REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ Tahar Molay Saida

Faculté des Sciences et Technologie

Département des mathématiques et Informatique

Projet de fin d'étude présenté en vue de l'obtention du diplôme de

Master

Domaine : mathématiques et Informatique

Spécialité : Informatique

Thème

La protection des données personnelles des systèmes basés sur l'internet des objets

Présenter par : ABDERAOUF nasri

BELKASSIM belakhdar

Sous la direction de :

M.NOUREDDIN adjir

Promotion : 2019/2020

ملخص

مع التطور السريع للحوسبة، والذي هو موجود في كل مكان في حياتنا اليومية، ومع إضفاء الطابع الديمقراطي على تقنيات والحوسبة السحابية، شهدت التطبيقات الجديدة يوم. يتم استخدامها يوميًا (IoT) الهاتف المحمول، وظهور إنترنت الأشياء في حياتنا وفي مختلف المجالات، مثل مجالات التعلم الإلكتروني والتجارة الإلكترونية والصحة الإلكترونية والخدمات المصرفية الإلكترونية، إلخ. ولكن مع وجود الكتلة الكبيرة من البيانات التي يتم جمعها عبر إنترنت الأشياء، والتي يتم نقلها عبر الإنترنت واستخدامها (المخزنة و / أو المعالجة) عبر السحابة، فإن أمان هذه البيانات وسلامتها يعد سؤالًا يتم طرحه بشدة. من السهل تخيل خطورة حجم التهديد لمالكي هذه البيانات بشكل عام وخصوصية المستخدم، حيث أصبحت البيانات الخاصة موردا نقديا. في الواقع، وصل هذا التهديد إلى مرحلة حيث تم استخدام البيانات بموافقة أصحابها أو بدونها. لا تقدم مشكلة الأمان نفسها على أنها كلاسيكية كما كانت في السابق، أي "المتسلل" التقليدي، ولكن يمكن تقديمها عن طريق مقدمي ، حيث تم استخدام البيانات Facebook-Cambridge Analytica الخدمة أنفسهم، طواعية أم لا. هذا هو الحال في حالة ، دون علم أصحابها، لأغراض سياسية. يوضح هذا المثال تمامًا مشكلة الثقة في مزود Facebook الشخصية لمستخدمي الخدمة وعواقب فقدان السيطرة على البيانات الشخصية من قبل أصحابها. لمعالجة هذه القضايا، يجب تنفيذ حلول قوية لحماية البيانات وآليات فعالة لتقييم الثقة. بسبب عدم الثقة في مقدم الخدمة وحجم المخاطر الناتجة عن فقدان السيطرة، هناك .حاجة لإيجاد حلول وآليات فعالة لتقييم البيانات الشخصية للمستخدمين من أجل حماية خصوصية المستخدمين.

ولكن مع ذلك، إذا أردنا استخدام الأساليب التقليدية لحماية المعدات، فإن إنترنت الأشياء هو التحدي الأول المتعلق بالقيود المادية (الطاقة والذاكرة والمعالج) للكائنات المتصلة. يطرح إسناد مزودي الخدمة (مثل السحابة) مشكلة الثقة، حيث لم يعد المستخدم يتحكم في بياناته، لذلك يجب إيجاد حلول لاستعادة الموثوقية من حيث الأمن وجودة الخدمة.. أصبح المسار أكثر قابلية للتطبيق مع ظهور نماذج جديدة من الاستعانة بمصادر خارجية لمعالجة الكمبيوتر.

الكلمات المفتاحية: إنترنت الأشياء، الاستعانة بمصادر خارجية للتجهيز، الأمن، المنحنيات الإهليليجية.

Résumé

Avec le développement rapide de l'informatique, qui est omniprésente dans notre vie quotidienne, et avec la démocratisation des technologies de téléphonie mobile, l'apparition de l'Internet des objets (IoT) et du cloud computing, de nouvelles applications ont vu le jour. Ces dernières sont utilisées journellement dans notre vie et dans les divers domaines, tels que les domaines de e-learning, e-commerce, e-santé et e-banque, etc. Mais, avec la masse importante de données collectées via l'Internet des objets, véhiculées par l'internet et utilisées (stockées et/ou traitées) via le cloud, la sécurité et l'intégrité de ces données sont une question fortement posée. Il est facile d'imaginer le risque de l'ampleur de la menace des propriétaires de ces données d'une manière générale et pour la vie privée de l'utilisateur, car les données privées sont devenues une ressource monétaire. En fait, cette menace a atteint une phase où les données sont devenues utilisées avec ou sans l'accord des propriétaires. Le problème de la sécurité ne se présente pas aussi classique qu'auparavant, i.e. le traditionnel "pirate informatique", mais peut être portée par les fournisseurs de services eux-mêmes, volontairement ou non. C'est le cas de l'affaire Facebook-Cambridge Analytica, où des données personnelles d'utilisateurs de Facebook ont été utilisées, à l'insu de leurs propriétaires, à des fins politiques. Cet exemple illustre parfaitement le problème de confiance envers le fournisseur de service et les conséquences de la perte de contrôle sur les données personnelles par leurs propriétaires. Pour remédier à ces problèmes, des solutions de protection des données robustes et des mécanismes efficaces pour l'évaluation de la confiance doivent être mise en œuvre. En raison du manque de confiance dans le fournisseur de services et de l'ampleur des risques résultant de la perte de contrôle, Il est nécessaire de trouver des solutions et des mécanismes efficaces pour évaluer les données personnelles des utilisateurs afin de protéger la vie privée des utilisateurs.

Mais même ainsi, si l'on veut utiliser des méthodes traditionnelles de protection des équipements, alors l'Internet des Objets est le défi numéro un lié aux limitations physiques (puissance, mémoire, processeur) des objets connectés. L'attribution des prestataires (ex. le cloud) pose le problème de la confiance, l'utilisateur n'ayant plus le contrôle de ses

données, il faut donc trouver des solutions pour restaurer la fiabilité en termes de sécurité et de qualité de service. La voie est devenue plus applicable avec l'apparition de nouveaux modèles d'externalisation du traitement informatique.

Mots-clés : l'Internet des objets, externalisation du traitement, sécurité, courbes elliptiques, cryptographie ABE.

Abstract

With the rapid development of computing, which is ubiquitous in our daily life, and with the democratization of mobile phone technologies, the appearance of the Internet of Things (IoT) and cloud computing, new applications have seen the day. These are used daily in our life and in various fields, such as the fields of e-learning, e-commerce, e-health and e-banking, etc. But, with the large mass of data collected via the Internet of Things, conveyed by the Internet and used (stored and / or processed) via the cloud, the security and integrity of this data is a question which is strongly asked. It is easy to imagine the risk of the scale of the threat to the owners of this data in general and to the privacy of the user, as private data has become a monetary resource. In fact, this threat has reached a stage where data has become used with or without the consent of the owners. The security problem does not present itself as classic as it used to be, i.e. the traditional "hacker", but can be brought by the service providers themselves, voluntarily or not. This is the case in the Facebook-Cambridge Analytica case, where personal data of Facebook users was used, without the knowledge of their owners, for political purposes. This example illustrates perfectly the problem of trust in the service provider and the consequences of the loss of control over personal data by its owners. To address these issues, robust data protection solutions and effective trust assessment mechanisms need to be implemented. Due to the lack of trust in the service provider and the scale of the risks resulting from the loss of control, there is a need to find effective solutions and mechanisms to assess the personal data of users in order to protect the privacy of users. users.

But even so, if we want to use traditional methods of protecting equipment, then the Internet of Things is the number one challenge related to the physical limitations (power, memory, processor) of connected objects. The attribution of service providers (e.g. the cloud) poses the problem of trust, the user no longer having control of his data, so solutions must be found to restore reliability in terms of security and quality of service... The path has become more applicable with the emergence of new models of outsourcing computer processing.

Keywords: Internet of Things, processing outsourcing, security, elliptical curves, ABE cryptography.

Remerciement

Tout d'abord, nous remercions Dieu Tout-Puissant pour la volonté, la santé et la patience qu'il nous a accordées pendant toutes ces longues années d'étude afin que nous puissions y parvenir.

Nous remercions nos chères familles qui ont toujours été à nos côtés : "Vous avez tout sacrifié pour vos enfants, ne ménageant ni santé ni efforts. Vous avez donné un bel exemple de travail et de persévérance."

Nous tenons à exprimer ma gratitude à notre encadreur M. Noureddine Adjir, Merci d'être là et de nous faire confiance. Nous tenons également à le remercier pour son soutien et ses précieux conseils qui nous ont permis de faire ce travail. Nous ne saurions trop le remercier, car vous trouvez dans ce souvenir l'expression de ma profonde gratitude et de mon respect sans bornes.

Nous remercions sincèrement tous les professeurs, les intervenants, tous et toutes les personnes qui ont guidé nos pensées avec leurs mots, écrits, conseils et critiques et ont accepté d'être interviewés avec nous et ont répondu à nos questions lors de nos recherches.

Nous remercions les membres du jury d'avoir honoré notre travail avec l'honneur de l'arbitrage.

De peur d'oublier qui que ce soit, nous remercions sincèrement tous ceux qui nous ont aidés à nous souvenir de cet humble souvenir.

Merci tout simplement !

Dédicace

À nos parents pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études,

À nos chères sœurs pour leur encouragement constant et leur soutien moral,

A nos chers frères pour leur soutien et leurs encouragements,

A toutes nos familles pour les accompagner tout au long de notre carrière universitaire,

Que cette œuvre soit la réalisation de vos soi-disant désirs et une évasion de votre soutien indéfectible,

Merci d'être toujours avec nous.

Table des matières

Tables des figures

Listes des tableaux

Première partie

Introduction

1. Introduction

1.1 Contexte et problématique

Les systèmes d'information à base des nouvelles technologies de l'information et de la communication sont omniprésents dans notre vie quotidienne. Ils sont devenus de plus en plus fonctionnel, notamment à travers le développement du concept d'IoT, l'externalisation des services des capacités de calcul et de mémoire pour les équipements à limitations physiques. Cette extension de capacité est proposée via le paradigme du cloud computing et plus récemment via les nouveaux paradigmes (Edge et Fog Computing) qui améliorent les performances en rapprochant ces services de l'utilisateur final.

Cependant, le nombre de techniques et d'applications qui manipulent nos données personnelles met en risque la préservation de notre vie privée. En outre, l'utilisation de l'Internet des Objets introduit des défis pour la mise en œuvre d'outils de sécurité traditionnels (chiffrement, PKI, etc.) alors que l'externalisation de nos traitements pose le problème de la confiance. En effet, en faisant appel aux fournisseurs de services pour traiter et stocker nos données, on perd le contrôle effectif sur celles-ci. Au final, nous devons nous fier à la capacité du fournisseur de services d'assurer une protection adéquate de nos données et dans un cas extrême à son honnêteté. Cela, dans un monde ou les données personnelles sont une ressource monnayable.

Dans ce qui suit, la section 1.2 est consacrée au concept de l'Internet des Objets ainsi qu'aux paradigmes utilises pour l'externalisation des traitements. Ces concepts et paradigmes seront illustres par un cas d'utilisation du domaine de la e-santé, à chaque fois que ceci s'avère opportun. La problématique de recherche ainsi que les objectifs visés sont détaillées dans la section 1.3. La section 1.4 est dédiée aux contributions de ce travail et nous finirons par une conclusion.

1.2 Concepts mis en œuvre

1.2.1 Internet des objets (IdO)

Selon l'Union internationale des télécommunications, l'Internet des objets (IdO) 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 »[1].*

En réalité, la définition de ce qu'est l'Internet des objets n'est pas figée. Elle recoupe des dimensions d'ordres conceptuel et technique.

- D'un point de vue conceptuel, l'Internet des objets caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel.

- D'un point de vue technique, l'IdO consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http...) d'un objet physique grâce à un système de communication sans fil qui peut être une puce RFID, Bluetooth ou Wi-Fi.

Figure 1.1 _ L'Internet des objets regroupe tous les objets physiques communicants dotés d'une identité numérique unique.

Les objets connectés produisent de grandes quantités de données dont le stockage et le traitement entrent dans le cadre de ce que l'on appelle les big data. En logistique, il peut s'agir de capteurs qui servent à la traçabilité des biens pour la gestion des stocks et les acheminements. Par exemple, dans le domaine de l'environnement, les capteurs surveillent la qualité de l'air, la température, le niveau sonore, l'état d'un bâtiment, etc. En domotique, l'IdO recouvre tous les appareils électroménagers communicants, les capteurs (thermostat, détecteurs de fumée, de présence...), les compteurs intelligents et systèmes de sécurité connectés des appareils de type box domotique.

L'IdO est également très utilisé dans le domaine de la santé et du bien-être avec le développement des montres connectées, des bracelets connectés et d'autres capteurs surveillant des constantes vitales. Selon diverses projections, le nombre d'objets connectés devrait largement augmenter au fil des ans.

1.2.2 Externalisation des services informatiques

Avec l'utilisation importante des techniques de l'Internet des objets (IdO), caractérisées par des limitations en ressources tels que l'énergie, la puissance de calcul et la mémoire, on a constaté que les traitements liés à ces applications ne peuvent être effectués sur l'objet lui-même. La solution viable est l'externalisation des services informatiques i.e. externaliser certaines taches vers des équipements n'ayant pas de contraintes de ressources [4]. C'est une évolution très importante des systèmes informatiques vers la notion de service informatique. Ainsi, les ressources peuvent être facilement partagées et gérées de n'importe où et à tout moment. Le Cloud a été le composant principal de cette norme, qui fournit un grand espace de stockage et une grande capacité de calcul, grâce à la virtualisation, car les ressources sont disponibles de n'importe où et pour n'importe qui, en tant que service et non en tant que produit. Il est donc possible de louer à la demande des capacités informatiques (capacités de calcul et de stockage aux logiciels) sur des serveurs centralisés et distants, accessibles via le réseau Internet. C'est le paradigme du Cloud Computing ou l'informatique en nuage. Internet est l'une des technologies les plus répandues de nos jours grâce à l'élégance des technologies de l'information. Aujourd'hui, il est au bord d'une révolution, où les ressources sont interconnectées à l'échelle mondiale. Ainsi, les ressources peuvent être facilement partagées et gérées de n'importe où et à tout moment.

Cependant, avec la taille massive des données à traiter (big-data en anglais), de l'informatique ubiquitaire associée à l'Internet des objets, le modèle du Cloud Computing est rendu inefficace. Cette inefficacité résulte principalement de la distance géographique entre les data center et les clients finaux. La solution à cette situation, et qui prendre en compte les contraintes des objets connectés, de nouveaux paradigmes ont fait leur apparition. Ces paradigmes ont en commun l'objectif de rapprocher les fonctionnalités du Cloud du client final comme par exemple le Cloud mobile (ou mobile Cloud

computing en anglais) [143], l'informatique en brouillard (fog computing) [138] et l'infrastructure réseau des frontières (ou mobile edge computing en anglais) [136].

Un aperçu sur ces paradigmes qui permettent d'extérioriser les services informatiques (capacité de calcul, de stockage, plates-formes de développement, logiciels applicatifs, etc.) est présente dans ce qui suit. La figure 1.2 schématise le fonctionnement global de cette architecture.

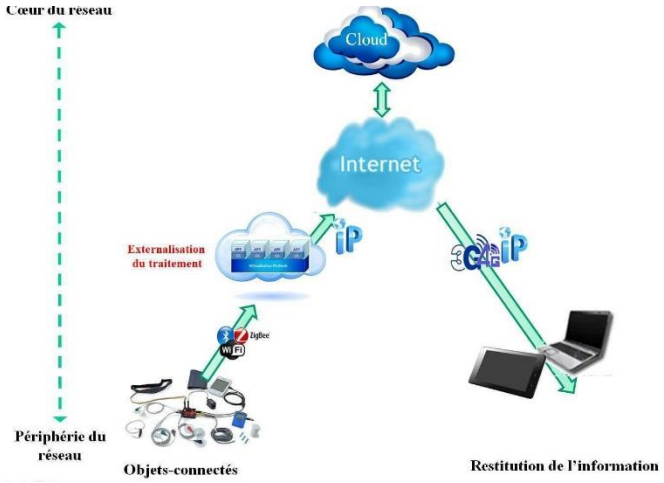


Figure 1.2 – Architecture IoT-Edge/fog-Cloud, application e-santé monitoring

1.2.2.1 L'informatique en nuage (Cloud Computing)

De plus en plus utilisé par les entreprises de toutes les industries, le Cloud Computing est la nouvelle forme de stockage de données principalement et de leurs traitements du 21ème siècle.

Le cloud computing est un modèle permettant de créer un accès réseau à la demande à un ensemble commun de ressources informatiques configurables. Ces ressources sont, par exemple, les réseaux, les serveurs, l'espace de stockage, les applications et les services. Ils peuvent être fournies rapidement avec un minimum d'effort administratif et d'interaction avec le fournisseur de services.

