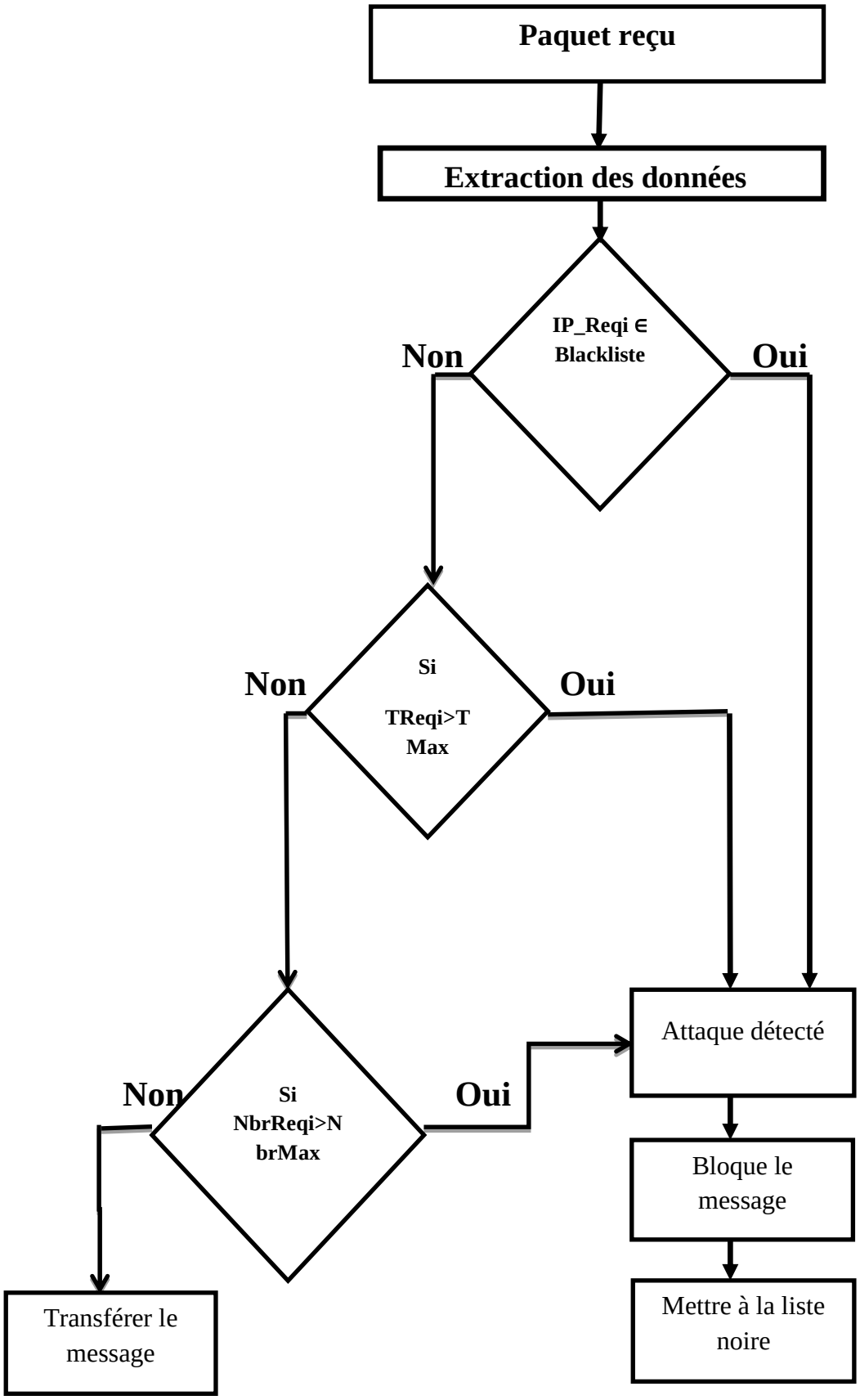


Figure III.3: l'organigramme de fonctionnement de notre modèle de détection

III.2.1 attaque check :

En entrée de l'algorithme, sont utilisées des données agrégées par flux caractérisés par le 5-tuple (IP_source, IP_destination, Port_source, Port_destination, P_rotocole), auxquels sont associées plusieurs métriques, telles que le nombre de paquets, et la taille en octets. Ces données sont enregistrées dans une liste temporaire. A l'arrivé d'une requête, si les données associées à cette requête ne se trouve pas dans la liste, une ligne caractérisée par le 5-tuple sera ajouté sinon le nombre de paquets est mis à jour. Dans le cas où l'adresse IP_source se trouve dans la liste noire, le paquet sera bloqué et la liste noire est mis à jour en exécutant l'algorithme 2. Si l'adresse IP_Source ne se trouve pas dans la liste noire, la taille du paquet est vérifiée si elle est inhabituelle le paquet sera rejeter et @ IP est ajouter à la liste noire. Si le nombre de paquet reçu pendant l'intervalle de temps T, dépasse la limite maximale autorisé, ce IoT est considéré comme malveillant, son IP_Source est ajoutée à la liste noire et les paquets arrivé de la part ce IoT seront rejeté

variable	Description
Req_i	le paquet ou la requête reçu de la part IoT *i*
$NbrReq_i$	le nombre de paquet reçu du même IoT *i*
IP Req_i	l'adresse IP du IoT *i*
TMax	la taille maximale autorisé pour une requête
NbrMax	le nombre de requêtes maximale autorisé pendant un intervalle de temps.

Table III.1 : la description de variable

Algorithme Attaque Check

Début

NbrReq$_i$++ // Incrémenter le nombre de requête reçu du même @IP
Si(*IP_Req$_i$ ∈ Blackliste****) alors***
    Bloquer Req$_i$;
Sinon
    Si(*TReq$_i$ > TMax****)* **alors**
        Ajoute IP_Req$_i$dans Blackliste ;
        BloquerReq$_i$;
    Sinon
        Si (*NbrReq$_i$ > NbrMax****)* **alors**
            Ajoute IP_Req$_i$ dans Blackliste ;
            BloquerReq$_i$;
        Fin
    Fin
Fin

Update(Blackliste) ;

Fin

III.2.2 mise à jour :

Le deuxième algorithme, s'exécute à intervalles régulier et il est invoqué par l'algorithme Attaque Check. A l'expiration de l'intervalle, update décrémente le nombre de requête pour adresse IP qui se trouve dans la liste noire, si le nombre de requête est égale à zéro, alors l'adresse IP est supprimé de la liste noire et le IoT peut envoyer des nouvelles requêtes. Cet algorithme permet d'éviter que les IoT restent bloqués définitivement et autorise les fogs à traiter leurs requêtes si leurs comportements redeviennent normaux.

Algorithme update

Début

Pour chaque *($IP_i \in Blackliste$)* **alors**
NbrReq$_i$ -- ;
Si(NbrReq$_i$=0***)alors***
Supprimer IP_i de Blackliste ;
Fin
Fin

Fin

Conclusion

Les attaques DoS sont aujourd'hui très répandues car elles sont assez simple à réaliser mais malgré ça elles peuvent mener à des conséquences désastreuses. En .en outre la détection et la prévention de ce genre d'attaques sont difficiles et quasiment tous les systèmes informatiques sont vulnérables. Pour cela nous avons proposé un module de détection et prévention des attaques DoS que nous avons présenté dans ce chapitre.

Le module proposé est basé sur deux algorithmes, le premier algorithme permet de détecter les attaques et le second permet de mettre à jour la liste des adresses IP bloquées. cette liste noire est utilisé comme un moyen de prévention des nouvelles attaques. Afin de rendre cette solution plus efficace, les Fog partagent leurs listes noires avec le Cloud et se dernier diffuse une liste globale à tous les autres Fogs. Afin d'évaluer notre solution, nous allons implémenté le module proposé dans le simulateur ifogSim, cette implémentation sera détaillée dans le chapitre suivant.

CHAPITRE IV

Introduction

Ce chapitre est consacré à la réalisation et l'implémentation de notre solution proposée pour la détection et la prévention des attaques DoS. Dans un premier temps nous présentons l'environnement de notre travail, puis nous détaillons le simulateur que nous avons utilisé, ensuit nous définissons le modèle de notre application, après nous citons les classes que nous avons modifié et nous présentons quelques interfaces graphiques, finalement nous présentons une série de simulation et leurs interprétations pour mettre en évidence notre solution.

IV.1 Langage et l'environnement de notre travail

Nous avons développé le simulateur sur une machine avec un processeur Intel(R) Pentium(R) CPU N3520 @ 2.16GHz 2.16 GHz, capacité mémoire de 4GB,sous Windows 10 64bit .Nous avons utilisé l'environnement de développement NetBeans IDE 8.0.2.

IV.1.1 Langage de programmation Java

Java est un langage de programmation orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au *SunWorld*.La société Sun a été ensuite rachetée en 2009 par la société Oracle qui détient et maintient désormais Java.

Une particularité de Java est que les logiciels écrits dans ce langage sont compilés vers une représentation binaire intermédiaire qui peut être exécutée dans une machine virtuelle Java (JVM) en faisant abstraction du système d'exploitation. [38].

IV.1.1.1 Les avantages de langage Java

- Java est facile à écrire et à exécuter.
- C'est la raison pour laquelle de nombreux développeurs l'utilisent.
- On peut l'utiliser pour créer des applications complètes qui peuvent s'exécuter sur un seul ordinateur.
- L'on a également la possibilité de les distribuer sur les serveurs et les clients d'un réseau.

- Il permet de créer facilement des applications mobiles ou exécuter sur des applications de bureau qui utilisent différents systèmes d'exploitation et serveurs, tels que Linux ou Windows. [39]

IV.1.2L'environnement de développement

NetBeans est un environnement de développement intégré (IDE) pour Java, placé en open source par Sun en juin 2000 sous licence CDDL (Common Développent and Distribution License). En plus de Java, NetBeans permet également de supporter différents autres langages, comme Python, C, C++, XML et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages web). NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X et Open VMS. NetBeans est lui-même développé en Java, ce qui peut le rendre assez lent et gourmand en ressources mémoires. [40]

IV.2 Simulateur IfogSim

IfogSim est conçu de manière à pouvoir évaluer les politiques de gestion des ressources applicables aux environnements Fog en ce qui concerne leur impact sur la latence (rapidité), la consommation d'énergie, la congestion du réseau et les coûts opérationnels. Il simule les appareils périphériques, les centres de données cloud et les liens réseau pour mesurer les mesures de performance. [41]

IV.2.1 Les principales classes d'iFogSim

Dans ce chapitre nous présentons les détails de quelques classes principales d'iFogSim et leurs interactions (figure IV.1).

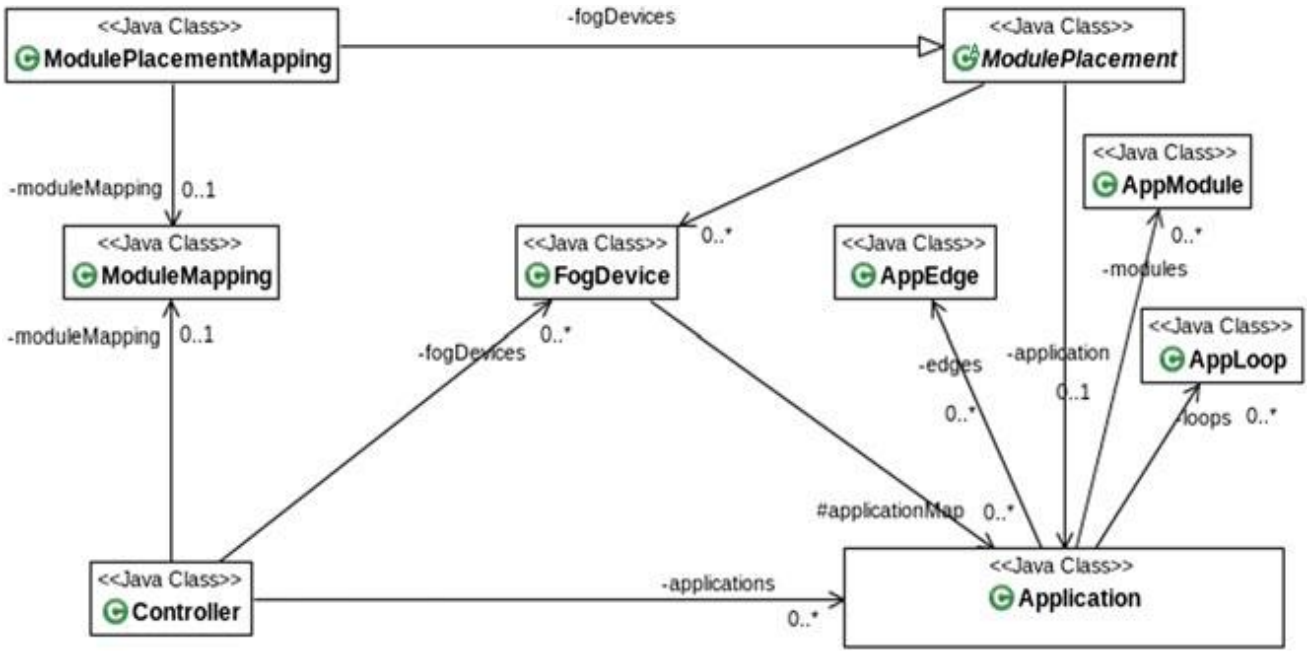


Figure IV.1 : Principales classes d'iFogSim

IV.2.1.1 FogDevice

Cette classe spécifie les caractéristiques matérielles des appareils Fog et leurs connexions à d'autres appareils, capteurs et actionneurs Fog. Réalisés par extension de la classe PowerDatacenter dans CloudSim, les attributs majeurs de la classe FogDevice sont la mémoire accessible, le processeur, la taille de stockage, les bandes passantes montantes et descendantes (définissant la capacité de communication des appareils Fog). Les méthodes de cette classe définissent la manière dont les ressources d'un périphérique Fog sont planifiées entre les modules d'application exécutés sur celui-ci et la manière dont les modules sont déployés et désactivés sur ceux-ci. Le remplacement de ces méthodes permet aux développeurs de plug-in des politiques personnalisées pour les fonctions mentionnées ci-dessus.

IV.2.1.2 Sensor

Les instances de la classe sensor sont des entités qui agissent comme des capteurs IoT décrits dans l'architecture. La classe contient des attributs représentant les caractéristiques d'un capteur, allant de sa connectivité aux attributs de sortie. La classe contient un attribut de référence à l'appareil passerelle Fog auquel le capteur est connecté et la latence de connexion entre eux. Plus important encore, il définit les caractéristiques de sortie du capteur et la distribution du temps inter-transmission ou inter-arrivée de tuple - qui identifie le taux d'arrivée de tuple à la passerelle.

IV.2.1.3 Tuple

Les tuples forment l'unité fondamentale de communication entre les entités dans le brouillard. Les tuples sont représentés comme des instances de la classe Tuple dans iFogSim, qui est héritée de la classe Cloudlet de CloudSim. Un tuple est caractérisé par son type et les modules d'application source et destination. Les attributs de la classe spécifient les exigences de traitement (définies en millions d'instructions (MI)) et la longueur des données encapsulées dans le tuple.