Figure 1.3_ Schéma de Cloud computing

Le Cloud Computing, apporte une réponse viable aux défis auxquels l'Internet des objets est confronté, notamment la croissance du volume de données, qui est accentuée par la prolifération de capteurs et d'objets connectés. A titre d'exemple, et dans le domaine de e-santé, General Electric (GE) Healthcare estime qu'en moyenne, le suivi d'un patient atteint 1,5 Go de données par jour. L'utilisation de plus en plus répandue de terminaux mobiles (Smartphones, tablettes, etc.) nécessite l'extension de leurs capacités limitées en utilisant celles du Cloud. [2]

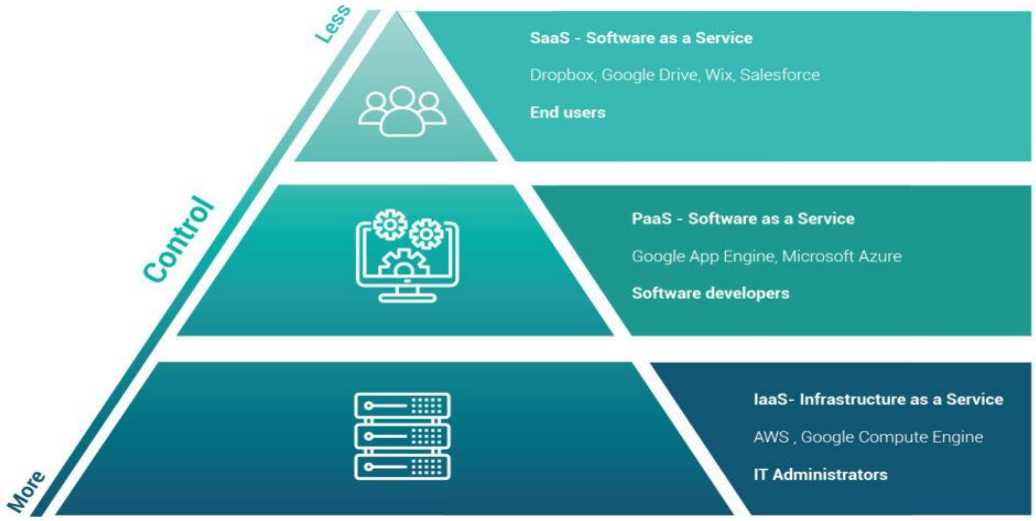


Figure 1.4_Les modèles de livraison du Cloud Computing

Le Cloud offre comme nous pouvons le voir sur la figure 1.4, une variété de services d'infrastructure (IaaS pour Infrastructure as a Service) tels que des infrastructures réseau virtuelles, de plates-formes (PaaS pour Platform as a Service) tels que des systèmes d'exploitation ou encore de

logiciels (Saas pour Software as a Service) comme les applications d'authentification, de comptabilité ou autre.

1.2.2.2 Traitement des données à la périphérie du réseau (Edge-computing)

Le volume de données générées par les objets connectés est en pleine explosion. Dans ce contexte, les spécialistes estiment qu'il est irréaliste de transmettre toutes ces données entre leurs sources et les Data Centres Cloud de façon stable et rapide afin d'être analysées. En outre, les propriétaires des données comme la manufacture, la santé, les télécommunications et la finance ont besoin d'être en mesure d'analyser les données les plus importantes le plus rapidement possible, presque en même temps qu'elles sont collectées. Face à cette problématique est apparue le concept de Edge Computing qui est une forme d'architecture informatique qui est devenue comme concurrent direct, alternative ou solution complémentaire au Cloud Computing et Fog Computing (voir section suivante). Il s'agit de traiter les données en périphérie du réseau directement où elles sont générées par des appareils connectés IoT plutôt que de les transférer vers le Cloud ou un Data Center [3]. La figure1.5 illustre le concept.

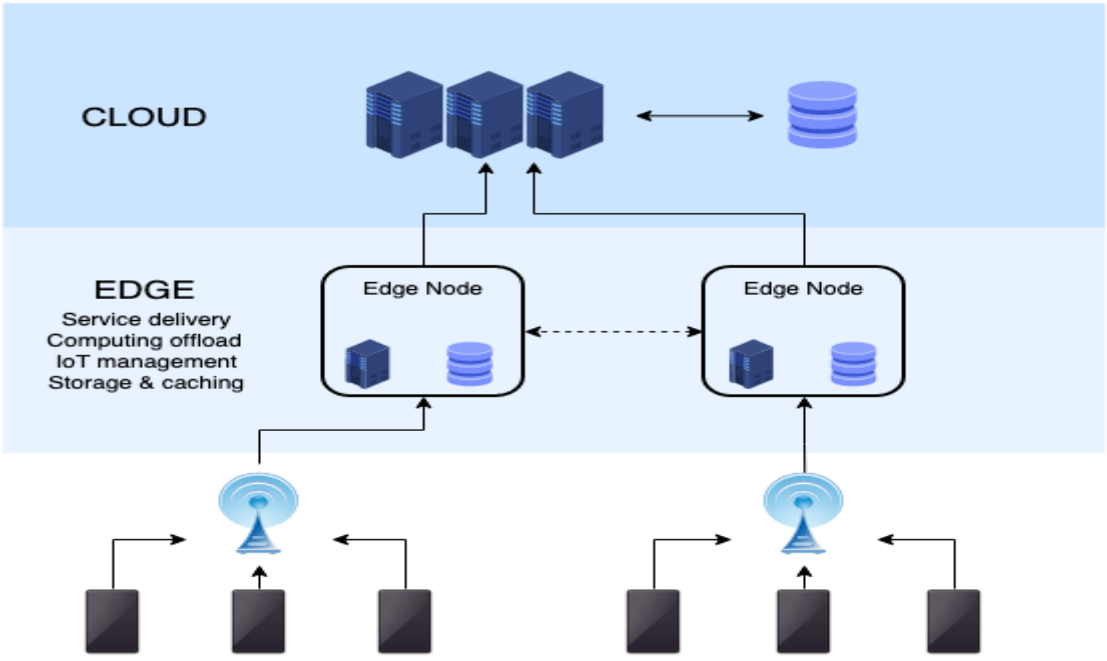


Figure 1.5_edge computing

1.2.2.3 L'informatique en brouillard (Fog computing)

Le Fog Computing, aussi appelé "informatique dans le brouillard", définit une infrastructure chargée de stocker et de traiter des données transmises par les objets connectés. Le Fog Computing, solution alternative ou complémentaire au Cloud Computing, permet de stocker et de traiter les données via des équipements implantés à la périphérie du réseau sans avoir à solliciter un data center situé à plusieurs centaines de kilomètres ou un Cloud. Il crée une interface supplémentaire que l'on peut situer entre le Edge Computing et le Cloud Computing. [4]

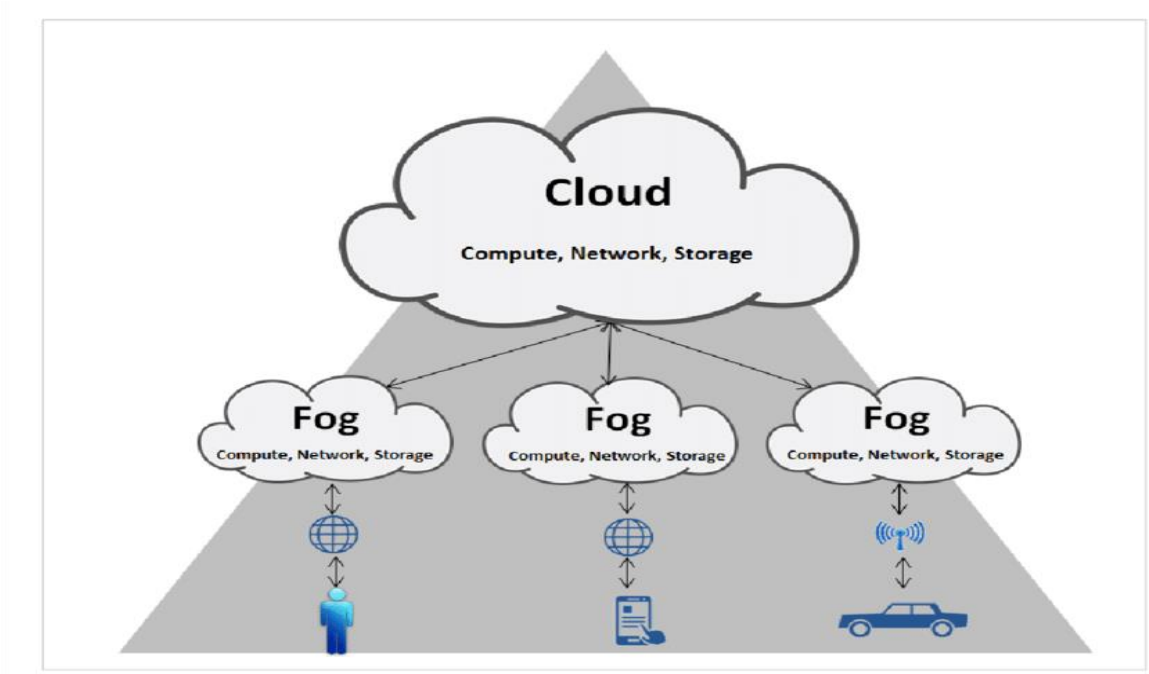


Figure1.6_Fog computing

1.2.2.4 Différence entre Cloud Fog et Edge Computing

- Le cloud computing permet des structures hiérarchiques dans lesquelles les données collectées par les appareils connectés (capteurs, etc.) sont traitées localement avant de subir un traitement global ultérieur au niveau du cloud.

- Les concepts de Fog et Edge sont si proches l'un de l'autre qu'on arrive parfois à confondre entre eux. Cependant, contrairement aux nœuds de calcul du Edge, le déploiement des nœuds de Fog

Computing ne se limite pas à la périphérie du réseau, mais peut être effectué plus profondément dans le réseau.

- Aussi, Le Fog computing peut facilement étendre les modèles de services (IaaS, PaaS, Saas) fournis par le Cloud jusqu'à la périphérie du réseau.

La figure 1.7 donne une vue générale des différents modèles utilisés pour la déportation des traitements dans un environnement IoT.

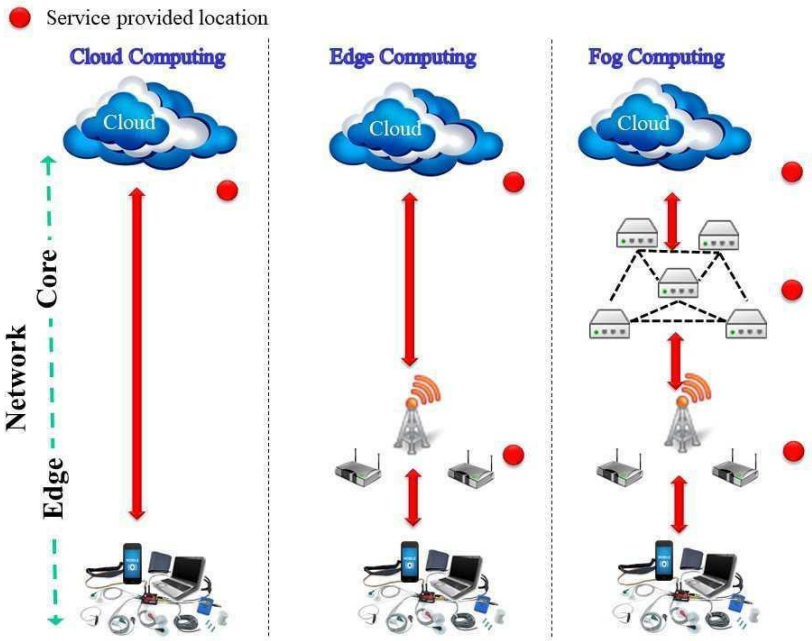


Figure1.7_ Vues globales des paradigmes de déportation des traitements

1.3 Aperçu Général sur les Problèmes et les Méthodologies de la sécurité en IoT

Basé sur de nombreuses recherches sur les dernières technologies de sécurité des données dans l'environnement IoT / Cloud, les spécialistes de la sécurité sont rendus compte que : Le propriétaire des données doit avoir un contrôle effectif sur le processus de (i) chiffrement et (ii) de partage de ces données, indépendamment de leur emplacement. Pour assurer ces deux fonctionnalités et de manière simultanée, certains chercheurs, comme le cas de [], ont opté pour le chiffrement par attributs []. Cependant, les restrictions des capacités des objets connectés réduisent la portée de ces processus (cryptage et partage des données). Ces limites rendent difficile l'application de ce type de chiffrement voir même impossible sur certains types particuliers de ces objets. C'est ce qui a appelé les chercheurs à opter pour le choix d': (i) externaliser et valoriser certaines tâches de chiffrement grâce à des

technologies de pointe (ii) ainsi qu'à des techniques d'authentification pour des prestataires tiers qui garantissent la qualité du service rendu et la confiance. Il faut bien remarquer le mot certaines tâches, et y penser, et non pas tout le processus de chiffrement. Ce choix est soutenu, en particulier, par les avancées techniques plus particulièrement la virtualisation et les réseaux 5G. Avec cette solution, l'utilisation des ressources des objets connectés est fortement bien réduite, à savoir la charge de calcul et l'utilisation de la mémoire, tout en répondant aux exigences de protection des données personnelles. Par contre un autre problème est émergé. En fait, l'externalisation des processus de sécurisation nécessite une garantie sur la qualité de service qui sera délivrée par les tiers fournisseurs de service et la confiance dans leur comportement. Car les solutions cryptographiques n'offrent aucune garantie du comportement futur du prestataire en termes de sécurité et de qualité de service. La sécurité collaborative repose sur l'utilisation des informations issues des expériences des utilisateurs pour fournir une évaluation raisonnable du fournisseur de services lui-même.

Ceci étant, notre travail s'articule autour du premier problème de la sécurité cryptographique des équipements à fortes contraintes de ressources alors que le deuxième problème de la sécurité collaborative des systèmes a multi-offres de services n'est pas à la portée de ce mémoire et peut être traité à travers les mécanismes de gestion de la confiance.

Pour ce faire, il a abordé la question de la sécurité cryptographique des équipements connectés avec les puissantes limitations de ressources que représente le monde de l'IoT (énergie, mémoire, puissance de calcul, etc.).

1.4 Contribution

Sécuriser les données des utilisateurs et protéger leur confidentialité n'est pas une tâche facile dans l'écosystème IdO, en particulier lorsque l'on prend en compte les contraintes de ressources, car les applications IoT sont de plus en plus appliquées aux infrastructures informatiques et confrontées aux problèmes de confiance inhérents. Notre contribution peut se résumer en deux points principaux :

- Le premier se concentre sur la nécessité pour le propriétaire des données de contrôler le processus de chiffrement et de distribution des données, dans lequel nous nous sommes appuyés sur un chiffrement basé sur attributs.
- Le deuxième garantit la confidentialité et l'intégrité des données personnelles de l'utilisateur, quels que soient les prestataires de services de calcul et de stockage, en intégrant le nouveau système de cryptage selon le système d'attributs dans un protocole de sécurité en considérant les prestataires externes comme des entités honnêtes.

Deuxième partie :

Sécurité des données dans un environnement internet des objets et cloud

2.1 Solutions de Sécurité des Données Classiques vs. Hétérogénéité de l'Environnement IdO-Cloud

L'hétérogénéité des deux environnements, l'Internet des objets et le Cloud, rend plus difficile le défi de développer des solutions complètes pour sécuriser les données et protéger la vie privée tout en fournissant toutes les fonctions.

D'un côté, le manque de ressources dans l'environnement IoT en termes de puissance, de mémoire et de capacité de calcul, qui caractérise les objets connectés, limite le déploiement de solutions de sécurité traditionnelles alors que ce problème n'existe pas au niveau du cloud car les ressources sont relativement illimitées. Cependant, l'utilisateur peut rencontrer un problème de confiance au niveau du cloud.

A partir de ce qui précède, trouver et développer une solution générale et viable pour sécuriser les données, depuis le début de leur introduction jusqu'à leur traitement ou leur stockage i.e. de bout en bout et applicable, est une tâche très difficile. Cela n'a pas empêcher les chercheurs à proposer plusieurs solutions pour sécuriser les données et protéger la confidentialité dans cet environnement hétérogène, internet des objets et Cloud e.g. [113], [78], [43], [67] et [128]. Cependant, Certain de ces chercheurs soit qu'ils ont proposé une solution pour le contrôle d'accès dans l'environnement Cloud, mais qui ne prend pas en compte les contraintes de l'IdO, soit encore ils proposent de sécuriser les données et de protéger la vie privée dans l'environnement IdO sans pour autant proposer de solutions pour le partage de données et le contrôle d'accès au Cloud, ou bien ils adaptent des solutions existantes avec un minimum d'innovation, a des cas d'utilisation précis, en imposant des hypothèses sur l'environnement au risque de s'éloigner du monde réel. Dans cette dernière proposition de solution, il est impératif de disposer d'un Cloud privé totalement sécurisé. De là, on voit que le problème du contrôle d'accès se pose au niveau du cloud qui doit être de confiance. Ainsi, il existe des solutions qui proposent de résoudre ce problème. A titre d'exemple, la solution qui repose sur le chiffrement d'attributs (ABE) pour contrôler l'accès aux données. Ce type de contrôle est centré sur le propriétaire des données et caractérisé par la confidentialité, une protection renforcée de la confidentialité en réduisant les privilèges des données de l'hôte. Cependant, la solution proposée n'élimine pas complètement l'autorité faisant autorité de l'administration du contrôle d'accès et ne prend pas en charge les ressources limitées des objets connectés. Une solution est d'externaliser des services qui fait l'objets du prochain paragraphe.

2.1.2 Externalisation des services

Face au constat suivant : (i) impossibilité d'augmenter les capacités physiques des objets connectés, et/ou (ii) à défaut d'améliorer l'efficacité des algorithmes d'un côté, et avec les nouveaux paradigmes du Cloud computing, du Fog, etc. d'un autre côté, la solution au problème est donc l'externalisation des calculs lourds. La migration ou l'externalisation est une solution viable au problème des ressources limitées pour effectuer des opérations mathématiques lourdes et enrichir les tâches fournies par l'IoT. Cependant, le mécanisme d'externalisation pour l'IoT présente une menace envers la protection de la vie privée comme par exemple la possibilité de diffuser des services malveillants et la curiosité d'acteurs « honnêtes », ce qui amène au problème précédemment évoqué de la gestion de la confiance et au problème de la sélection des fournisseurs de services informatiques. Ce problème peut être résolu grâce à des systèmes d'évaluation de la confiance et de sélection de services.

2.1.3 Dépendance des Exigence de Sécurité du Domaine d'application

Déterminer les exigences de sécurité de l'environnement IoT sans définir son domaine d'application est un peu difficile en raison (i) de sa présence dans divers domaines (smart city, santé, voitures autonomes, etc.) et (ii) des technologies qui ont vues le jour avec l'augmentation des objets connectés (cloud, brouillard, etc.).