IV.2.1.4 Actionneur

Cette classe modélise un actionneur en définissant ses propriétés de connexion réseau. Un attribut de la classe fait référence à la passerelle à laquelle l'actionneur est connecté et à la latence de cette connexion. La classe définit une méthode pour effectuer une action à l'arrivée d'un tuple d'un module d'application.

IV.2.1.5 Application

Une application est modélisée sous la forme d'un graphe orienté, les sommets du DAG représentant les modules qui effectuent le traitement des données entrantes et les arêtes indiquant les dépendances de données entre les modules. Ces entités sont réalisées à l'aide des classes suivantes :

IV.2.1.5.1AppModule

Les instances de la classe AppModule représentent les éléments de traitement des applications Fog. AppModule est implémenté en étendant la classe PowerVm dans CloudSim. Pour chaque tuple entrant, une instance AppModule le traite et génère des tuples de sortie qui sont envoyés aux modules suivants dans le DAG. Le nombre de tuples de sortie par tuple d'entrée est décidé à l'aide d'un modèle de sélectivité - qui peut être basé sur une sélectivité fractionnaire ou un modèle en rafales.

IV.2.1.5.2 AppEdge

Une instance AppEdge indique la dépendance des données entre une paire de modules d'application et représente un bord dirigé dans le modèle d'application. Chaque arête est caractérisée par le type de tuple qu'elle transporte, qui est capturé par l' attribut tupleType de la classe AppEdge ainsi que les exigences de traitement et la longueur des données encapsulées dans ces tuples. IFogSim prend en charge deux types de bords d'application - périodiques et basés sur des événements. Les tuples sur un AppEdge périodique sont émis à intervalles réguliers. Un tuple sur un bord basé sur des événements=*(tu, v)*est envoyé lorsque le module source*tu* reçoit un tuple et le modèle de sélectivité de*tu*permet l'émission de tuples portés pare

IV.2.1.5.3AppLoop

AppLoop est une classe supplémentaire, utilisée pour spécifier les boucles de contrôle de processus qui intéressent l'utilisateur. Dans iFogSim, le développeur peut spécifier les boucles de contrôle pour mesurer la latence de bout en bout. Une instance AppLoop est fondamentalement une liste de modules commençant à l'origine de la boucle jusqu'au module où la boucle se termine.

IV.2.2 Les classes modifier

Nous avons modifié dans les classes **FogDivece**, **Sensor**, **Tuple**, **Application**

- **FogDivece :**dans cette classe nous créons une méthode **processupdateblackliste ( )** qui fait la mise ajour de la liste noire chaque 10 secondes et on ajoutons dans la méthode **processTupleArrival ()** notre proposition de détection.
- **Sensor** : dans cette classe nous ajoutons dans la méthode transmit () le paquet qui contient l'adresse IP source et destination et le protocole utilisé « TCP »
- **Tuple :**dans cette classe nous ajoutons les attribues paquet, size et nous insérons leurs codes
- **Application :** dans cette classe nous ajoutons dans la méthode **getResultantTuples()** deux tuples (tuple. getpaquet , tuple.getsize).

IV .3 Modèle d'application

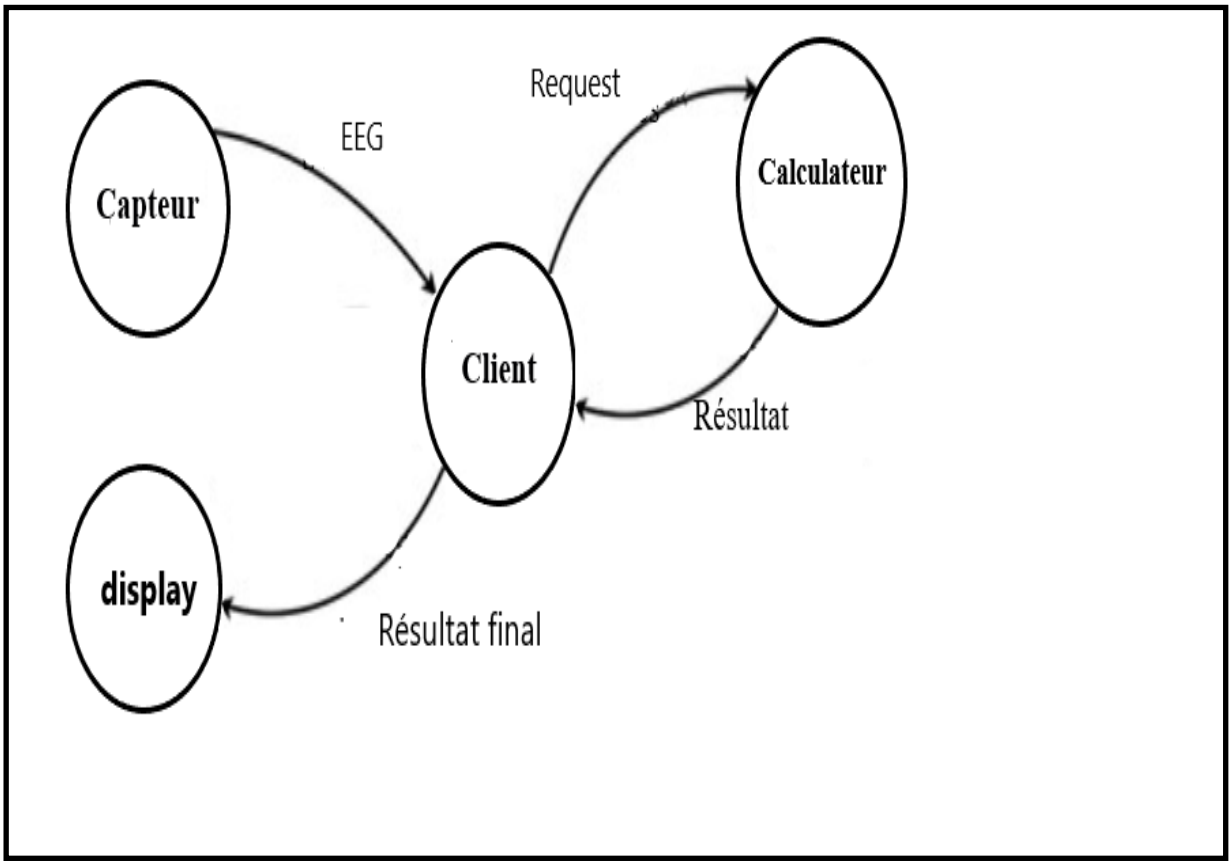


Figure IV.2: Modèle d'application d'our app

Nous avons défini un modèle simple pour notre application, notre modèle se compose de deux module, module Client et module Calculateur, le module Client est déployé sur le mobile et le module Calculateur est mis en place au niveau du Fog; Le module client collecte des données à partir d'un capteur et fait un prés traitement avant de l'envoyé au module Calculateur. Le module Calculateur traite les données reçues de la part du mobile et les résultats de ce traitement sont ensuite envoyé au module Client afin de les affiché via l'affichage du mobile (display).Les modules d'application sont modélisés dans iFogSim à l'aide de la classe AppModule.Les dépendances entre les modules sont modélisées à l'aide de la classe AppEdge dans iFogSim

IV.4 Diagramme de séquence

Le diagramme de séquence est l'un des vues dynamiques les plus importantes d'UML.La figure IV.3illustre le diagramme de séquence de traitement d'une requête sans attaque. Un IoT fait un prés traitement sur les données collectées à partir de son capture ensuite il envoie une requête au Fog qui se trouve dans la même région. Quand le fog reçoit cette requête, il analyse le paquet en utilisant l'algorithme 1, si aucune menace n'est détectée, il traite cette requête et ensuite le résultat est envoyé au mobile. Dans le cas où le Fog détecte une attaque (figure IV.4), il va bloquer cette requête et il va ajouter l'adresse IP source de cette requête à la liste noir. Le fog va informer le Cloud de la présence d'une attaque, le Cloud va mettre à jour la liste noire et il va diffuser cette nouvelle liste à tous les autres Fog qui vont l'utilisé afin de bloquer les attaques du même mobile

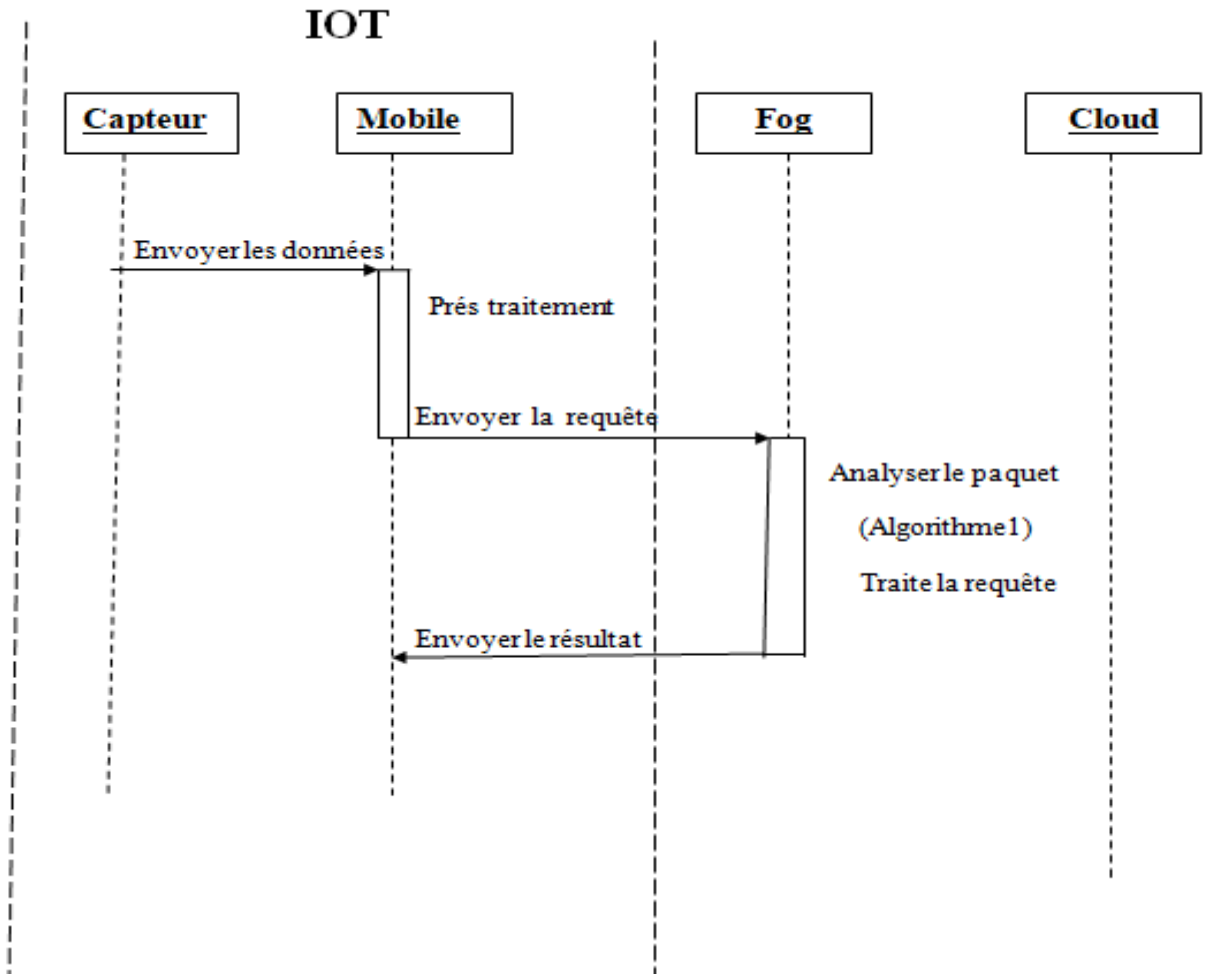


Figure IV.3 : diagramme de séquence sans attaque

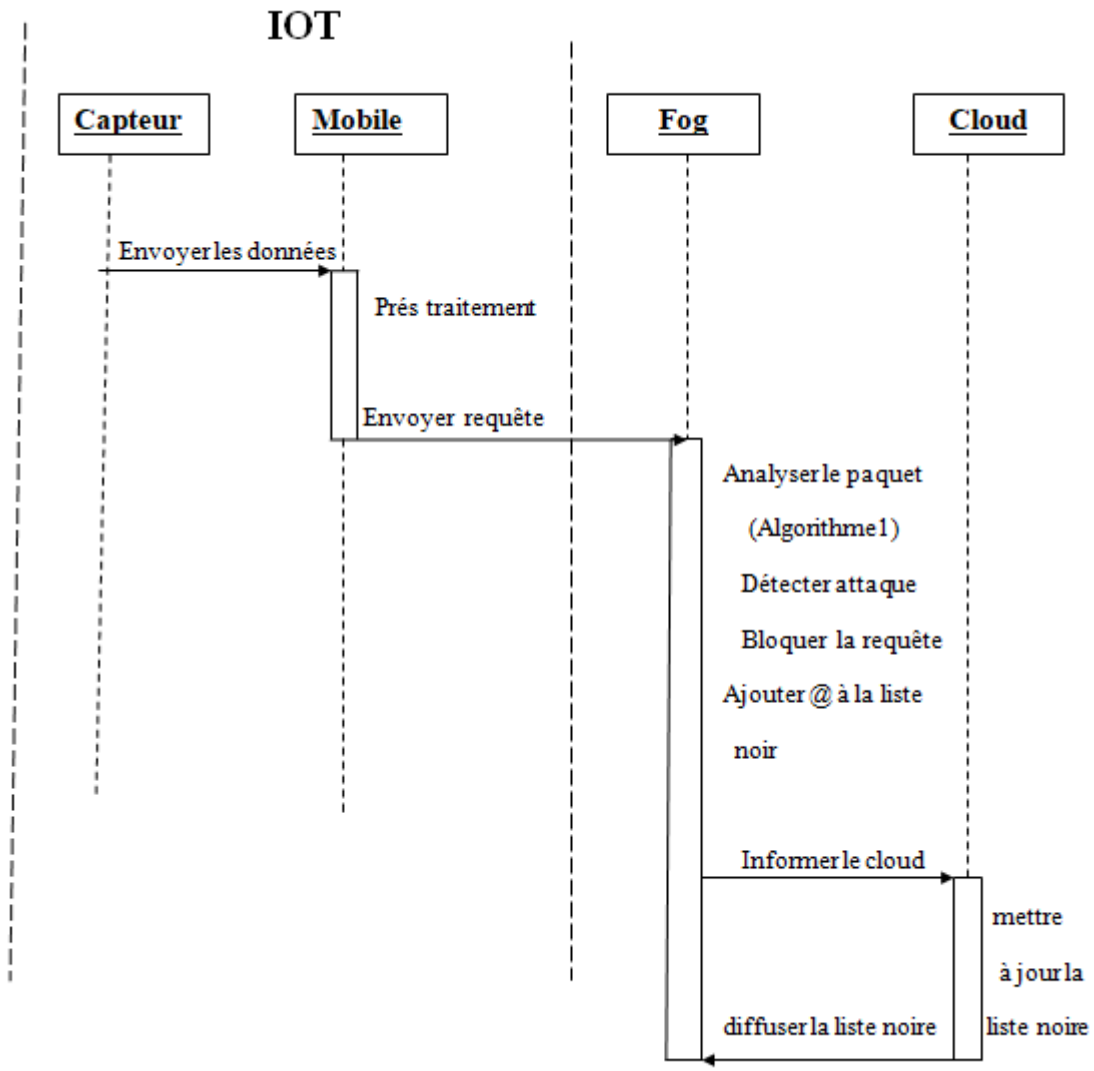


Figure IV .4 : diagramme de séquence avec attaque

IV.4L'interface

Le simulator IfogSim n'pas une interface graphique, la configuration et l'exécution se fait sur console ,Nous avons créé une interface qui facilite l'accès au simulateur .Les figures (4.5,4.6) montrent les fenêtres de configuration différents paramètres nécessaire à la simulation de notre solution. Notre interface, contient deux parties principales :

IV.4.1 FogDivece

Dans la fenêtre représentée par la figure IV.5, nous pouvons entrer les paramètres nécessaires à la création d'un Fog. Ces paramètre sont: le nom du fog, la RAM, la bande passante up , la bande passant down et le MIPS. La configuration des différents paramètres du Cloud se fait aussi dans cette fenêtre.