Dans notre sujet, nous avons choisi le domaine des maisons intelligente, en raison des fortes restrictions sur la protection des données personnelles, les exigences en matière de sécurité ont été définies comme suit :

- Confidentialité : le contenu des données personnelles ne doit pas être divulgué à des tiers non autorisés.

- Authentification : les données ne doivent être accessibles qu'aux personnes désignées et autorisées à y accéder.

- Protection de la vie privée : les données ne doivent divulguer aucune information sur le patient (pathologie, localisation, etc.).

- Intégrité : vous ne devez pas modifier le contenu des données.

2.2 Confidentialité et Authenticité des Données par le Chiffrement

Le schéma traditionnel de la cryptographie était d'assurer la sécurité des échanges point à point, en d'autres termes, un processus par lequel nous voulons empêcher quiconque de comprendre un document qui ne possède pas de clé de déchiffrement. Mais avec le développement récent typique de l'environnement informatique, de nouvelles exigences sont apparues. Le nouveau parmi eux est le contrôle complet du propriétaire des données sur la distribution de ses données personnelles, en d'autres termes, empêcher les fournisseurs de services informatiques d'accéder aux données non chiffrées. C'est ce qu'une solution de chiffrement par des attributs fournit pour répondre à ces besoins. Surtout dans l'environnement IoT car il représente une forte contrainte en termes de mise à disposition des ressources nécessaires pour mettre en place des solutions de sécurité robustes.

On distingue deux types de systèmes de chiffrement traditionnel et un type émergent qui nous intéressent :

- Chiffrement symétrique.
- Chiffrement asymétrique.
- Chiffrement par attributs.

2.2.1 Chiffrement symétrique :

Dans un système de chiffrement symétrique ou chiffrement à clé secrète, un expéditeur et un destinataire partagent une même clé secrète. Cette clé est utilisée à la fois pour le chiffrement et pour le déchiffrement et doit rester secrète de toute autres personnes. Ce fonctionnement est présenté dans la figure suivante :

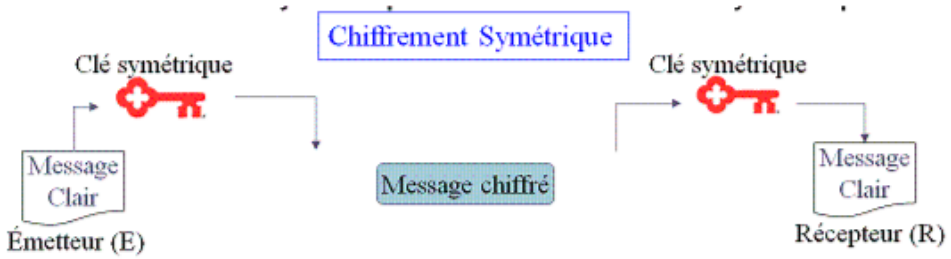


Figure 2.1_ *:* principe du chiffrement symétrique

Les algorithmes symétriques sont de deux types :

1- Les algorithmes de chiffrement de flux (ou chiffrement par flot), qui agissent sur le message en clair un bit à la fois.

2- Les algorithmes de chiffrement par bloc, qui opèrent sur le message en clair par groupes de bits appelés bloc.

2.2.1.1 Algorithme de chiffrement de flux :

Le principe consiste à générer un flux pseudo aléatoire et de le combiner avec l'information bit à bit par l'opération XOR[3]. A la réception, on applique le même mécanisme, et on restitue l'information. Quelques exemples sur les algorithmes de chiffrement : RC4, E0, …

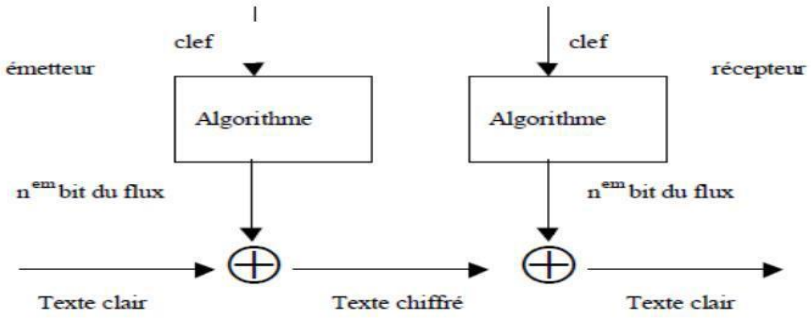


Figure 2.2_Chiffrement par flux

2.2.1.2 Algorithme de chiffrement par bloc :

Un algorithme de chiffrement par bloc (Block Cipher) transforme des blocs de données de taille fixe en bloc de données chiffrées de la même taille. Les blocs font généralement 128 bits, mais ils peuvent aller de 32 à 256 bits selon l'algorithme. La transformation reste la même pour chaque bloc. Quelques exemples sur les algorithmes de chiffrement : DES, AES, …

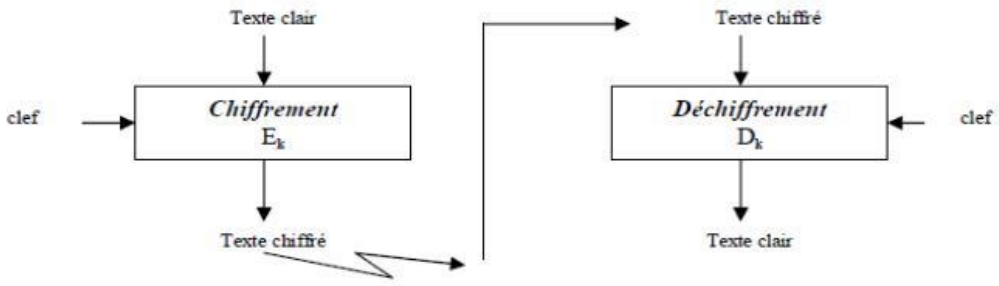


Figure 2.3_Chiffrement par bloc

2.2.2 Chiffrement asymétrique :

Le principe de la cryptographie asymétrique (appelé aussi chiffrement à clé publique) est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation de clés, une clé publique (qui est diffusée) et une clé privée (gardée secrète), la première permettant de coder le message et la deuxième de le décoder, comme le montre la figure ci-dessous. Exemples sur le chiffrement asymétrique : RSA, ElGamel, ECC

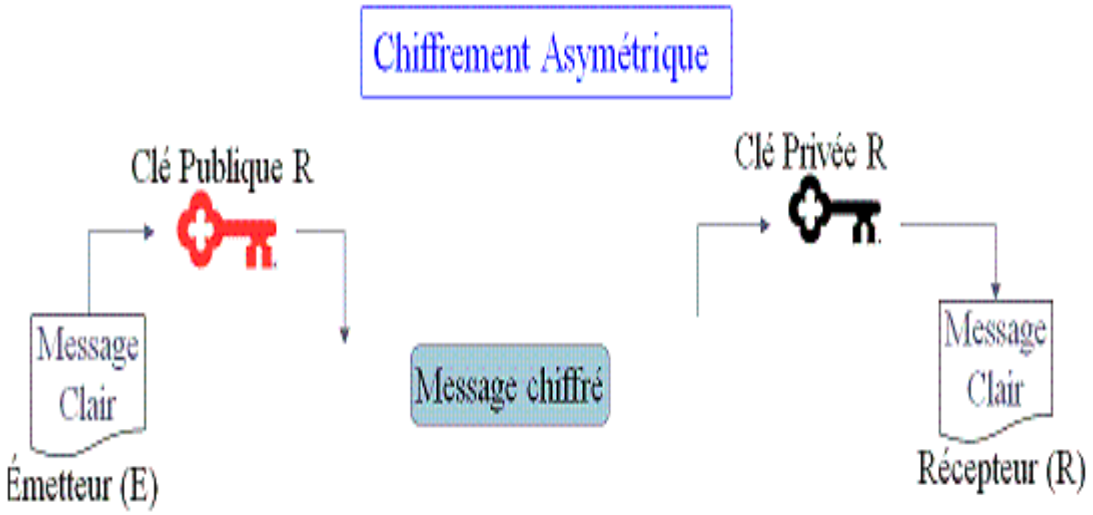


Figure 2.4_Chiffrement Asymétrique

Le tableau suivant représente les avantages et les inconvénients des deux types de Chiffrement :

Chiffrement	avantages	Inconvénients
Symétrique	- Le chiffrement /déchiffrement est très rapide - Clés relativement courtes	- Gestion de clés difficile - Point faible = échange d'un secret - L'utilisation d'une clé unique présente un problème lors de l'échange de clé .
Asymétrique	- Renforcer la sécurité, Même en interceptent le message impossible de le décryptez sans la clé privée.	La relation clé privé /clé public impose : - Dés cryptos systèmes beaucoup plus lents que symétrique. - Gestion certificats des clés public

Tableau 1 _ Avantages et inconvénients de la cryptographie symétrique/asymétrique

La combinaison du cryptage symétrique et asymétrique permet de réduire le temps de cryptage / déchiquetage en cryptant le message avec un cryptage symétrique. La clé de cryptage symétrique est envoyée en même temps que l'envoi du texte crypté et en utilisant différentes clés aléatoires pour chaque message, réduisant ainsi la surface de vulnérabilité et en même temps résolvant le problème de la distribution des clés de session.

2.2.3 Chiffrement par attributs

Malgré le succès des systèmes de chiffrement traditionnels, y compris le transfert et le stockage sécurisés des données dans un environnement cloud, il présente un inconvénient, qui est la difficulté de configurer un contrôle d'accès avec une grande précision. Pour partager des données, surtout si nous ne connaissons pas l'identité des utilisateurs auparavant. Une solution de cryptage via des fonctionnalités ou « cryptage basé sur les fonctionnalités » est une solution viable. Qui peut être défini comme suit :

Le chiffrement basé sur les attributs ou « chiffrement basé sur les fonctionnalités » (ABE) est un type de système de cryptographie à clé publique de type un-à-plusieurs, Un avantage évident de cette technologie est que chaque utilisateur dispose d'une clé dédiée, en cas de révocation d'une clé, il n'est pas nécessaire de refaire l'opération des données. Les données peuvent être chiffrées à partir de la source et stockées telles quelles, et le fournisseur de services n'a jamais accès à l'effacement. En plus de sécuriser la transmission et le stockage des données, il fournit également un contrôle d'accès très précis, une gestion évolutive des clés, une distribution flexible des données, ainsi qu'un cryptage et un partage de données basés sur des fonctionnalités descriptives, sans aucune connaissance préalable de l'identité du destinataire. Plusieurs facteurs influencent les performances de l'ABE dans les applications du monde réel, tels que le niveau de sécurité souhaité, la capacité du périphérique sous-jacent (c'est-à-dire la mémoire disponible et la vitesse du processeur), ainsi que le nombre et le type d'attributs utilisés dans la définition de la politique d'accès.

2.2.3.1 Structure d'accès associée à ABE

La structure d'accès prend généralement la forme d'un arbre d'accès. La Figure 3.1 illustre un arbre d'accès pour un exemple de politique d'accès simple : $P = Att1 \vee ((Att2 \wedge Att3) \vee (Att4 \wedge Att5))$. Chaque feuille représente un attribut et chaque nœud interne est une porte logique ($\wedge$, $\vee$).

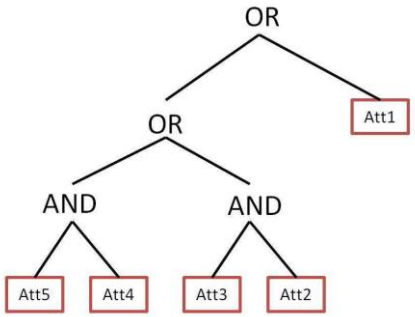


Figure 2.5 – Arbre d'accès pour un exemple de politique simple

On distingue deux principales variantes :

2.2.3.2 Contrôle d'accès CP-ABE (Ciphertext-Policy Attribut Based Encryption)

Proposée pour la première fois par Bethencourt *et al.* [19] en 2007, où chaque utilisateur est associé à un ensemble de traits. Sa clé secrète est créée en fonction de ses attributs. Lors du cryptage d'un message, le codeur définit la structure d'accès de seuil pour ses attributs intéressés. Ce message est ensuite chiffré sur la base de cette architecture d'accès afin que seuls ceux dont les attributs correspondent à l'architecture d'accès puissent le déchiffrer. Grâce à la technologie CP-ABE, les données cryptées peuvent rester confidentielles et protégées contre les attaques de collusion. CP-ABE applique la politique d'accès directement sur les données : la clé de chaque utilisateur est associée à un ensemble d'attributs, et un utilisateur peut déchiffrer un texte chiffré si ses attributs satisfont la politique d'accès définie sur les données.

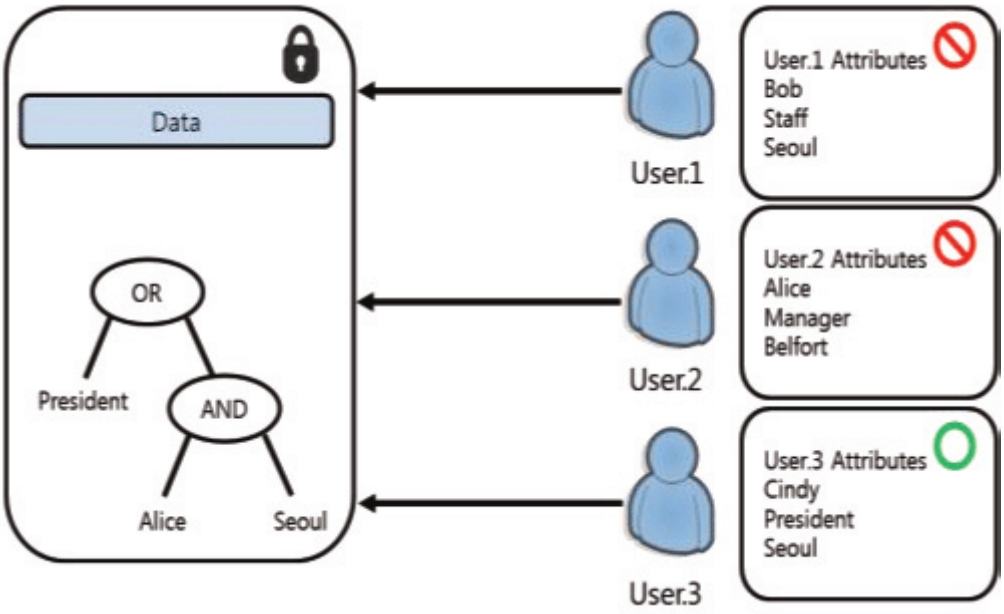


Figure 2.6_CP-ABE (Ciphertext-Policy Attribute Based Encryption)

Le chiffrement ABE peut être défini comme un quadruplet de quatre algorithme (Setup, Enc, Dec, KeyGen).

Algorithme	Description des entrées/sorties
Setup :	***Entrée :*** Un paramètre de sécurité *l*. ***Sortie :*** Une clé publique de chiffrement *P k* et une clé secrète principale *M Sk* qui servira à générer les clés secrètes de déchiffrement.
Enc :	***Entrée :*** Message à chiffrer *m*, la clé publique *P k* et un ensemble d'attributs a_i dans le cas de KP-ABE ou une politique d'accès *P* dans le cas de CP-ABE. ***Sortie :*** Le chiffré *c*.
KeyGen :	***Entrée :*** La clé secrète principale *M Sk* et un ensemble d'attributs a_i dans le cas de CP-ABE ou une politique d'accès *P* dans le cas de KP-ABE. ***Sortie :*** une clé de déchiffrement secrète *Sk*, liée à un ensemble d'attributs a_i dans le cas de CP-ABE ou à une politique d'accès *P* dans le cas de KP-ABE.
Dec :	***Entrée :*** Le chiffré *c* et une clé de déchiffrement *Sk*. ***Sortie :*** Si l'ensemble d'attributs a_i satisfont la politique *P* alors sortie *m* sinon

Tableau 2_ Entrées/Sorties des algorithmes de CP-ABE

2.2.3.2.1 Exemple illustratif

La figure 2.6 illustre un exemple du CP-ABE. Dans ce schéma, le propriétaire des données crypte les données en spécifiant la politique d'accès : (Dev_family = Board_XYZ ∧ Dev_role = Role_1) ∨ (Release_Date> 2013) dans le cadre du cryptage.

Un utilisateur pourra déchiffrer le texte chiffré, si sa clé secrète est associée à un ensemble d'attributs pouvant satisfaire la politique d'accès.

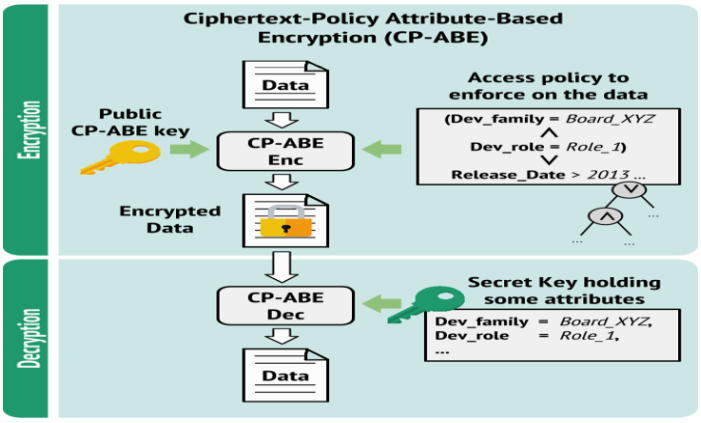


Figure 2.7 _ CP-ABE

2.2.3.3 Chiffrement KP-ABE (Key-Policy Attribute Based Encryption)

Chiffrement "KP-ABE" dans lequel la politique d'accès est intégrée dans la clé secrète, c'est-à-dire que nous décidons pour chaque utilisateur à quels objets il peut accéder. Nous attachons à chaque texte chiffré un ensemble de fonctionnalités. Une clé secrète spécifique peut être, avec une politique Accès spécifique, déchiquetant uniquement le texte chiffré avec des attributs qui répondent à sa politique d'accès.