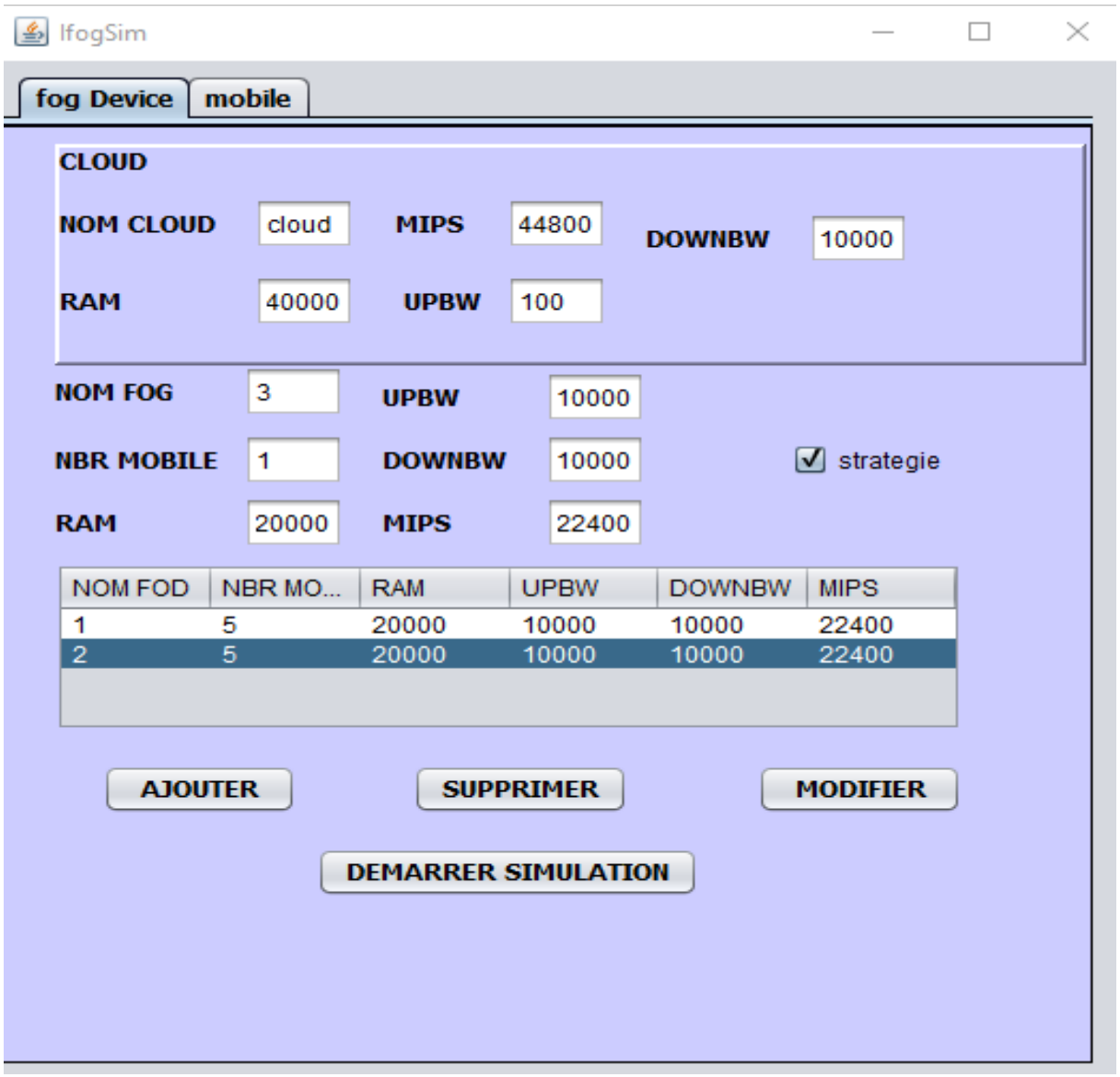
Nous avons créé des boutons :

1-Bouton ajoute : permet d'ajouter les paramètres de chaque fog dans un tableau.

2-Bouton supprime : ce bouton permet la suppression du Fog sélectionné.

3-Bouton modifier : pour faire la modification des paramètres d'un fog séléctionné.

4-Bouton démarrer simulation : Ce bouton est très important dans notre interface, il fait appel à toutes les méthodes pour créer l'environnement et de démarrer la simulation.



FigureIV.5 : interface FogDivece

IV.4.2Mobile

Cette fenêtre représente l'interface de création d'un mobile. Elle permet de configurer les paramètres nécessaires pour la création du mobile (figureIV.6) comme : nom de mobile, le nom de fog à lequel ce mobile est lié, la RAM, la taille des paquet des différents requête envoyé par ce mobile, le nombre de requêtes qui vont être envoyé par ce mobile, la bande passante up , la bande passant down et MIPS.

Nous avons créé des boutons

1-Bouton ajoute : Afin d'ajouter les paramètres de chaque mobile dans le tableau.

2-Bouton supprime : ce bouton permet la suppression d'un mobile.

3-Bouton modifier : Permet la modification des paramètres d'un mobile.