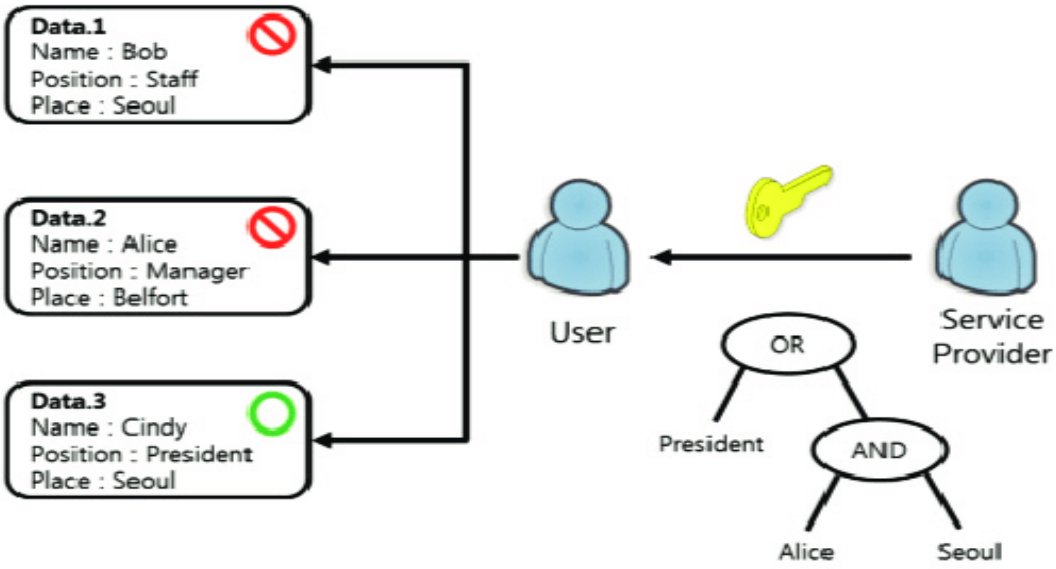


Figure 2.8_ KP-ABE (Key-Policy Attribut Based Encryption)

2.2.3.3.1 Exemple illustratif

Dans KP-ABE, la clé de chaque utilisateur représente une politique d'accès, par exemple (Dev_family = Board_XYZ ∧ Dev_role = Role_1) ∨ (Release_Date> 2013), où Dev_family et Dev_role représentent des attributs de chaîne, Release_Date représente un attribut numérique, et ∧ et ∨ sont les opérateurs booléens AND et OR, respectivement.

La figure 2.8 montre un exemple de KP-ABE, où un propriétaire de données crypte les données en spécifiant une liste d'attributs.

Si le propriétaire des données attribue l'ensemble d'attributs suivant au texte chiffré : {Dev_family = Board_XYZ, Dev_role = Role_1} ou {Release_Date = 2014}, l'utilisateur pourra déchiffrer le texte chiffré.

Parce que, dans ces cas, la politique d'accès associée à la clé secrète de l'utilisateur peut être satisfaite par les attributs attribués au texte chiffré.

De même, le cryptage KP-ABE nécessite deux exponentiations pour chaque attribut appliqué sur le texte chiffré. La complexité de déchiffrement dans CP-ABE est limitée par L exponentiations et 2L opérations d'appariement [10], tandis que dans KP-ABE par seulement 1 opérations d'appariement ; l est le nombre d'attributs « correspondant » à la politique d'accès (dans CP-ABE) ou à la politique de clé (dans KP-ABE).

Pour une évaluation plus complète de l'ABE, dans cette recherche, nous analysons également l'impact de l'utilisation d'attributs numériques avec des attributs de chaîne.

Nous pensons que, bien que l'utilisation d'attributs numériques puisse être coûteuse, elle fournit une expressivité supplémentaire dans les définitions de politique, en particulier dans CP-ABE.

À titre d'exemple, il peut y avoir des situations où l'accès aux données doit être limité à un seul modèle de périphériques, libéré après une certaine date (qui peut être représentée sous la forme d'un entier de 64 bits).

Dans KP-ABE, la clé de chaque utilisateur représente une politique d'accès, par exemple (Dev_family = Board_XYZ ∧ Dev_role = Role_1) ∨ (Release Date> 2013), où Dev_family et Dev_role représentent des attributs de chaîne, Release Date représente un attribut numérique, et ∧ et ∨ sont les opérateurs booléens AND et OR, respectivement.

La figure 1 (a) montre un exemple de KP-ABE, où un propriétaire de données crypte les données en spécifiant une liste d'attributs.

Si le propriétaire des données attribue l'ensemble d'attributs suivant au texte chiffré : {Dev_family = Board_XYZ, Dev_role = Role_1} ou {Release Date = 2014}, l'utilisateur pourra déchiffrer le texte chiffré.

Parce que, dans ces cas, la politique d'accès associée à la clé secrète de l'utilisateur peut être satisfaite par les attributs attribués au texte chiffré.

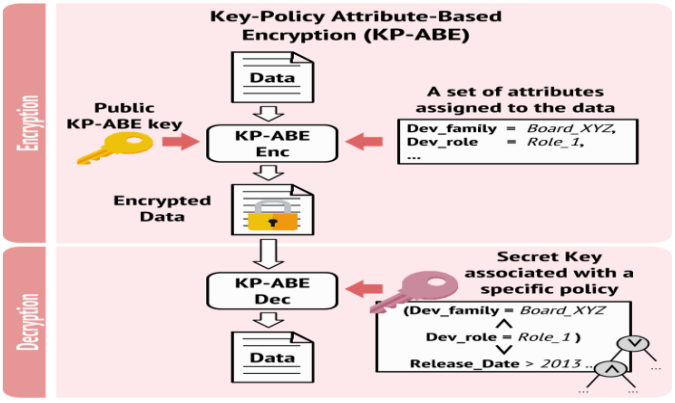


Figure 2.9 _ CP-ABE

2.2.3.4 Comparaison entre KP-ABE et CP-ABE

Le nombre d'attributs, en particulier, joue un rôle fondamental dans les performances ABE : le chiffrement dans CP-ABE nécessite de calculer deux exponentiations pour chaque attribut dans la politique d'accès résultante.

De même, le cryptage KP-ABE nécessite deux exponentiations pour chaque attribut appliqué sur le texte chiffré. La complexité de déchiffrement dans CP-ABE est limitée par L exponentiations et 2L opérations d'appariement [10], tandis que dans KP-ABE par seulement 1 opérations d'appariement ; l est le nombre d'attributs « correspondant » à la politique d'accès (dans CP-ABE) ou à la politique de clé (dans KP-ABE).

Pour une évaluation plus complète de l'ABE, dans cette recherche, nous analysons également l'impact de l'utilisation d'attributs numériques avec des attributs de chaîne.

Nous pensons que, bien que l'utilisation d'attributs numériques puisse être coûteuse, elle fournit une expressivité supplémentaire dans les définitions de politique, en particulier dans CP-ABE.

À titre d'exemple, il peut y avoir des situations où l'accès aux données doit être limité à un seul modèle de périphériques, libéré après une certaine date (qui peut être représentée sous la forme d'un entier de 64 bits).

La principale déférence est que dans CP-ABE, la politique d'accès est incluse dans le chiffré et les attributs sont inclus dans la clé de déchiffrement, alors que dans KP-ABE, c'est exactement l'inverse. Comme ce qui est montré dans la figure suivante :

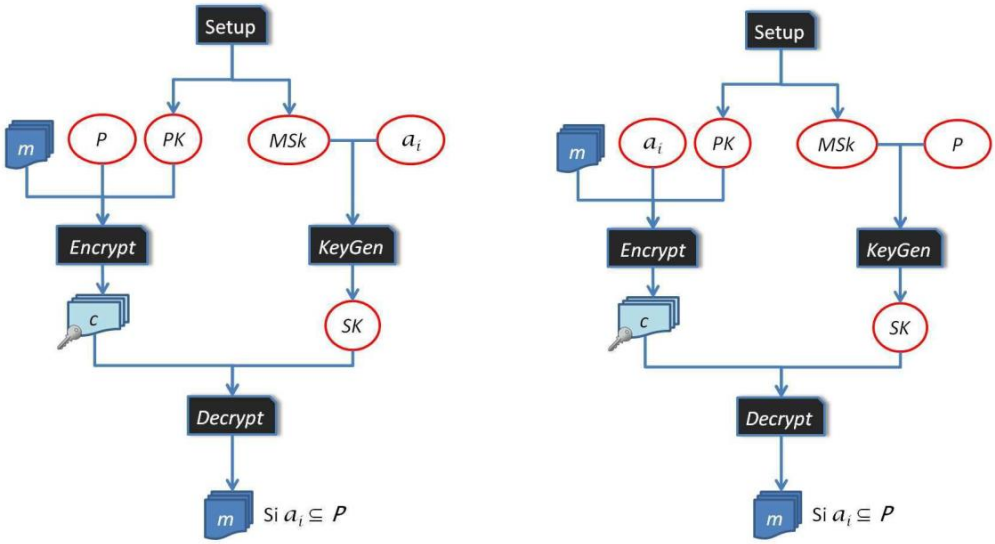


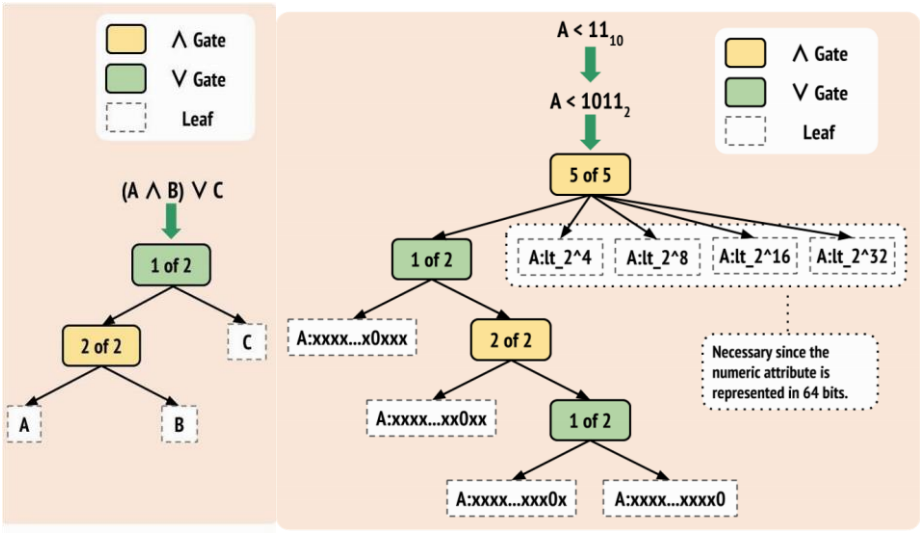
Figure 2.10_ Schémas fonctionnels de CP-ABE et KP-ABE

2.2.4 Attributs numériques dans ABE

Selon la conception originale de CP-ABE [10], les politiques d'accès sont exprimées comme conjonction de prédicats booléens, par exemple, P (i.e. P = vrai), ou P < n avec n ∈N. Elles et sont représentées sous forme d'arbres. Les nœuds feuilles de ces arbres (par exemple, A, B et C sur la figure 4 (a)) sont des attributs, tandis que les nœuds internes représentent des portes de seuil logiques de la forme K de N, ce qui signifie que, pour qu'un ensemble d'attributs satisfasse le sous-arbre enraciné dans une telle porte, l'ensemble doit (récursivement) satisfaire au moins K des N sous-arbres du nœud interne. Un nœud feuille, c'est-à-dire un attribut, est satisfait par une clé, si un tel attribut est associé à la clé.

Prenons l'exemple de la figure 4 (a), la politique : (A∧B) ∨C se traduit par un arbre à trois feuilles et deux portes de seuil intérieures. L'opérateur booléen ∧ est traduit en une porte 2 sur 2 (c'est-à-dire que les deux sous-arbres connectés à cette porte doivent être vrais, pour que cette porte soit considérée

comme vraie), tandis que l'opérateur ∨ comme une porte 1 sur 2 (c'est-à-dire, si au moins un des nœuds connectés à cette porte est vrai, cette porte sera considérée comme vraie)



(a) Politique simple (b) Politique avec attributs numériques

Figure 2.11_ Traduction de la politique d'accès CP-ABE.

Un attribut numérique, tel qu'A = 9, peut être traduit en un ensemble d'attributs simples indiquant la valeur de chaque bit dans la représentation binaire de l'attribut. Par exemple, en utilisant une représentation 64 bits pour un entier, l'attribut $A = 9_{10}$ est 1001_2. Il est traduit en :

A : xxxx...1xxx, A : xxxx...x0xx,

A: xxxx...xx0x, A: xxxx...xxx1,

A: eq_09, A:gt_2ˆ02, A: lt_2ˆ04, …

Cela représente la traduction binaire de 9 (x est une valeur de bit générique), plus un attribut de correspondance exacte (A : eq_09), et d'autres attributs, par exemple, ceux de la forme A : lt_2 ^ N) et A : gt_2ˆN (A> 2 ^ N), qui sont des représentations « compressées » des bits restants, requises en raison de la représentation sur 64 bits d'un attribut numérique.

Les clauses numériques uniques peuvent être converties en arborescences d'accès d'attributs simples. La figure 4 (b) montre la translation d'A <11.Comme nous pouvons le voir, même les politiques de contrôle d'accès simples impliquant des attributs numériques génèrent des arbres assez complexes,

avec un impact conséquent sur les performances des opérations cryptographiques. Pour mieux comprendre cet impact, nous avons mesuré le temps d'exécution du chiffrement CP-ABE à l'aide de politiques simples de la forme A <2 ^ X, où X varie de 1 à 24. La figure 4 (c) présente nos résultats, expérimentés sur un Raspberry Pi. Nous tirons deux observations importantes pour la pratique : (1) le temps de chiffrement (qui dépend de la taille de l'arbre) ne croît pas directement avec la taille du nombre considéré, mais plutôt avec le « nombre minimum d'octets » nécessaire pour représenter le nombre ; (2) les nombres d'une puissance de 2 génèrent des arbres d'accès plus simples, avec un temps de chiffrement réduit par conséquent. De plus, pour une puissance de 2, plus le bit le plus significatif à 1 est proche de la taille du mot de bit utilisé (c'est-à-dire 8, 16, 24 ou 32), plus l'arbre d'accès correspondant sera simple. Par exemple sur la figure 4 (c), la politique d'accès A <256 (2 ^ 8) génère un arbre d'accès avec onze feuilles et deux portes ET, nécessitant ≈1,941 sec pour le chiffrement ; tandis que, le chiffrement avec A <32768 (2 ^ 15) génère un arbre d'accès plus simple avec seulement trois feuilles et une porte ET, nécessitant ≈0,547 sec. Notez que les considérations ci-dessus sur l'utilisation des attributs numériques peuvent également être étendues au schéma KP-ABE dans [9], car il utilise une construction d'arbre d'accès similaire à celle de [10].

2.2.5 Problèmes Liés à l'Application du ABE à l'environnement IoT

Le système de sécurité ABE est devenu intéressant, notamment à travers ses multiples fonctions, qui sont sa focalisation sur la protection de la vie privée et l'incapacité du fournisseur de services à obtenir un accès non crypté aux données. Le propriétaire des données contrôle le processus de cryptage et leur partage avec une grande précision. Cependant, ABE est une méthode de cryptage coûteuse en termes de capacité de calcul. En effet, s'il ne pose pas de problèmes particuliers pour une application dans le cloud, ce n'est pas le cas pour l'implémentation sur des appareils avec des contraintes de ressources. L'adapter à l'environnement IoT nécessite de prendre en compte de nombreux aspects liés aux limites des objets connectés (mémoire, processeur, puissance, bande passante).

L'un des meilleurs moyens de mettre en œuvre ABE dans un écosystème IoT consiste à utiliser le modèle Fog ou Edge Computing, via l'externalisation des processus informatiques Zhang et al [47]. Ces auteurs ont proposé un protocole à utiliser dans un environnement IoT où le propriétaire des données transfère d'abord au nœud de relais, la structure d'accès qui génère un cryptage intermédiaire qui est renvoyé au nœud IoT pour le calcul de cryptage final avant qu'il ne soit renvoyé au fournisseur de services cloud, ce qui signifie une plus grande utilisation du réseau et donc Augmentation de la consommation d'énergie du nœud IoT. Une autre approche a donc été envisagée pour adapter le

chiffrement par attribut à l'Internet des objets. Cette approche propose de remplacer les processus de consommation liés aux applications à deux lignes par des opérations sur des courbes elliptiques.

2.3 Conclusion

Dans ce chapitre, nous avons présenté un aperçu général sur la sécurité des données personnelles dans l'environnement IOT et le Cloud Nous avons, dans un premier temps, discuté les solutions cryptographiques d'une manière générale et ensuite le la solution chiffrement ABE

Troisième partie

Protection cryptographique concepts et outils scientifiques pour le chiffrement basés sur les attributs

3. Introduction

Tout schéma de chiffrement fait appel à des outils mathématiques spécifiques. Dans ce qui suit, nous allons rappeler les outils et les notions mathématiques nécessaires à la compréhension formelle du chiffrement basé sur les attributs.

3.1 Les Groupes

L'ensemble G muni de la loi de composition interne notée • : G × G → G forme une structure algébrique de groupe notée (G, •) si la loi est :

- Associative,
- Symétrique et
- Admet un élément neutre. L'élément neutre est noté 1 en notation multiplicative (×) et 0 en notation additive (+).

Un groupe G est dit *fini*, si sa cardinalité est finie i.e. son nombre d'éléments. Le cardinal fini d'un groupe est appelé son ordre de G. Si cet ordre est premier, et qui est noté *p*, alors on dira que le groupe G est d'ordre premier *p*.

Un élément g ∈ G est dit générateur du groupe G, si ∀x ∈ G, ∃n ∈ N tel que $x = g^n$ ($g.g...g$ n fois). Le groupe G est dit *cyclique*, s'il est *fini* et qu'il admet un seul élément générateur.

Concrètement, les groupes cycliques sont construits à partir des corps finis comme par exemple Z/P_z avec p premier (également noté Z^*), ou des courbes elliptiques.

3.2 Courbes elliptiques (Équation de Weierstrass)

Une courbe elliptique est l'ensemble des points avec des éléments d'un champ fini décrit par l'équation :

$$y^2 = 3x^3 + ax + b$$

La géométrie peut être utilisée pour regrouper les points d'une courbe elliptique. Une courbe elliptique

Le groupe G comprend les points de la courbe elliptique, Q, et une opération de groupe appelée addition, notée '+'. De plus, le point à l'infini sert d'élément d'identité, où l'ajout de points sur une courbe elliptique est la fermeture. La loi d'addition sur le groupe de courbes elliptiques a des propriétés qui sont présentées comme suit

(a) $P + \phi = \phi + P = P \; \forall \; P \in E$.

(b) $P + (-P) = \phi \; \forall \; P \in E$.

(c) $P + (Q + R) = (P + Q) + R \; \forall \; P, Q, R \in E$.

L'opération d'addition de groupes de courbes elliptiques a la propriété d'être commutative, c'est-à-dire pour tous $P, Q \in G$, puis $P + Q = Q + P$.

3.3 Cryptographie à base de courbes elliptiques

Les courbes elliptiques ont été proposées en cryptographie dans les années quatre-vingt par Miller [92] et Neal [99]. La cryptographie à courbe elliptique (ECC) est un type de cryptage à clé publique basé sur des groupes de courbes elliptiques sur des champs finis [12]. La longueur des chaînes de bits manipulées dépend de la taille du groupe utilisé.

Les déférents schémas de chiffrement se basent sur des problèmes algorithmiques dit difficiles. A titre d'exemple, la sécurité du RSA est basée sur la difficulté de factoriser un grand nombre entier en facteurs premiers. L'hypothèse de sécurité de RSA affirme que si un algorithme permet de résoudre ce problème de factorisation facilement alors il pourra casser la sécurité du RSA. Un autre problème difficile est le logarithme discret qui permet de définir un ensemble de problèmes difficiles sur les groupes cycliques d'ordre premier.

3.3.0.1 Problème du logarithme discret (DL)

Etant donné un groupe cyclique G d'ordre p et de générateur g. Le problème du logarithme discret revient à trouver x, connaissant g et g^n ; avec x choisi aléatoirement dans Z^e_p.

Cette notion sera utilisée pour démontrer la sécurité de notre schéma de chiffrement en prenant comme hypothèse de sécurité le problème de Diffie-Hellman bilinéaire décisionnel.

3.3.0.2 Le problème Diffe-Hellman bilinéaire décisionnel

L'hypothèse du problème décisionnel bilinéaire de Diffie-Hellman, noté (DBDH) est une hypothèse de difficulté algorithmique basée sur la difficulté de calcul des logarithmes discrets dans des groupes cycliques.

3.3.0.3 Définition 13 (Le problème Diffe-Hellman bilinéaire décisionnel)

Étant donné e, p, g, G^a, G^b, G^C, T, avec a, b, c ∈ Z^e_p, choisis aléatoirement et p premier, décider si T = e (g, g) ^{abc} ou généré aléatoirement.

Il est utile également de reprendre la définition donnée par Waters [144] pour le contexte d'ABE.

Un challenger sélectionne un groupe G0 d'ordre premier p, conformément au paramètre de sécurité choisi et g son générateur. Soient a, b, s ∈ Z^* choisis aléatoirement. Si le challenger fournit à l'adversaire (g, Ga, Gb, gn) alors cet adversaire ne doit pas distinguer le résultat valide e (g, g) ^{abs} ∈ G_T d'un élément quelconque Z ∈ G_T avec un avantage non négligeable.

Ceci nous amène à la formulation suivante de la notion d'avantage d'un algorithme pour résoudre un problème dans l'environnement de groupes finis symétriques d'ordre premier

Il existe une variante calculatoire du problème Diffe-Hellman bilinéaire décisionnel, dans laquelle le problème revient à calculer g^{xy} connaissant g, g^x et g^y.

3.4 Avantage d'utilisation des courbes elliptiques en cryptographie

Les courbes sur des corps finis d'ordre premier ont été utilisées comme une alternative au chiffrement asymétrique. Les principaux avantages de l'utilisation des courbes elliptiques en cryptographie se résument comme suit :

- Les groupes de courbes elliptiques permettraient des clés plus courtes, avec un niveau de sécurité similaire au groupe multiplicatif conventionnel d'un corps fini comme par exemple le RSA.
- En raison de la taille des clés relativement petite et des calculs relativement rapides, l'ECC devient le choix le plus utilisé pour le cryptage à clé publique, en particulier celles qui utilisent des capteurs (par exemple, pour atteindre un niveau de sécurité de 80 bits, il est nécessaire

d'utiliser un Clé de 1024 bits en RSA, alors que seule une courbe de 160 bits en ECC est nécessaire).

- La difficulté accrue pour résoudre le problème mathématique sous-jacent par rapport aux autres schémas de cryptographie à longueur de clé égale. Pour un niveau de sécurité donné, nous avons des chaînes de bits plus petites que d'autres chaines déduites des autres schémas. Le problème difficile sur lequel reposent les schémas ECC est le problème du logarithme discret (DLP) peuvent fournir un niveau de sécurité suffisant si les paramètres associés sont correctement choisis. On a une meilleure performance en termes d'implémentation [50].

3.5 Conclusion

Dans ce chapitre, nous avons décrit les outils qui seront nécessaires à la construction et à la validation (en termes de sûreté) d'un schéma de chiffrement basé sur les attributs.

Quatrième partie

Faisabilités du ABE sur les appareilles de l'internet des objets

4. Introduction

L'Internet des objets est une tendance croissante peuplant le monde de milliards d'appareils interconnectés. Ces dispositifs concernent des « choses » physiques, allant des capteurs portables aux smartphones et voitures intelligentes [1]. Malheureusement, bien que l'IoT ait le potentiel de permettre de nouveaux services innovants et de simplifier la communication entre les personnes et les objets, il apporte de nouveaux défis en matière de sécurité et de confidentialité. Par exemple, considérons un capteur compatible IP dans un système de santé intelligent, qui transmet les données médicales des patients à un serveur de soins de santé distant. Dans ce scénario, les données médicales véhiculées peuvent être acheminées via un réseau non approuvé ou peuvent être stockées dans un service cloud non approuvé, exposant des données potentiellement confidentielles à des cyberattaques.

Outre les problèmes génériques de sécurité et de confidentialité de l'IoT, le concept d'IoT distribué [1] présente des défis supplémentaires spécifiques au contexte. Les appareils envoient non seulement leurs données dans le cloud, mais peuvent également former un « Intranet des objets », communiquant entre eux et avec d'autres systèmes IoT. Par exemple, dans un système de santé intelligent, les appareils de la maison intelligente d'un patient peuvent avoir besoin d'interagir directement avec le système IoT de l'hôpital. Les entités collaboratrices peuvent ne pas être fiables ou les données transmises peuvent devoir être révélées uniquement à certaines parties sélectionnées. Ces défis nécessitent un besoin urgent d'authentification efficace et de mécanismes de contrôle d'accès précis, nécessitant des méthodes cryptographiques avancées.

En outre, un aspect important à prendre en compte lorsqu'il s'agit d'appareils IoT à ressources limitées est la fourniture de protocoles de gestion de clés flexibles ; qui a motivé les chercheurs à développer des solutions de sécurité efficaces pour les systèmes IoT [2].

4.1 Chiffrement basé sur les attributs et IoT

Ces dernières années, plusieurs protocoles de sécurité ont adopté le cryptage basé sur les attributs (ABE) comme élément constitutif dans différents environnements distribués [3], tels que l'IoT [4], les services cloud [5] et les systèmes médicaux [6]. Compte tenu des exigences susmentionnées dans les

scénarios IoT distribués et hétérogènes, ABE fournit un mécanisme de contrôle d'accès plus efficace par rapport aux algorithmes cryptographiques classiques [3], [6], [7], à savoir :

(i) il permet un contrôle d'accès précis basé sur les attributs des destinataires ;

(ii) il autorise des échelles indépendantes du nombre d'utilisateurs autorisés ;

(iii) il résiste aux attaques de collusion ;

(iv) ne nécessite pas de partage de clés ni d'algorithmes de gestion de clés entre les parties participantes (le propriétaire des données n'a pas besoin d'identifier le client de destination).

Outre ses avantages notables, un algorithme de révocation de clé approprié est toujours un problème difficile dans ABE (au-delà de la portée de cet article), et un effort de recherche continu [3]. Plus pertinent pour notre travail, ABE souffre d'une surcharge de calcul élevée [6], [8].

Cependant, la littérature manque encore d'une évaluation appropriée de l'efficacité de l'ABE sur les appareils à ressources limitées, largement utilisé dans le domaine de l'IoT.

Afin de mettre en lumière la faisabilité de l'ABE dans l'IoT, nous effectuons une analyse complète du coût des opérations ABE sur les appareils à ressources limitées.

4.2 Faisabilité d'ABE sur les objets IoT

Malgré l'argument de certains chercheurs concernant les performances non acceptables d'ABE sur les appareils mobiles [8], nous avons implémenté une bibliothèque ABE pour le système d'exploitation Android.

Dans le même ordre d'idées, dans cette section, nous discutons de la faisabilité d'ABE sur les appareils IoT à ressources limitées.

Dans la section 4, nous présentons un exemple de cas d'utilisation de soins de santé intelligents qui utilise CP-ABE pour le cryptage des données.

4.3 Cas d'utilisation : l'IoT dans le secteur de la santé

Pour donner une « idée » de la faisabilité de l'utilisation d'ABE dans des scénarios IoT du monde réel, nous considérons un cas d'utilisation simple mais réaliste : les soins de santé intelligents.

Nous avons mis en œuvre un prototype de système de lecteur de données de santé sans fil pour la surveillance, la collecte et le traitement des données à distance. Dans notre système, les mesures des capteurs médicaux sont collectées, cryptées avec CP-ABE et envoyées à un serveur de collecte de données (via Wi-Fi), par une carte Intel Edison équipée d'un e-Health Sensor Shield V2.0.

L'ensemble du processus est réalisé par deux services fonctionnant sur la carte : le premier lit les données des capteurs et les écrit dans des fichiers (un par type de données) ; le second chiffre les fichiers avec CP-ABE et les envoie au serveur, qui peut représenter une passerelle non approuvée, un service cloud ou un autre appareil IoT. La figure 5 (a) résume nos paramètres d'application.

Les exigences spécifiques de taux d'échantillonnage du système nous donnent des contraintes de latence claires en fonction de laquelle choisir la plage acceptable pour le nombre d'attributs et le niveau de sécurité.

En général, les taux de lecture et d'envoi doivent être à peu près les mêmes, afin de garantir la qualité de service attendue. De plus, comme la majeure partie du trafic dans notre scénario est constituée de données ECG, environ 1500 Octets / s (500 lectures de 3 octets par seconde), dans ce qui suit, nous nous concentrons sur les données ECG. Compte tenu des ≈80 ms pour la transmission de données (par paquet UDP), et des 45 ms en moyenne pour crypter le fichier de mesures avec AES, les opérations les plus coûteuses sont liées au CP-ABE. Afin de trouver un équilibre raisonnable entre le niveau de sécurité assuré et l'expressivité (en termes de nombre d'attributs), nous avons effectué des tests utilisant jusqu'à 10 attributs et un niveau de sécurité de 80 bits, mesurant la latence globale. En se référant à la figure 5 (b), la latence reste plus petite, ou proche d'une seconde (notre limite supérieure pour la latence) avec un maximum de 5 attributs. Nous pouvons conclure que CP-ABE peut être utilisé dans un tel scénario prenant en charge jusqu'à 5 attributs avec une sécurité de 80 bits. Notez que le temps de cryptage est un peu plus long que les résultats de la section 3.2, car : (1) le temps inclut le cryptage AES et la génération de clé par fichier ; et (2) le service de lecture d'arrière-plan est toujours occupé à enregistrer des données.

4.4 Conclusion

Nous avons montré la faisabilité de l'adoption de l'ABE dans des systèmes IoT représentatifs. Nos résultats peuvent être une référence pour les chercheurs et les concepteurs de nouvelles solutions de sécurité basées sur ABE. Nous pensons que les recherches futures devraient se concentrer sur l'amélioration de l'efficacité de l'ABE, via une sélection rigoureuse des attributs et des optimisations logicielles et matérielles pour la bibliothèque cryptographique. Notre analyse montre que la bibliothèque utilisée peut être considérablement optimisée via une gestion appropriée de la mémoire, un déploiement de structure de données personnalisé et une simplification des opérations arithmétiques cryptographiques en tenant compte des attributs d'entrée. De plus, compte tenu du fait que la complexité de CP-ABE et KP-ABE dépend du nombre d'exponentiations et d'opérations d'appariement effectuées par chacun de leurs algorithmes, des travaux futurs pourraient aborder la migration d'opérations arithmétiques complexes, telles que l'exponentiation, vers des accélérateurs matériels. (Par exemple, logique personnalisée sur les réseaux de portes programmables sur site) afin d'améliorer l'efficacité énergétique et le temps d'exécution total

Cinquième partie

Conception

5. Introduction

Dans le domaine de la santé, le cloud peut être considéré comme une plate-forme qui permet de stocker d'énormes volumes de données sur la santé (dossiers médicaux). Il sert également pour une gestion structurée des données entre les médecins et les patients. Une grande partie de données stockées dans le cloud e-santé sont très sensibles et doit être sécurisée afin de protéger la vie privée des patients et parvenir à assurer la confidentialité au sein du cloud. Dans ce chapitre, nous proposons une solution pour un système de cloud e- santé sécurisé. Nous commençons par décrire l'architecture générale de notre système. Ensuite, nous détaillons la conception de notre application.

5.1 Description de la Solution

Dans le système PHR (Personal Health Records), l'accès aux données stockées doit être contrôlé pour garantir la confidentialité et l'intégrité des données. Le modèle de contrôle d'accès permet de contrôler les autorisations d'accès, et les techniques de chiffrement/déchiffrement peuvent aussi renforcer le contrôle d'accès, assurer la confidentialité des données et des privilèges des utilisateurs, et sécuriser la distribution de ces derniers. De plus, les utilisateurs, notamment les patients, doivent garder leur l'identité anonyme dans le cloud pour se protéger des autres utilisateurs. La meilleure façon de protéger l'identité du patient dans le serveur cloud est l'authentification anonyme. Notre solution combine tous ces mécanismes (contrôle d'accès + chiffrement/déchiffrement + authentification anonyme) pour sécuriser un système de cloud e-santé.

A partir de notre étude de travaux existants (chapitre 2 sections 4 et chapitre 3 sections 3), notre solution englobe deux approches : le contrôle d'accès basé sur les attributs (ABAC) et sur le chiffrement CP-ABE et l'authentification anonyme sans certificat [42] qui est basé sur le problème de Diffie-Hellman (CDPH). L'application de ces deux approches dans notre système est décrite dans les sections suivantes.

5.2.1 Contrôle d'Accès basé sur les Attributs et sur le Chiffrement CP ABE

Dans notre système, l'utilisateur (patient ou médecin) possède un ou plusieurs attributs qui sont gérés par une autorité de confiance. Notre univers d'attributs est défini comme étant {Allergies, Diabète, Cancer, hypertension artérielle, Médecin, professeur, Ingénieur, Retraité, Etudiant, Homme, Femme, Dénutrition, Maigreur, Corpulence normale, Surpoids, Obésité13 } Notre modèle se repose aussi sur l'utilisation de l'approche de chiffrement par attributs CP- ABE qui incorpore un processus de génération des clés de chiffrement et de déchiffrement et la notion de politique d'accès basée sur des attributs, offrant ainsi des fonctionnalités de chiffrement et de contrôle d'accès. En effet, l'autorité de confiance définit les attributs pour chaque utilisateur et génère les clés secrètes qui sont une combinaison d'un ensemble d'attributs. Les propriétaires de données (médecins) définissent des politiques d'accès pour le chiffrement. Seuls les utilisateurs avec des attributs qui satisfont une politique d'accès aux données chiffrées peuvent déchiffrer ces données. Notre version de l'algorithme de CP-ABE est illustrée dans la figure suivante :

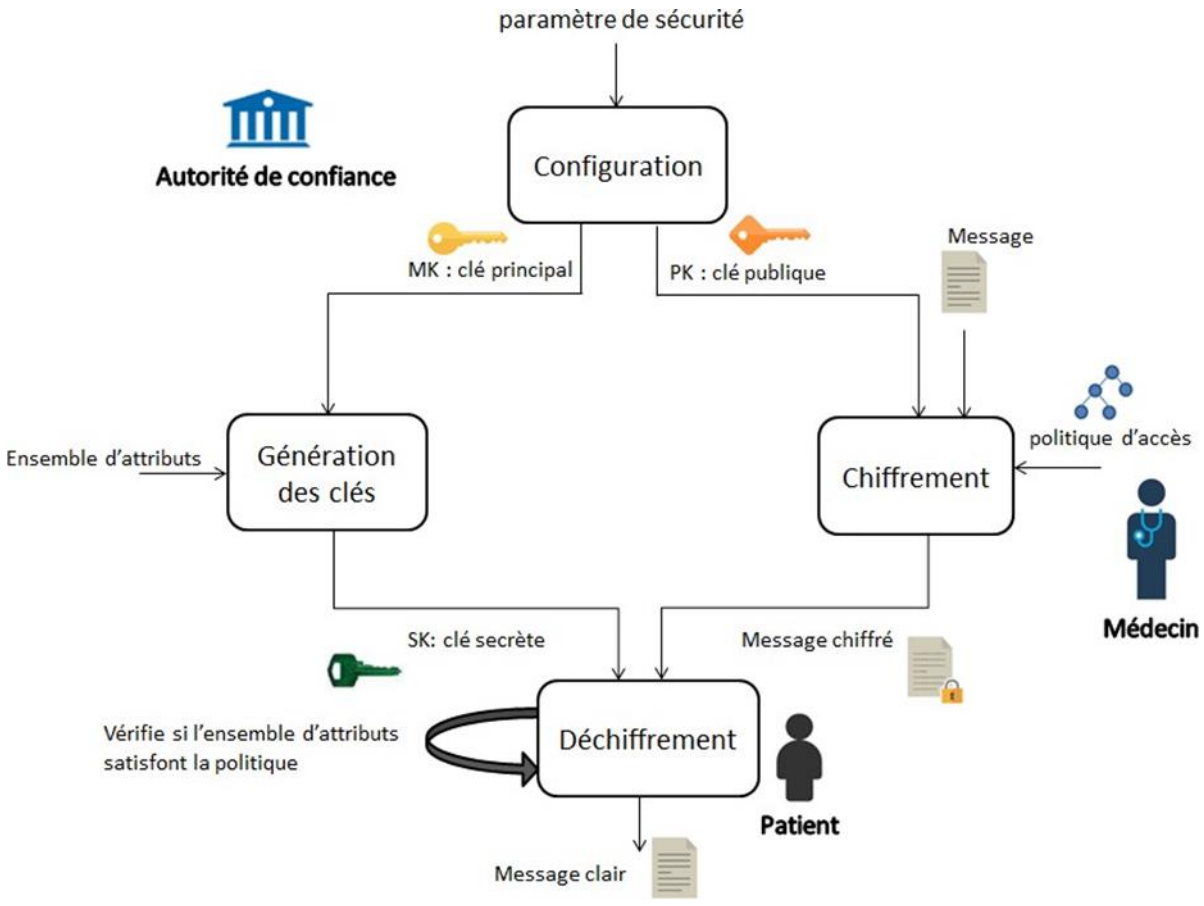


Figure 5.1 _algorithme CP ABE

Afin de mieux comprendre, nous allons la donner un exemple ; supposons que le patient 1 reçoit une clé pour les attributs {Retraité, Diabète} et que le patient 2 reçoit une clé pour les attributs {Retraité, Cancer}. Si le médecin chiffre un fichier et définit la politique étant {Retraité ∧ (Diabète v hypertensions artérielle)} alors le patient 1 pourra alors déchiffrer, tandis que le patient 2 ne pourra pas déchiffrer.