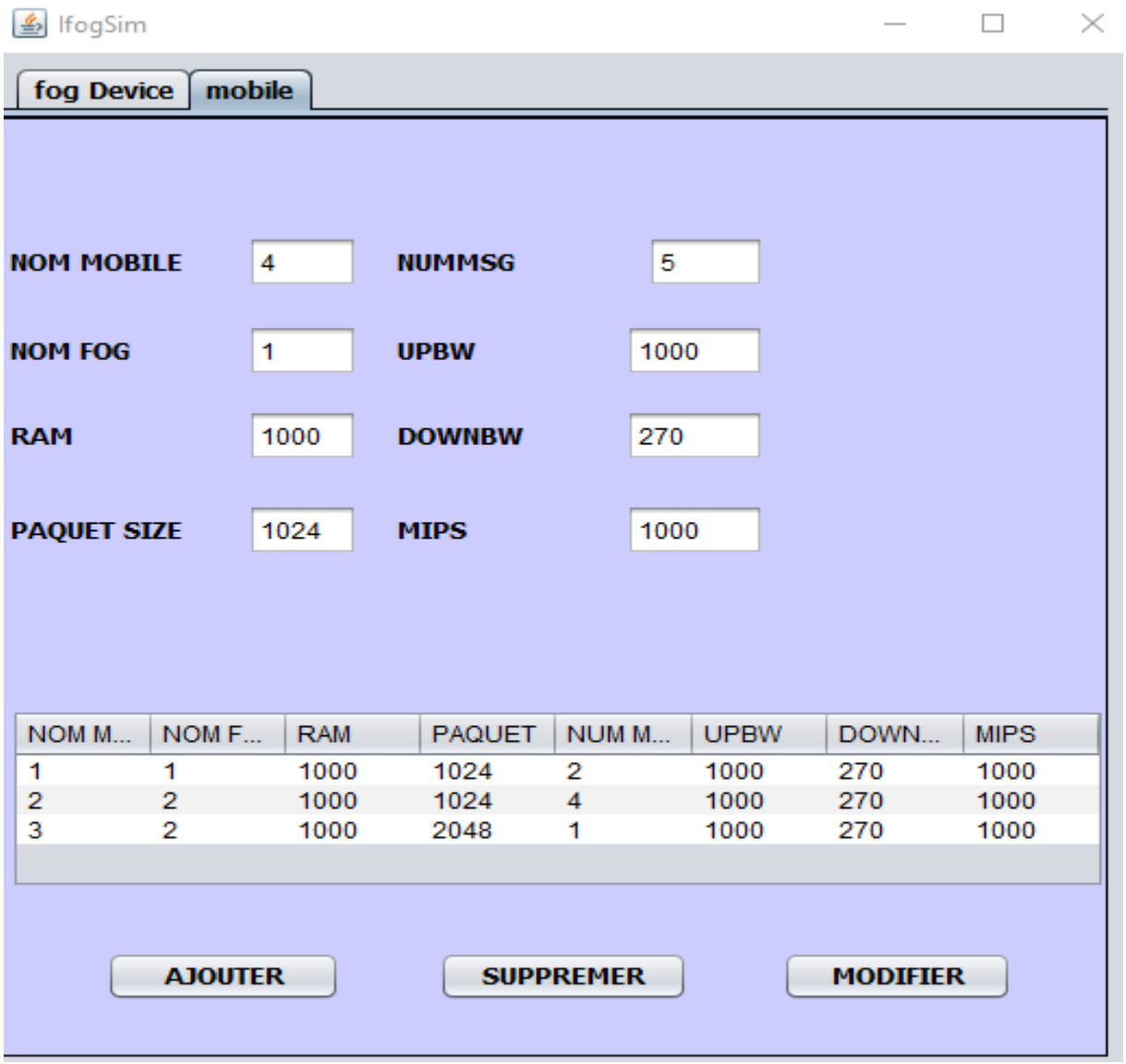


Figure IV.6: interface mobile

IV.5 Résultats expérimentaux

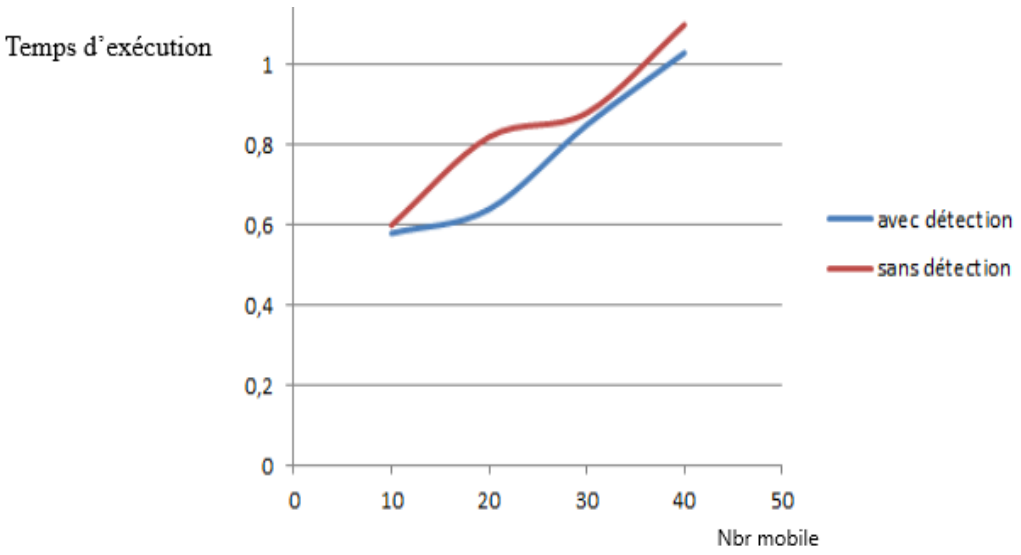
Afin de valider et d'évaluer notre module de détection et de prévention des attaques Dos, nous avons effectué une série d'expérimentation dont les résultat et les interprétation sont présenté dans cette section.

IV.5.1 Expérience 1 : temps d'exécution

Dans cette première simulation nous avons mesuré le temps d'exécution moyen pour les requêtes des utilisateurs avec détection des attaques et nous l'avons comparé avec le temps d'exécution des requêtes des utilisateurs sans la détection des attaques. Cette simulation a été réalisée avec les paramètres suivant : un cloud, deux fog et quarante mobiles. Les résultats de cette simulation sont présentés dans la figure IV.7, nous remarquons que le temps d'exécution avec détection des attaques est inférieur au temps d'exécution sans détection, ce résultat permet de confirmer notre proposition.

Nombre de mobile	10	20	30	40
Avec détection	0.58	0.64	0.85	1.03
Sans détection	0.6	0.82	0.88	1.10

Tableau IV.1 : temps d'exécution avec et sans détecter des attaques



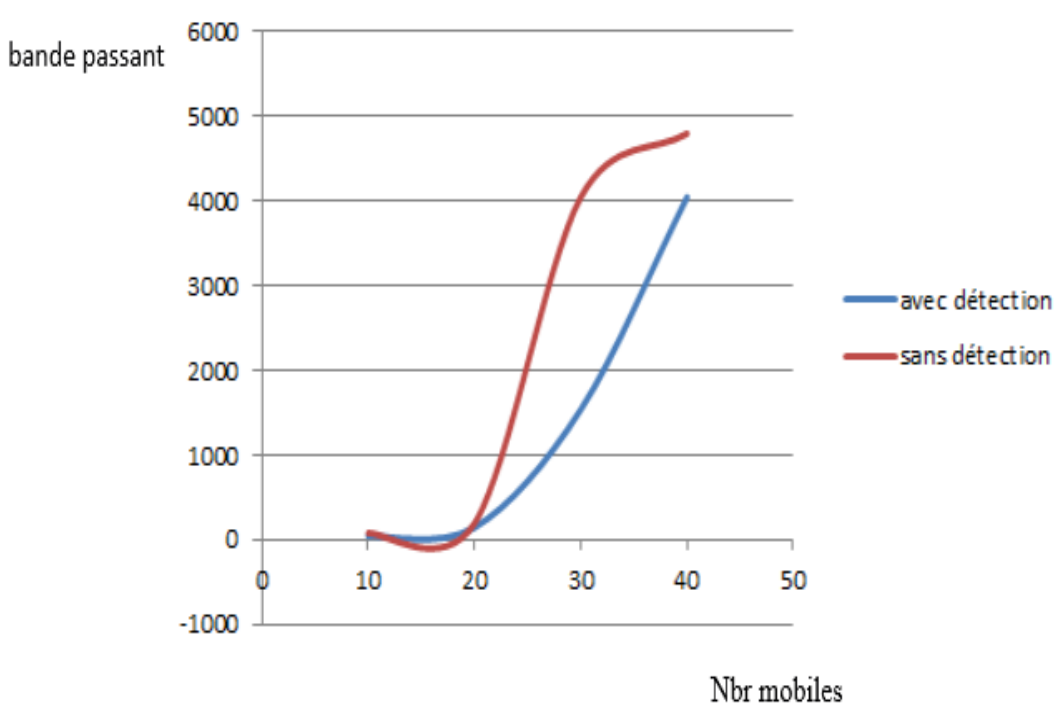
FigureIV.7 : temps d'exécution avec et sans détecter des attaques

IV.5.2 Expérience 2 : la bande passante

La seconde série d'expérimentation consiste à étudier l'utilisation de la bande passante dans le fog dans le cas de détection des attaques et dans le cas sans détection d'attaque. Les résultats de cette simulation sont montrés dans la figure IV.8. Nous remarquons que l'utilisation de la bande passante avec détection des attaques est inférieur à l'utilisation de la bande passante sans détection des attaques.