5.2.2 Architecture Générale

En résumé, notre système se compose de cinq éléments (Figure 5.2) : Cloud, Médecin (propriétaire de données), Patient (utilisateur), Autorité de confiance et proxy anonymat.

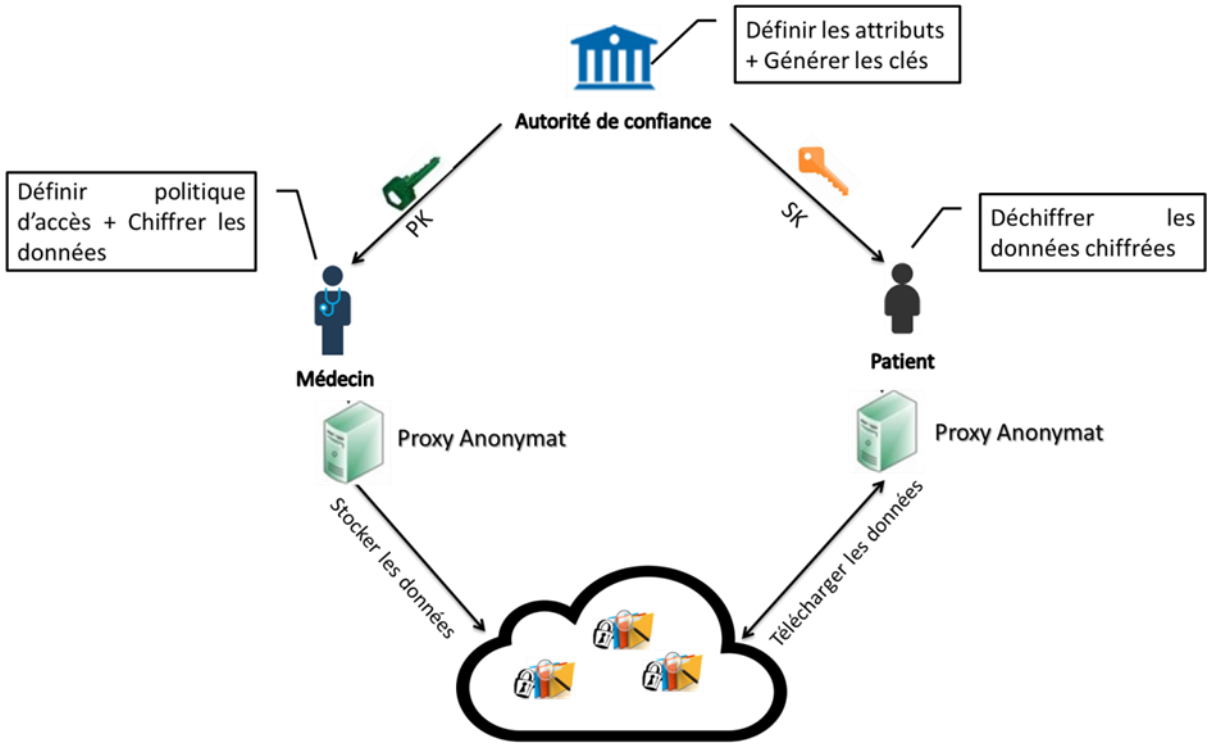


Figure 5.2 _ architecture du système

Chaque composant de notre système possède un rôle précis dans le système :

- Cloud : C'est une entité qui fournit un service de stockage de données. Il est chargé de contrôler les accès des utilisateurs extérieurs aux données stockées. Nous supposons que le Cloud est honnête mais curieux. C'est-à-dire qu'il exécutera honnêtement les tâches assignées dans le système ; cependant, il aimerait apprendre le plus d'informations possible sur les contenus chiffrés.

- Médecin (propriétaire des données) : Il s'agit d'un individu qui possède des données et qui souhaite les stocker dans le cloud externe pour faciliter le partage ou pour réduire les coûts. Le médecin est responsable de définir une politique d'accès (basée sur les attributs) et de l'appliquer à ses propres données qui souhaitent les chiffrer

- Patient : C'est une entité qui veut accéder aux données. Elle peut seulement consulter les données du cloud. Si un patient possède un ensemble d'attributs satisfaisant à la politique d'accès des données chiffrées, il pourra déchiffrer les données chiffrées par son médecin et obtenir les informations.

- Autorité de confiance : C'est une entité qui génère les clés publiques, principales et secrètes pour l'algorithme de chiffrement/déchiffrement CP-ABE. Il est chargé de définir et d'émettre les principaux d'attributs des utilisateurs. En fonction des attributs, il génère les clés secrètes (SK) de déchiffrement.

- Proxy d'anonymat : c'est une entité qui permet de rendre l'utilisateur anonyme dans le cloud lors de stockage ou téléchargement des données chiffrées.

5.3 Etude conceptuelle de notre application

Pour mettre en place notre solution, nous allons développer une application qui doit satisfaire les besoins fonctionnels suivants :

- Chiffrement/Déchiffrement à base d'attribut (CP-ABE) des données.
- Stockage des données dans le cloud.
- Téléchargement des données du cloud.
- Partage des données entre les utilisateurs
- Authentification anonyme sans certificat des utilisateurs.

5.3.1 Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation est destiné à représenter les besoins des utilisateurs par rapport au système. Dans notre solution, nous distinguons trois acteurs :

–médecin : un individu jouant un rôle au sein de l'hôpital et accède aux dossiers médicaux de ses patients

–patient : un individu qui accède à son dossier médical.

– autorité de Confiance (AC) : est responsable de la gestion des attributs des utilisateurs et des clés

5.3.2 Gérer les clés

Elle permet à l'administrateur de confiance de définir les clés de chiffrement (PK) et déchiffrement (SK)

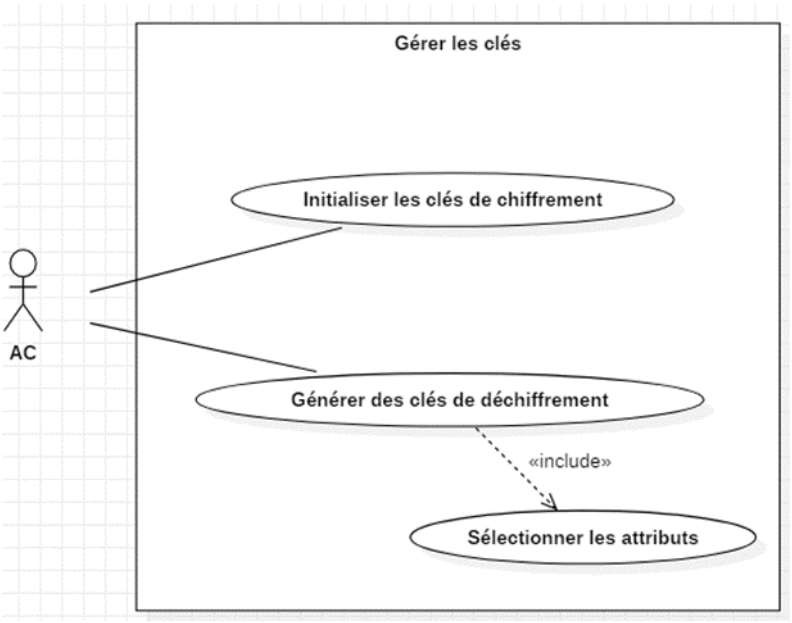


Figure 5.3_Diagramme cas d'utilisation Gerer des clés

Cas d'utilisation	Acteurs	Description
Initialiser les clés de chiffrement	Autorité confiance	Définir les deux clés: PK (clé publique) pour le chiffrement et MK (clé principale) pour la génération de clé de déchiffrement
Générer les clés de déchiffrement	Autorité confiance	Génération de la clé SK (clé secrète) pour le déchiffrement après avoir sélectionné un ensemble d'attributs de l'univers qui correspondent à l'utilisateur choisi

Tableau 3 : Descriptions des cas d'utilisation du diagramme Gérer les clés

5.3.3 Gestion des clés

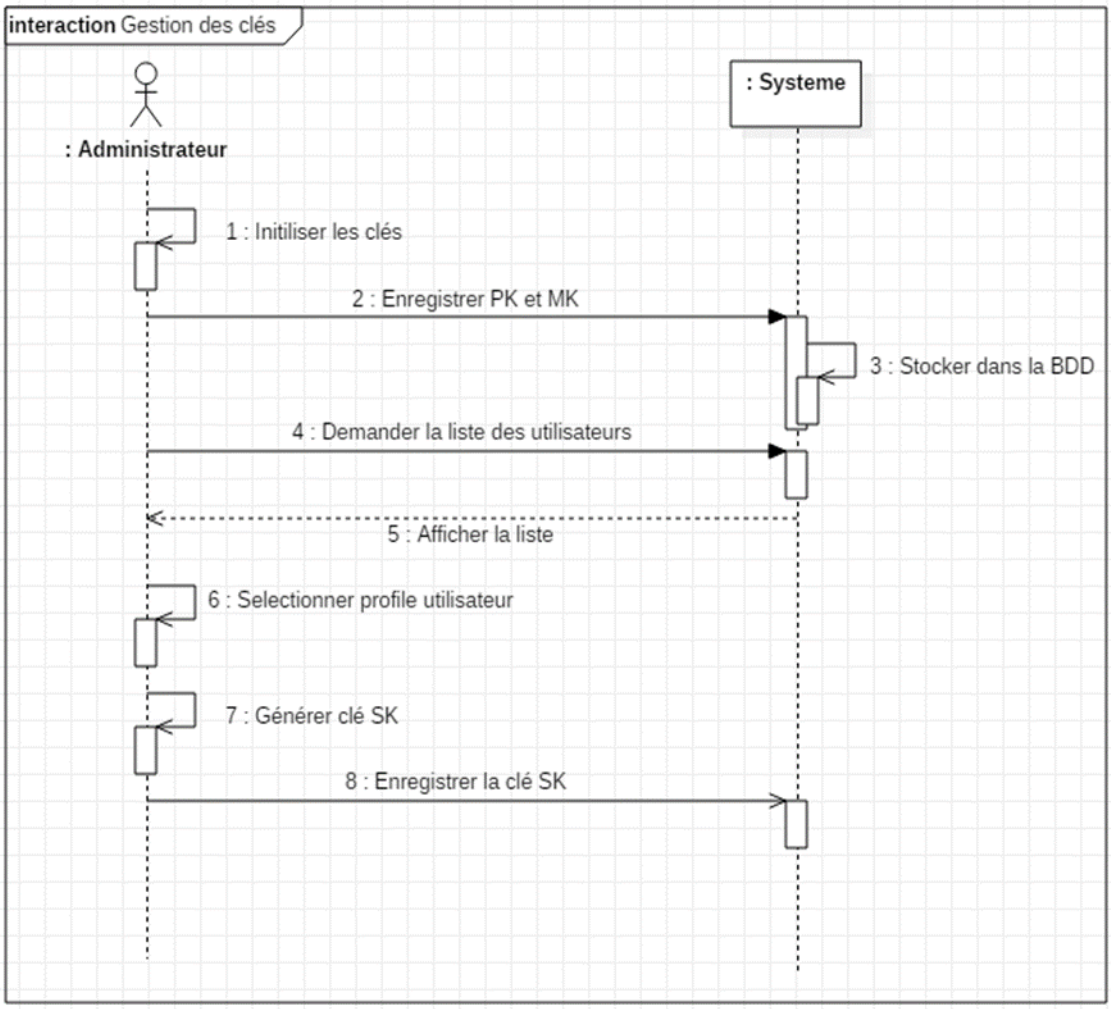


Figure 5.4_L'administrateur établit deux étapes

a. Initialisation des deux clé (publique PK, principale MK), La clé publique sera envoyée à l'utilisateur (médecin) pour que ce dernier puisse chiffrer.

b. Génération des clés secrètes SK, pour cela l'administrateur doit avant tout accéder aux profiles des utilisateurs afin de déduire leurs attributs. Ensuite il génère la clé SK pour chaque utilisateur (médecin, patient) à l'aide de la clé principal MK et l'ensemble d'attributs de dernière à l'utilisateur pour qu'il puisse déchiffrer.

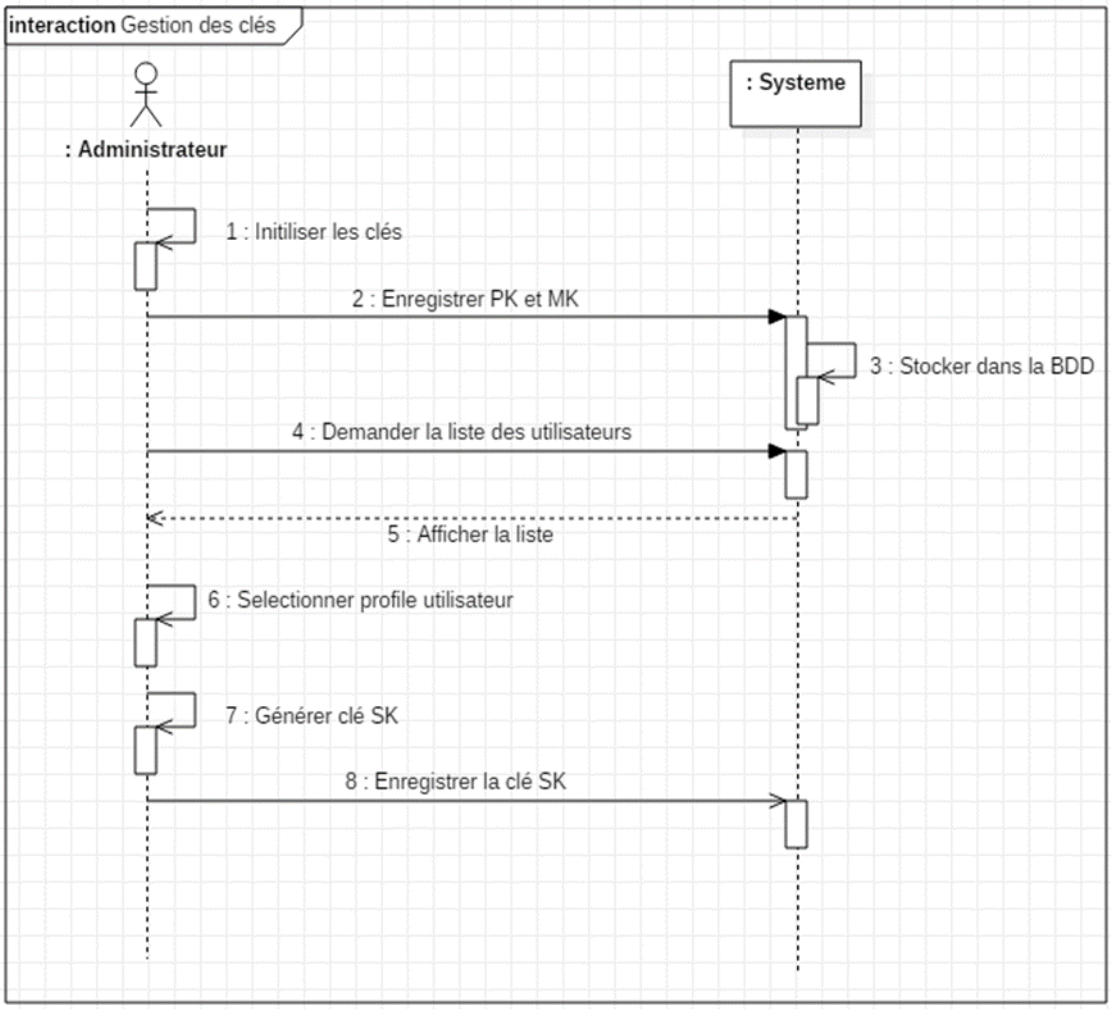


Figure 5.5_ diagramme de séquence ‘’Gestion des clés’’