Nombre de mobile	**10**	**20**	**30**	**40**
Avec détection	44	144	1537.5	4045.5
Sans détection	65	192.5	1834.5	4795

Tableau IV.2 : L'utilisation de la bande passante avec et sans détecter des attaques



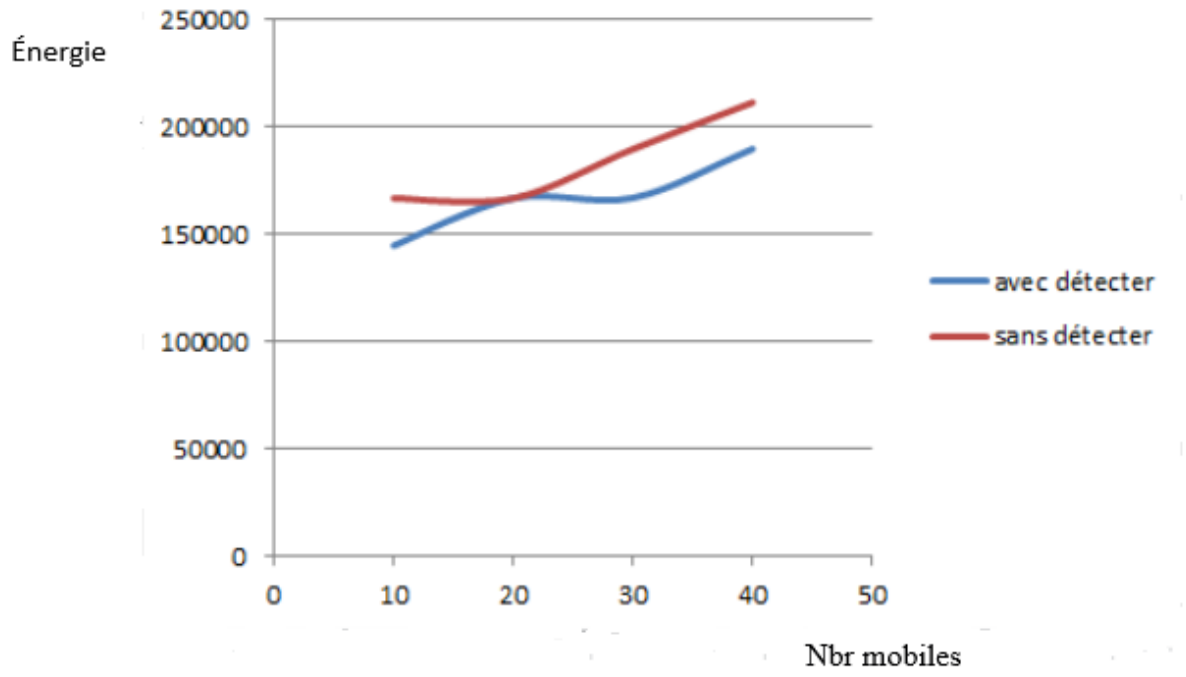
FigureIV.8 : L'utilisation de la bande passante avec et sans détecter des attaques

IV.5.2) Expérience 2 : Énergie

Dans la dernière simulation nous avons mesuré l'énergie consommé par les fogs dans les deux situation avec et sans détection des attaques. La figureIV.9 représente les résultats obtenu de cette série de simulation. Nous trouve dans le cas d'absence de détection d'attaqué, l'énergie consommé par les fog est plus importante que le cas avec de détection.

Nombre mobile	10	20	30	40
Avec détection	144866	166866.59	167090.83	189863.54
Sans détection	166866	166866	189819.65	211494.69

Tableau IV.3 :l'énergie de fog avec et sans détecter des attaques



FigureIV.9 : L'énergie de fog avec et sans détecter des attaques

Conclusion

IfogSim permet la modélisation et la simulation du calcul du fog pour évaluer les politiques de gestion et de planification des ressources sur les ressources de périphérie et de cloud dans différents scénarios.

Dans ce chapitre nous avons lancé plusieurs séries de simulation afin d'évaluer l'efficacité de notre module proposé, nous avons remarqué à partir de l'interprétation des résultats de simulation que le temps d'exécution, l'utilisation de la bande passante et l'énergie ont été largement réduit par notre module de détection et de prévention d'attaque.

Conclusion générale:

La sécurité informatique consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système d'information. Avec l'essor d'internet, les menaces visant les systèmes d'informations n'ont cessés d'augmenter et de se sophistiquer, faisant aujourd'hui de la sécurité informatique une nécessité pour tous les types de structure.

Les attaques DoS sont des attaques dominantes pour contester la disponibilité des services au niveau du fog computing et du cloud computing.

Dans ce travail. Nous avons proposé un module de détection et de prévention des attaques DoS, notre module est basé sur deux algorithmes, le premier algorithme permet de détecter les attaques et le second permet de mettre à jour la liste des adresses IP bloquée, cette liste est nommé liste noire, elle est utilisée comme un moyen de prévention des nouvelles attaques. Afin de rendre la prévention plus efficace, nous avons ajouté le partage des adresses bloqué entre le Cloud et les Fog. Nous avons étendu le simulateur iFogSim afin d'implémenter notre module. Pour évaluer notre proposition, nous avons lancer plusieurs séries de simulation. Nous avons remarqué à partir des résultats de simulation obtenus que le temps d'exécution moyen, l'utilisation de la bande passante et l'énergie consommé par les fog, ont été réduit par notre module de détection qui bloque les différent attaques.

BIBLIOGRAPHIE

[1] A. Kulkarni, S. Sathe (2014). Healthcare applications of the Internet of Things: A Review. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6229-6232.

[2] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015).Internet of things: A survey on enabling technologies, protocols, and applications.IEEE Communications Surveys & Tutorials, 17(4):2347–2376.

[3] Aldaej, A. (2019). Enhancing cyber security in modern internet of things (iot) using intrusion prevention algorithm for iot (ipai). IEEE Access, pages 1–1.

[4] Dragomir, D., Gheorghe, L., Costea, S., and Radovici, A. (2016). A survey on secure communication protocols for iot systems. In 2016 International Workshop on Secure Internet of Things (SIoT), pages 47–62.

[5] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6):599–616.

[6] Mell, P., Grance, T., et al. (2011). The nist definition of cloud computing).

[7] P. Sempolinski, D. Thain. (2010). A comparison and critique of eucalyptus,opennebula and nimbus. In Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science , CLOUDCOM '10, pages 417_426, Washington, DC, USA, 2010. IEEE Computer Society

[8] Vivansas.p.r.l (septempre2009) .Cloud Computing Enjeux, Perspectives et Impacts métiers

[9] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang, Q. Li. (2009). Comparisonof several cloud computing platforms. In Proceedings of theSecond International Symposium Information Science and Engineering , ISISE '09, pages 23_27, Washington,DC, USA,. IEEE Computer Society.

[10] Z. Ye, X. Chen, and Z. Li. (2010) "Video based mobile location search with large set of SIFT points icloud," in Proceedings of the 2010 ACM multimedia workshop on Mobile cloud media computing (MCMC),.