5.3.4 Chiffrement et Stockage

Comme déjà décrit précédemment, le médecin définit la politique d’accès. Ensuite, le système exécute l’algorithme de chiffrement en utilisant la fiche, la politique et la clé PK. Enfin, Il accède au cloud de manière anonyme pour stocker la fiche chiffrée. Le diagramme de séquence suivant illustre ces étapes :

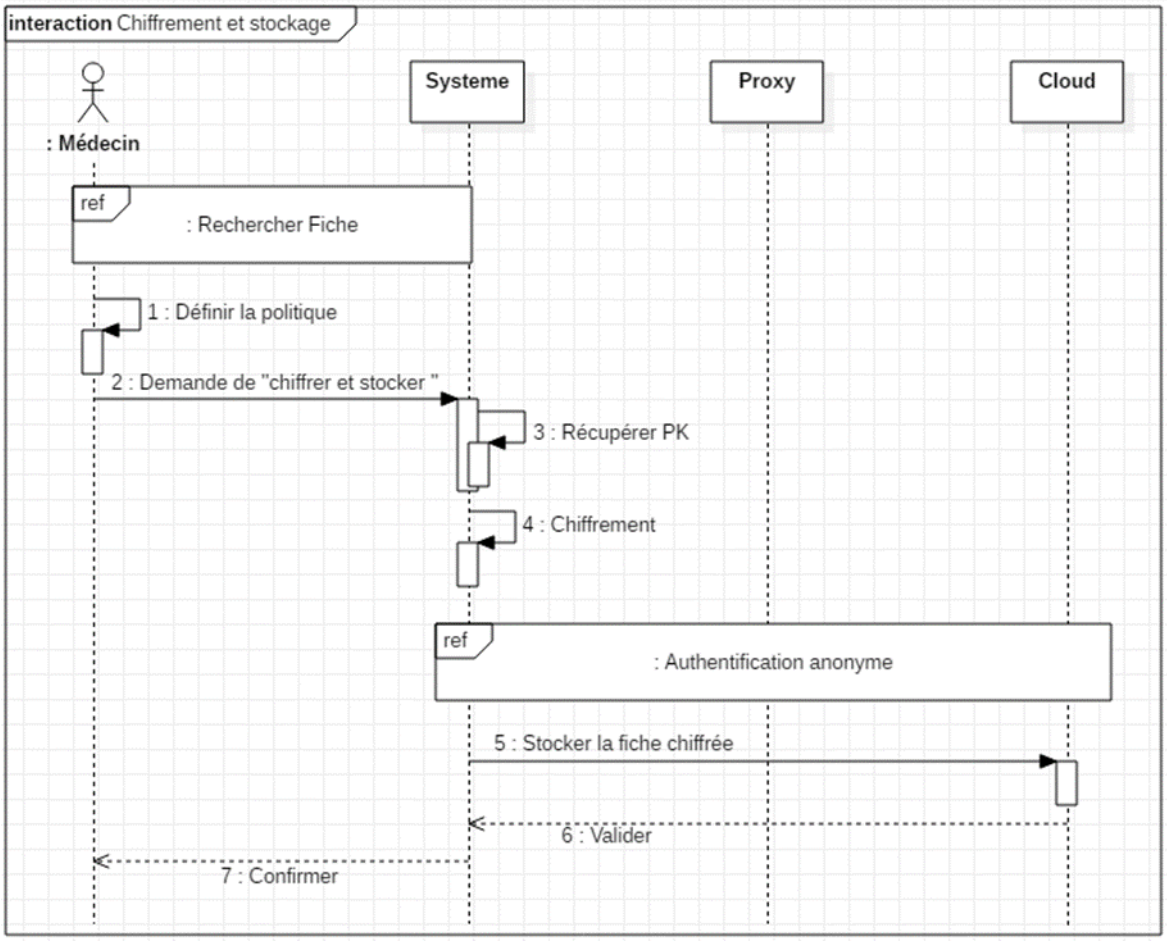


Figure 5.6 _ diagramme de séquence ‘'Chiffrerement et stockage’’

5.3.5 Téléchargement et Déchiffrement

L'utilisateur (médecin, patient) recherche une fiche dans le but de la télécharger et déchiffrer. Le système récupère la fiche de suivi désirée en établi une connexion anonyme avec le cloud. Ensuite, il récupère la clé SK pour déchiffrer la fiche en vérifiant si les attributs de l'utilisateur correspondent à la politique d'accès. Si oui alors le système pourra déchiffrer la fiche sinon un message d'échec sera affiché à l’utilisateur. Le diagramme de séquence suivant illustre ces étapes :

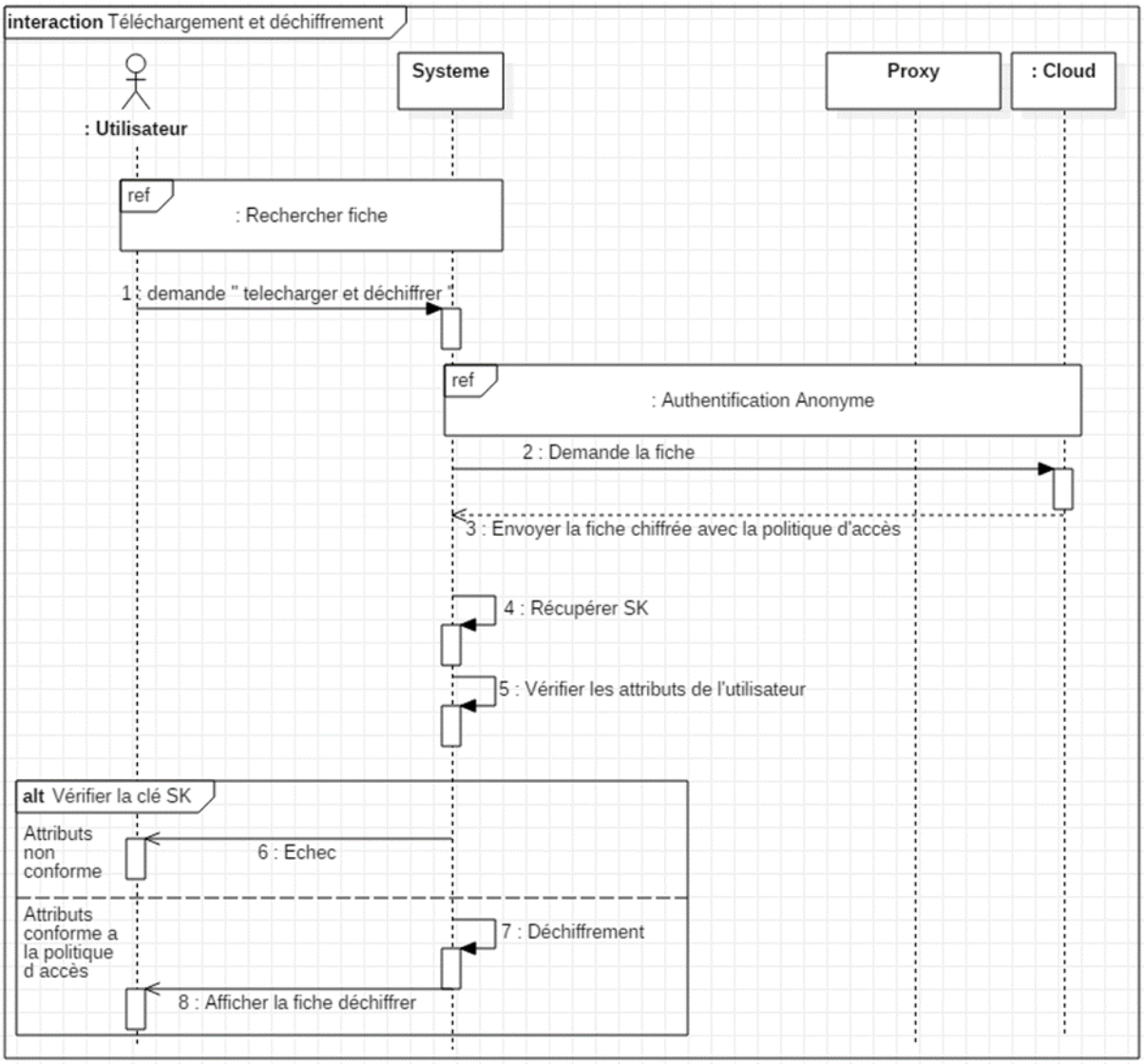


Figure 5.7 _diagramme de séquence ‘’Téléchargement et Déchiffrement’’

5.4 Schéma relationnelle de la base de données

Les données de notre application sont stockées dans une base de données que nous allons concevoir son schéma relationnel à partir du diagramme de classe en appliquant des règles de transformation. Cela fait l’objet de cette section

5.4.1 Diagramme de classe

Notre diagramme de classe présenté dans la figure 5.7 décrit la structure du système en montrant les classes intervenantes et les relations entre elles :

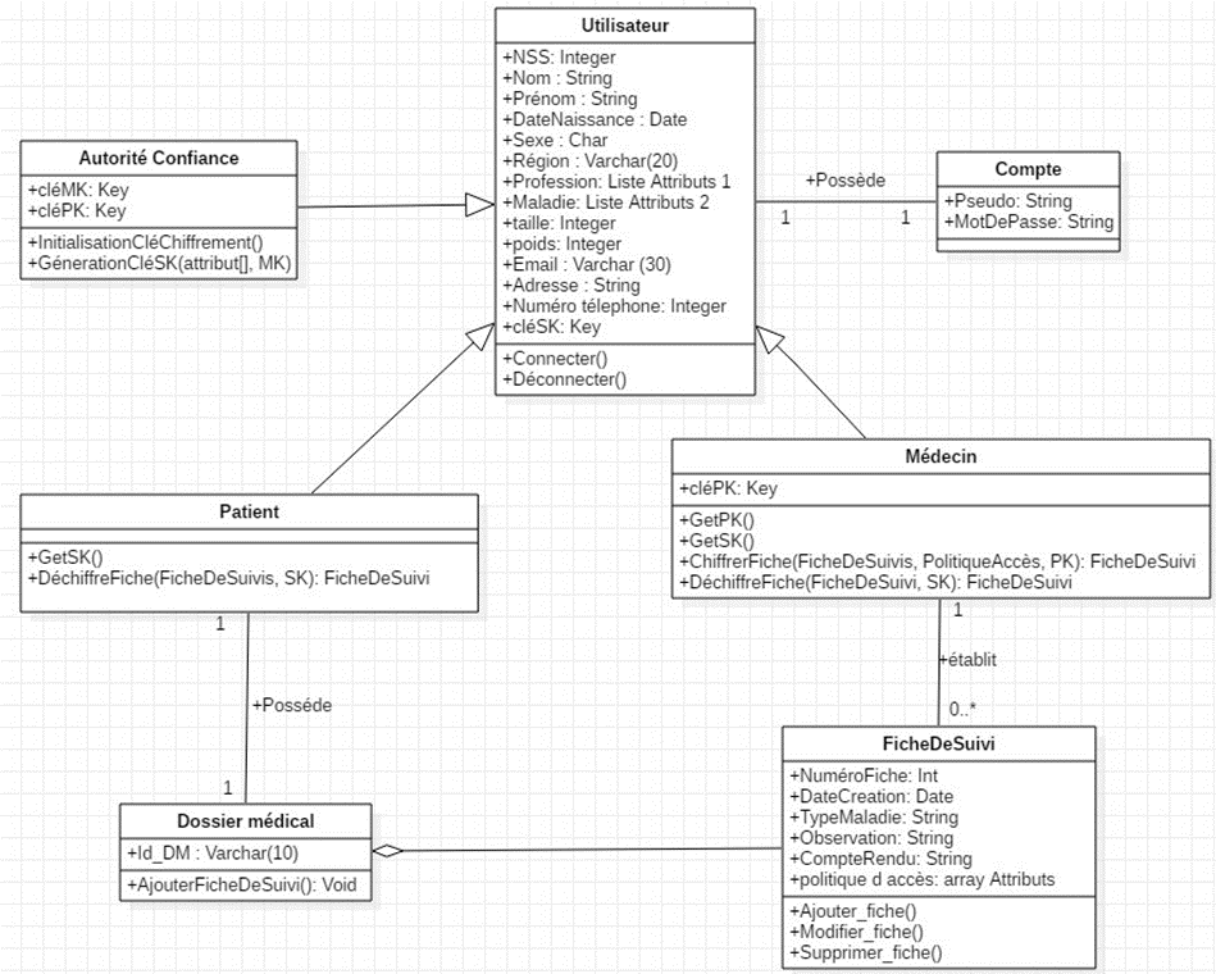


Figure 5.8 _ diagramme de classe

5.5 Conclusion

Dans ce chapitre, nous avons décrit notre approche pour un système du cloud e-santé sécurisé. L'approche se repose sur le contrôle d'accès ABAC avec chiffrement CPABE qui offre une solution efficace pour garantir le contrôle des données et sur l'authentification anonyme qui permet de garantir non seulement la confidentialité mais aussi la confiance des utilisateurs et. Pour mettre en place notre solution, nous avons conçu une application incluant toutes les fonctionnalités nécessaires. Dans le chapitre suivant, nous présenterons les étapes suivies dans l'implémentation et la réalisation de cette application.

Sixième partie :

Réalisation

6.1 Introduction

Nous allons présenter dans ce chapitre la partie réalisation de notre application qui a pour objectif de mettre en œuvre la solution décrite dans le chapitre précèdent. Pour ce faire, nous allons commencer tout d'abord par préciser l'environnement matériel et logiciel de travail. Ensuite, nous décrivons l'implémentation des approches proposées (contrôle d'accès basé sur le chiffrement CP-ABE et authentification anonyme sans certificat). Enfin, nous présenterons les principales interfaces graphiques de notre application.

6.2 Environnement de développement

Un environnement de développement se réfère à une suite d'applications et d'outils que nous avons installés sur nos machines pour nous aider à développer notre application. Comme montré dans la figure 42, nous avons utilisé deux machines virtuelles pour mettre en œuvre notre système. Les machines virtuelles sont créées en utilisant Oracle VM Virtuel Box15 avec les caractéristiques décrites dans le tableau 10. Notre système est implémenté comme une application client-serveur en utilisant le langage JAVA16 et l'environnement de développement Netbeans17 ainsi que ses interfaces graphiques JAVASwing18. Le serveur cloud est un serveur uwamp19 qui dispose d'un SGBD (système de gestion de base de données) appelé phpMyAdmin20 pour administrer notre base de données MySQL.

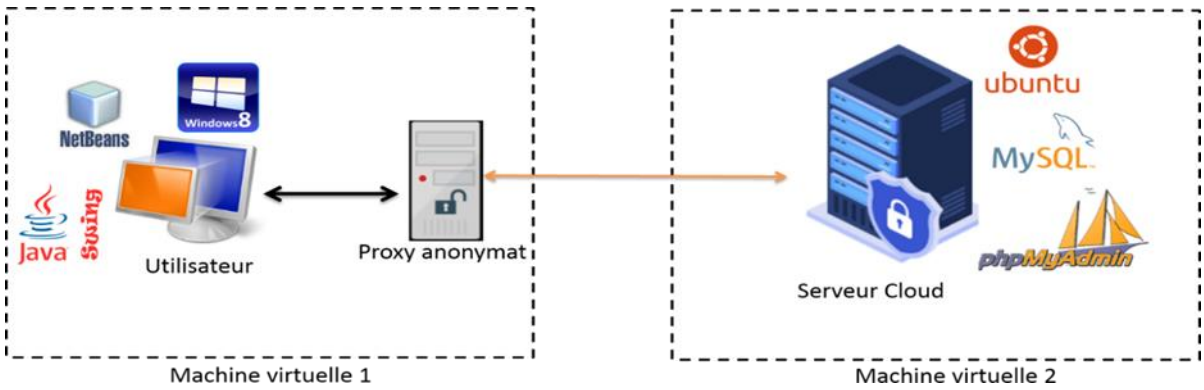


Figure 6.1 _Environnement de développement

[16] https://www.java.com/fr/

[17] https://netbeans.org/

[18] https://netbeans.org/features/java-on-client/swing.html

[19] https://www.uwamp.com/fr/

[20] https://www.phpmyadmin.net/

Machine virtuelle	1	2
Système d'exploitation	Windows 8	Ubuntu 18.04
RAM	8GO	1GO
Processeur	Intel® Pentium® CPU N3710 @1.60 GHz	Intel® Pentium® CPU N3710 @1.60 GHz
Acteurs présentés	Autorité de Confiance, Médecin, Patient et Proxy anonymat	Serveur cloud
Logiciels installées	MVJ, Netbeans 8.1 (JAVA, JAVASwing, DET ABE),	uWamp (MySQL, PHPMyAdmin)

Tableau 6.1 _ Caractéristiques des machines virtuelles.