BIBLOIGRAPHIE

[11] Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N. S., and Mahmoudi, C. (2018). Fog computing conceptual model. Technical report

[12] Bonomi, F., Milita, R., Zhu, J. et Addepalli, S. (2012). Fog computing and its role in the internet of things. Dans Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, MCC '12, 13-16., New York, NY, USA.ACM

[13] Bellavista, P. et Zanni, A. (2017). Feasibility of fog computing deployment based on docker containerization over raspberrypi. Dans Proceedings of the 18th International Conference on Distributed Computing and Networking, ICDCN'17, 16 :1-16 :10., New York, NY, USA. ACM.

[14] Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pages 13–16. ACM.

[15] F. Bonomi, al (2012). “Fog computing and its role in the internet of things”. In : Proceedings of the first edition of the MCC workshop on Mobile cloud computing., p. 13-16.

[16] Shanhe Yi , al. (2015). “Fog computing : Platform and applications”. In : 2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb). IEEE., p. 73-78.

[17]Frustaci, M., Pace, P., Aloi, G., and Fortino, G. (2018). Evaluating critical security issues of the iot world: Present and future challenges. IEEE Internet of Things Journal, 5(4):2483–2495.

[18] Maphats’oe, T. and Masinde, M. (2016). A security algorithm for wireless sensor networks in the internet of things paradigm. In 2016 IST-Africa Week Conference, pages 1–10.

[19] Nikam, A. and Ambawade, D. (2018). Opinion metric based intrusion detection mechanism for rpl protocol in iot. In 3rd International Conference for Convergence in Technology (I2CT), pages 1–6.

[20] A. Chonka . J. Abawajy. (Sept 2012). Detecting and mitigating hx-dos attacks against cloudweb services. In Network-Based Information Systems (NBiS), 2012 15th International Conference on, pages 429–434,.

[21] N. Gruschka . N. Luttenberger. (2006) Protecting web services from dos attacks bysoap message validation. In in Proceedings of the IFIP TC11 21 International Information Security Conference (SEC).

[22] Kasinathan, P., Pastrone, C., Spirito, M. A., and Vinkovits, M. (2013). Denial-of-service detection in 6lowpan based internet of things. In 2013 IEEE 9th International Conference on Wireless an Mobile Computing, Networking and Communications (WiMob), pages 600–607.

[23] U.D.Gandhi, R.V.S.M Keerthana . (2014)"Request Response Detection Algorithm for Detecting DoS Attack in V ANET", International Conference on Reliability, Optimization and Informatio Technology, MRIU, India, Feb 6-8 2014. Electronic ISBN: 978-1-4799-2995-5.

[24] S. Roselinmary, M. Maheshwari, M. Thamararaiselvan. (2013). « Early Detection of DOS Attacks in V ANET U sing Attacked Packet Detection Algorithm (APDA) ». Information Communication and Embedded Systems (ICICES),x International Conference, 21-22 Feb. 2013, Electronic ISBN: 978-1-4673-5788-3.

[25] L. He, W.T Zhu. (2012) « Mitigating DOS Attacks against Signature-Based Authentication in V ANETs », IEEE International Conference on Computer Science and Automation Engineering (CSAE). Electronic ISBN: 978-1-4673-0089-6

[26] K. Verma, H. Hasbullah, A. Kumar. (2013). «An Efficient Defense Method against UDP Spoofed Flooding Traffic of DeniaI of Service (DOS) Attacks in V ANET », 978-1-4673-4529-3/$31.00. Advance Computing Conference(IACC), 22-23 Feb. 2013 IEEE 3rd International. Electronic ISBN: 978-1-4673-4529-3.

[27] B. Wang, Y. Zheng, W. Lou, Y.T. Hou (2014). Ddos attack protection in the era of cloud computing and software-defined networking. In Network Protocols (ICNP), IEEE 22nd International Conference on, pages 624–629, Oct 2014.

[28] S. Yu, Y. Tian, S. Guo, D.O. Wu. (2014). Can we beat ddos attacks in clouds ? Parallel and Distributed Systems, IEEE Transactions on, 25(9) :2245–2254, Sept 2014.

[29] S.Zhao, K.Chen, W.Zheng. (2009). Defend against denial of service attack with vmm. In Grid and Cooperative Computing, GCC ’09. Eighth International Conference on, pages 91–96, Aug 2009.

[30] A.M.Malla, I.V.Sahu « Security attacks with an effective solution for DOS attacks in V ANET ». International Journal of Computer Applications (0975 - 8887) Volume 66- No.22, March 2013.

[31] K. A. Jackson, al. (1999). Intrusion detection system (ids) product survey. Los Alamos National Laboratory

[32] K. Scarfone, P. Mell. (2012). Guide to intrusion detection and prevention systems (idps). Technical report, National Institute of Standards and Technology.

,[33] K.P Soman, M. Alazab, al. (2020). A comprehensive tutorial and survey of applications of deep learning for cyber security.

[34] Alrawais, A., Alhothaily, A., Hu, C., and Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 21(2):34–42..

[35] Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7):1497–1516

[36] Lu, Y. and Xu, L. D. (2019). Internet of things (iot) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2):2103–2115.

[37] Shafi, Q., Basit, A., Qaisar, S., Koay, A., and Welch, I. (2018). Fog-assisted sdn controlled framework for enduring anomaly detection in an iot network. IEEE Access, PP:1–1.

[38] J.M Dououx. (1999). : Développons en Java v 2.00 Copyright (C) 1999-2014 Jean-M ichel DOUDOUX

[39] Vikram, N., Harish, K. S., Nihaal, M. S., Umesh, R., Shetty, A., and Kumar, A. (2017). A low cost home automation system using wi-fi based wireless sensor network incorporating

[40] Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). Ddos in the iot: Mirai and other botnets. Computer, 50(7):

[41] P. Kabiri, A. A. Ghorbani. (2005). Research on intrusion detection and response: A survey. IJ Network Security.

ملخص

إن إنترنت الأشياء وحوسبة الضباب هي تقنيات مستخدمة حاليًا في العديد من المجالات. حقيقة أن هذه البيئات متصلة بالإنترنت تجعلها عرضة للتهديدات المختلفة ، مثل هجمات رفض الخدمة (DoS). في هذا العمل. لقد اقترحنا وحدة لاكتشاف الهجمات ومنعها من DoS، وتستند الوحدة الخاصة بنا إلى خوارزميتين ، ولتقييم اقتراحنا ، قمنا بتوسيع محاكي iFogSim الذي قمنا فيه بتنفيذ الوحدة النمطية الخاصة بنا ، وأطلقنا عدة سلاسل من عمليات المحاكاة. تظهر نتائج المحاكاة أنه تم تقليل متوسط وقت التنفيذ واستخدام النطاق الترددي والطاقة التي تستهلكها الضباب.

Abstract

The Internet of Things and Fog Computing are technologies currently used in many fields. The fact that these environments are connected to the Internet makes them vulnerable to various threats, such as denial of service (DoS) attacks. In this work. We have proposed a DoS attack detection and prevention module, our module is based on two algorithms, To evaluate our proposal, we have extended the iFogSim simulator in which we have implemented our module, we have launched several series of simulations. The simulation results show that the average execution time, band width usage and energy consumed by the fogs have been minimized.

Résumé

L'Internet des objets et le Fog Computing sont des technologies actuellement utilisées dans de nombreux domaines. Le fait que ces environnements soient connectés à Internet les rend vulnérables à diverses menaces, telles que les attaques par déni de service (DoS). Dans ce travail. Nous avons proposé un module de détection et de prévention des attaques DoS, notre module est basé sur deux algorithmes, Pour évaluer notre proposition, nous avons étendu le simulateur iFogSim dans lequel nous avons implémenter notre module., nous avons lancé plusieurs séries de simulation. Les résultats de simulations montrent que le temps d'exécution moyen, l'utilisation de la bande passante et l'énergie consommée par les fog, ont été minimisés .

.