6.3 Implémentation

Notre application est un ensemble de package (API) JAVA comme illustré dans la figure suivante :

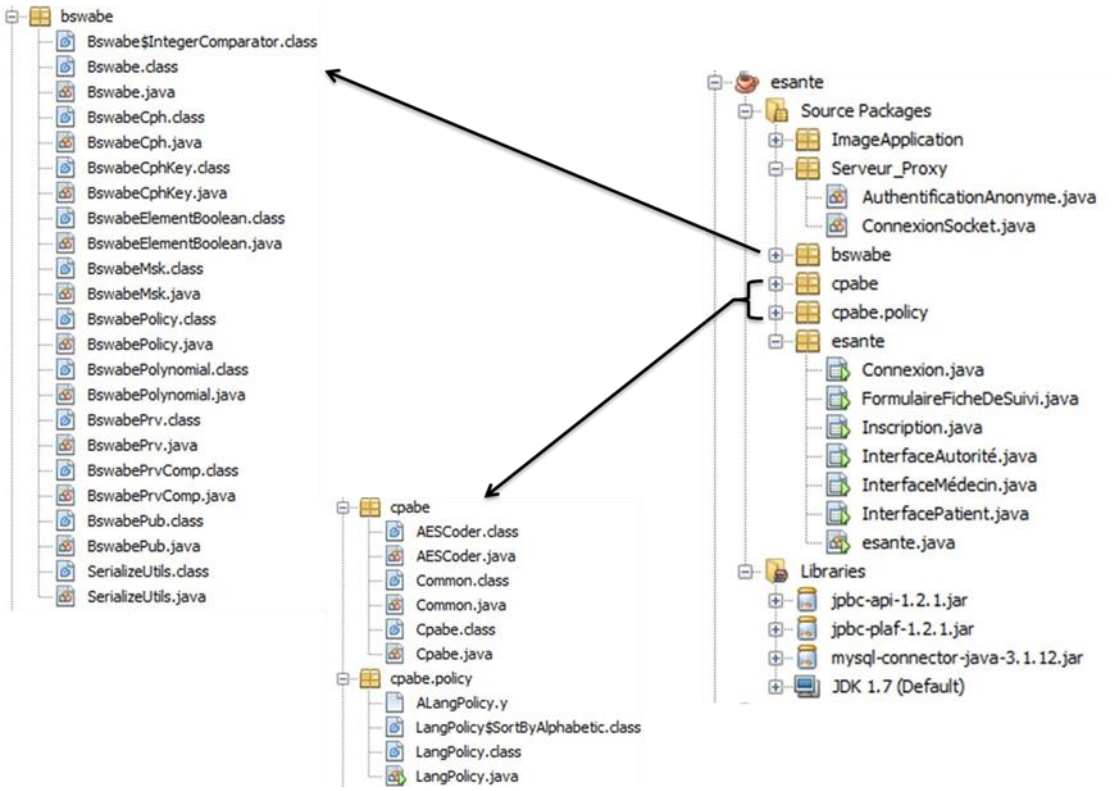


Figure 6.2 _ API de notre application

Dans ce qui suit, nous décrivons comment nous avons mis en place le chiffrement CP ABE en utilisant l'API DET ABE et comment nous avons implémenté le proxy anonymat.

6.3.1 Implémentation du Chiffrement CP ABE

Pour la construction du chiffrement CP ABE, nous avons déployé un ensemble pratique d'outils, appelé l'API DET ABE qui utilise l'API jPBC (java Pairing Based Cryptography), fondée sur la bibliothèque de cryptographie PBC. Cette dernière est livrée avec un support pour les deux chiffrements symétrique et asymétrique et dispose de solides primitives cryptographique, C'est une API qui permet de cacher les opérations cryptographiques de base en offrants aux utilisateurs une souplesse de programmation.

L'API DET-ABE contient plusieurs packagent, mais pour notre application, nous avons utilisé que les suivants :

- Bswabe qui fournit les classes concernant l'implémentation des clés MK, PK, et SK.

- Cpabe qui fournit les quatre fonctions de commande :
- cpabe-setup pour générer une clé publique et une clé master.
- cpabe-keygen pour générer une clé secrète en utilisant une clé master.
- cpabe-enc pour chiffrer avec une clé publique, un fichier sous une arborescence d'une politique d'accès spécifiée dans une langue de stratégie.
- cpabe-dec pour déchiffrer un fichier avec une clé privée.
- Cpabe.policy qui permet de définir l'arborescence de la politique en utilisant des règles de seuil qui se décrit comme « au moins attributs parmi », par exemple : au lieu de représenter un arbre avec des portes "AND" et "OR" en utilise respectivement 2 of 2 et 1 of 2 portes de seuil.

6.3.2. Proxy Anonymat

Nous avons créé serveur proxy qui exécute le processus d'authentification anonymat sans certificat (voir la section 2.2. Du chapitre IV). Ce serveur communique avec l'utilisateur à l'aide des sockets Java, les fonctions de communications (envoi et réception) sont illustrées dans la figure 6.3.

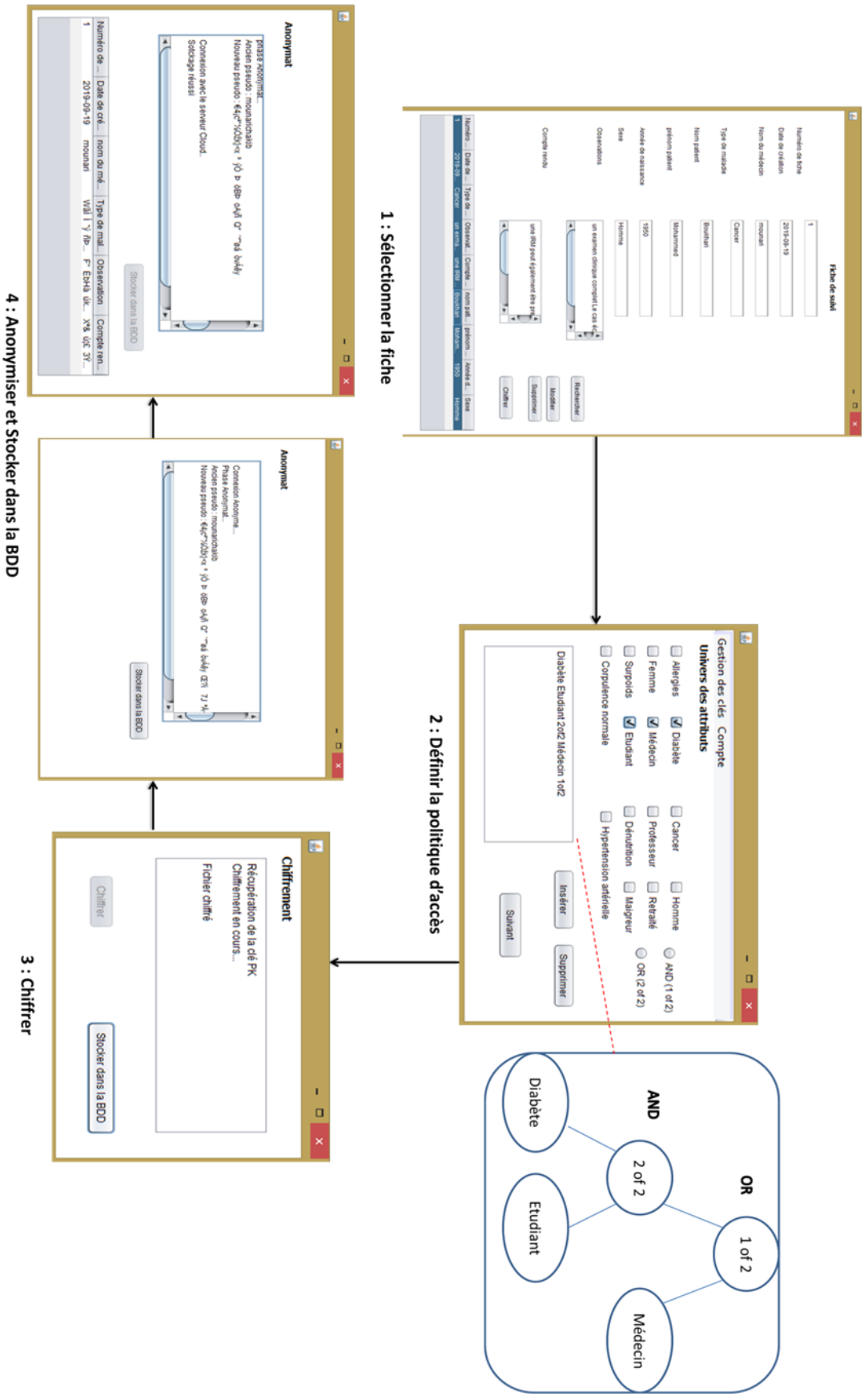


Figure 6.3 _ Chiffrement et Stockage d'une fiche.

6.4 Conclusion

Dans ce chapitre, nous avons décrit le processus de réalisation de notre application, en spécifiant les outils de développement et les librairies utilisés. Nous avons présenté les différentes interfaces graphiques qui composent les espaces des utilisateurs de notre système tout en exposant les fonctions qui constituent chaque espace. Nous avons achevé l'implémentation de notre application tout en respectant la conception élaborée.

Références

Références

- [1] l'union international de télécommunication https://www.futura-sciences.com/tech/definitions/internet-internet-objets-15158/ 14/06/2020 14 :25 PM

- [2] S. R. Moosavi et al., Session resumption-based end-to-end security for healthcare internet-of-things, IEEE CIT'15, Cloud computing selon Le National Institute of Standards and Technologie URLhttps://www.lebigdata.fr/definition-cloud-computing#:~:text=National%20Institute%20of%20Standards%20and,des%20application%20et%20des%20services. 22/ 6/2020 4.00 AM

- [3] edge computing selon le magazine I.A, cloud and big data URL https://www.lebigdata.fr/edge-computing-definition#:~:text=Le%20Edge%20Computing%20est%20une,directement%20où%20elles%20sont%20générées. 7/2020

- [4] Fog computing selon le journal JDN URL https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1440666-fog-computing-quel-role-pour-l-iot/#:~:text=Définition%20du%20fog%20computing,données%20issues%20d%27objets%20connectés. 7/2020

- [5] A. Sharma, T. Goyal, E. S. Pilli, A. P. Mazumdar, M. C. Govil et R. C. Joshi: A Secure Hybrid Cloud Enabled architecture for Internet of Things 7/2020.

- [6] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M.Rahmani et P. Liljeberg : On the feasibility of attribute-based encryption on internet of things devices. URL https://ieeexplore.ieee.org/abstract/document/7765239/ 05/2020.

- [7] CGTN : Jorf no 0129 du 6 juin 2010 p. texte no 42. Vocabulaire de l'informatique etde l'internet. URL https://www.legifrance.gouv.fr 06/2020.

- [9] M. Asim, M Petkovic et T Ignatenko: Attribute-based encryption with encryption and decryption outsourcing. URL http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1163&context=ism *18/6/2020*

- [10] Darrel Hankerson, Alfred Menezes et Scott Vanstone Springer: *Guide to Elliptic Curve Cryptography*, URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjVoPmj4NrrAhUK3aQKHTOCBPIQFjAAegQIAxAB&url=https%3A%2F%2Fwww.springer.com%2Fgp%2Fbook%2F9780387952734&usg=AOvVaw2O56pajyIYz2FMpElzuV51 06/2020

- [11] Ming Li, Shucheng Yu, Kui Ren et Wenjing Lou: Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiowner settings. *In Security and Privacy in Communication Networks*, URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiyrveW4NrrAhUI3qQKHbJqDUIQFjAAegQIBBAB&url=https%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F978-3-642-16161-2_6&usg=AOvVaw3l15ZUsqbZjc0EIgCFo7-w 06/2020

- [12] S. R. Moosavi et al., *Session resumption-based end-to-end security for healthcare internet-of-things*, IEEE CIT'15, 2015. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjn3-Sa3trrAhUlMewKHRV4ByAQFjAAegQIAxAB&url=http%3A%2F%2Fwww.divaportal.org%2Fsmash%2Frecord.jsf%3Fpid%3Ddiva2%3A932431&usg=AOvVaw1jtyWdO9aFYK4AsQw9EApx

- [13] S. SM. Chow, *A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation*, ACM SACMAT'16, 2016. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiKmaWm3trrAhVBhqQKHYv5BcsQFjAAegQIAxAB&url=https%3A%2F%2Fdl.acm.org%2Fdoi%2Fabs%2F10.1145%2F2914642.2914659&usg=AOvVaw1dZnPuPeksipp7I13lPrum

- [14] X. Li et al., *Smart community: an internet of things application*, IEEE Communications Magazine, 2011. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiU-eez3trrAhXLDewKHfBRB2gQFjAAegQIBBAB&url=https%3A%2F%2Fieeexplore.ieee.org%2Fdocument%2F6069711&usg=AOvVaw0Qdh2kfm0AWt0W943dUsGu

- [15] H. Ma et al., *Verifiable and exculpable outsourced Attribute-Based Encryption for access control in cloud computing*,

- [16] L. Ming et al., *Data security and privacy in wireless body area networks*, IEEE Wireless Communication, 2010. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiAx6DF3trrAhWpM-wKHSANC8EQFjAAegQIBhAB&url=https%3A%2F%2Fwww.researchgate.net%2Fpublication%2F308022977_On_the_Feasibility_of_Attribute-Based_Encryption_on_Internet_of_Things_Devices&usg=AOvVaw0uKindxeFNTKDke4epcnFt *

- [17] M. Ambrosin et al., *On the feasibility of attribute-based encryption on smartphone devices*, ACM MobiSys/IoT-Sys'15, 2015. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi74M3W3trrAhWxMewKHUvIByoQFjAAegQIBBAB&url=https%3A%2F%2Fdl.acm.org%2Fdoi%2F10.1145%2F2753476.2753482&usg=AOvVaw2FCjiePIlLTLgg1-FTkQBf

- [18] X. Wang et al., *Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT*, URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjwhqnl3trrAhUB36QKHRitD3oQFjAAegQIAhAB&url=https%3A%2F%2Fieeexplore.ieee.org%2Fdocument%2F6883405&usg=AOvVaw0-tM4oSYGM_kPrNQzfPIuG

- [19] V. Goyal et al., *Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data*, ACM CCS'06, 2006. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjuiuD93trrAhVFsKQKHXA1CrsQFjAAegQIBRAB&url=https%3A%2F%2Feprint.iacr.org%2F2006%2F309.pdf&usg=AOvVaw1Z-46Gy_487AQO69ILj5CU

- [20] A. Sharma, T. Goyal, E. S. Pilli, A. P. Mazumdar, M. C. Govil et R. C. Joshi: A Secure Hybrid Cloud Enabled architecture for Internet of Things URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjc_Z2L4NrrAhWFjqQKHT39DL8QFjAAegQIAxAB&url=http%3A%2F%2Fscholar.google.ae%2Fcitations%3Fuser%3D1t6o__4AAAAJ%26hl%3Dfr&usg=AOvVaw1F94i9fxSYQw9N9OW1lJAC. *05/2020*

- [21] J. Bethencourt et al., *Ciphertext-Policy Attribute-Based Encryption*, IEEE S&P'07, 2007. URL https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwixqOyL39rrAhUDGuwKHUJ9B2wQFjAAegQIAxAB&url=https%3A%2F%2Fwww.cs.utexas.edu%2F~bwaters%2Fpublications%2Fpapers%2Fcp-abe.pdf&usg=AOvVaw0VSl3-q1Ss24vhkpdrwvnb

- [22] R. NAgArAjAN, S. SELVAMuThuKuMArAN et R. ThiruNAVuKArAsu: A fuzzy logic based trust evaluation model for the selection of cloud services. In 2017 International Conference on Computer Communication and Informatics (ICCCI), pages 1–5, 2017. 39
- [23] Satoshi NAKAMoTo: Bitcoin: A peer-to-peer electronic cash system, 2008. 54.

- [24] Suyel NAMAsuDrA: An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 12 2017.

- [25] Koblitz NEAL: Elliptic curve cryptosystems. In Mathematics of computation, volume 48, pages 203–209, 1987.

- [26] Kim Thuat NguyEN, Maryline LAurENT et Nouha OuALhA : Survey on secure communication protocols for the internet of things. Ad Hoc Networks, 32:17 – 31, 2015. ISSN 1570-8705. Internet of Things security and privacy: design methods and optimization.

- [27] Kim Thuat NguyEN, Nouha OuALhA et Maryline LAurENT : Securely outsourcing the ciphertext-policy attribute-based encryption. World Wide Web, 21(1):169–183,2018. ISSN 1573-1413. 49,

- [28] Talal H. Noor, Quan Z. ShENg, Sherali ZEADALLy et Jian Yu: Trust management of services in cloud environments: Obstacles and solutions. ACM Comput. Surv., 46(1):12 :1–12 :30, juillet 2013. ISSN 0360-0300.

- [29] B. ONigA, S. H. FArr, A. MuNTEANu et V. DADArLAT : Iot infrastructure secured by tls level authentication and pki identity system. In 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pages 78–83, 2018. 44

- [30] D. Pandya, K. Ram, S. Thakkar, T. Madhekar, and B. S. Thakare, "An Overview of Various Authentication Methods and Protocols," Int. J. Comput. Appl., vol. 131, no. 9, pp. 25–27, 2015.

- [31] S. Milad Dejamfar and S. Najafzadeh, "Authentication Techniques in Cloud Computing: A Review," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 7, no. 1, pp. 95–99, 2017.

- [32] A. Djellalbia, N. Badache, S. Benmeziane, and S. Bensimessaoud, "Anonymous authentication scheme in e-Health Cloud environment," 2016 11th Int. Conf. Internet Technol. Secur. Trans. ICITST 2016, pp. 47–52, 2017.

- [33] Z. H. Zhang, J. J. Li, W. Jiang, Y. Zhao, and B. Gong, "An new anonymous authentication scheme for cloud computing," ICCSE 2012 - Proc. 2012 7th Int. Conf. Comput. Sci. Educ., no. Iccse, pp. 896–898, 2012.

- [34] J. Lopez, R. Oppliger, and G. Pernul, “Classifying public key certificates,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3545 LNCS, pp. 135–143, 2005.

- [35] A. Anwar, S. Ebersold, B. Coulette, M. Nassar, and A. Kriouile, “Vers une approche à base de règles pour la composition de modèles. Application au profil VUML,” International journal of Science and research. volume. 13, no. 4. pp. 73–103, 2007.

- [36] Miguel Morales-Sandoval and Arturo Diaz-Perez, “DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9311, pp. 20–35, 2015.

- [36] A. De Caro and V. Iovino, “jPBC: Java Pairing Based Cryptography,” Proc. - IEEE Symp. Comput. Commun., pp. 850–855, 2011.

- [37] The ownCloud developers, “ownCloud User Manual,” p. 68, 2015 disponible sur https://doc.owncloud.org/server/9.1/ownCloud_User_Manual.pdf.