République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département d'Informatique

Mémoire

Présenté par

DJELLALBIA Amina

Pour l'obtention du diplôme de Magister

Filière : Informatique

Option : Cloud Computing

Thème

Authentification Anonyme dans un environnement Cloud

Soutenu le : 29/09/2016 Devant le Jury composé de :

Nom et Prénom	Grade		
M. TARI Abdelkamel	Professeur	Université de Bejaïa	Président
M. BADACHE Nadjib	Professeur	CERIST, Alger	Rapporteur
M. BOUKERRAM Abdellah	Professeur	Université de Bejaïa	Examinateur
Mme BENZAID Chafika	MCA	USTHB, Alger	Invitée
Mme BENMEZIANE Souad	CR	CERIST	Invitée

Année Universitaire : 2015/2016

Remerciements

Au nom d'ALLAH le Tout Miséricordieux et que le Salut soit sur notre Prophète Mohamed aalayh assalet wa assalem.

Ce mémoire constitue le résultat d'un effort. Cet effort n'aurait pu aboutir sans la contribution d'un nombre de personnes, ainsi se présente l'occasion de les remercier.

Je remercie ***ALLAH*** *pour la volonté, la force, la santé et la patience qu'il m'a donné afin de réaliser et de pouvoir terminer ce travail.*

Mes remerciements, les plus vifs, ma profonde gratitude et mes respects s'adressent à Monsieur le Directeur du CERIST ***N. BADACHE****, de m'avoir offert l'opportunité de suivre une formation postdoctorale.*

Mes vifs remerciements vont à Monsieur ***A. TARI*** *pour l'honneur qu'il a bien voulu me faire en présidant le jury de ce travail.*

Je remercie ***Mme C. BENZAID*** *d'avoir accepté d'évaluer ce travail.*

Je remercie l'intérêt porté par Monsieur ***A. BOUKERRAM*** *d'avoir accepté d'être parmi le jury.*

J'adresse mes remerciements à Monsieur le Professeur ***N. BADACHE*** *d'avoir accepté d'encadrer ce travail et pour ses précieux conseils et orientations.*

J'adresse mes plus chaleureux remerciements à ***Mme S. BNEMEZIANE*** *qui est pour moi un exemple de rigueur, de m'avoir initié à l'univers de la sécurité informatique, d'avoir créé en moi le sens du savoir, lui exprimer toute ma reconnaissance pour son encadrement, ses remarques pertinentes et ses précieux conseils, son soutien constant, sa confiance et surtout sa patience. J'ai eu l'honneur de travailler sous sa direction pendant mon projet d'Ingéniorat, mon Magistère en espérant encore travailler avec elle dans le futur.*

Je remercie notre Responsable de la Division Sécurité ***M. NOUALI*** *pour sa bienveillance.*

Je remercie également mon mari ***Kaci*** *et ma très chère petite sœur, collègue et binôme* ***Sihem****.*

Je remercie également mes enseignants de la première année de Magistère pour leurs efforts voués à nous transmettre le savoir, notamment M. TARI et les Responsables du Département d'Informatique de l'Université de Béjaïa.

Je remercie également le service Formation du CERIST de nous avoir prodigué un excellent environnement de travail.

Je tiens à exprimer ma très grande affection à mes chers parents et beaux-parents pour leurs encouragements, leur patience et leur grand soutien durant ces trois années.

Dédicaces

A mes très chers parents qui ont toujours été là pour moi, qui m'ont donné un magnifique modèle de labeur et de persévérance. J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

A ***ma Mère****, qui m'a toujours tout donné, je ne saurai tout citer, ni trouver les mots pour la remercier de m'avoir inculqué le goût du savoir et de l'ambition.*

A ***mon Père*** *dont le rêve était toujours de me voir réussir.*

A mon cher mari « ***Kaci*** *», qui m'a apporté par son encouragement constant l'ingrédient le plus précieux de mon travail, qui m'a tant aidé de bon cœur, soutenu et conseillé, qu'il trouve dans ce travail, ma profonde gratitude et mon éternelle reconnaissance.*

A mes très chères sœurs « ***Salima*** *», «* ***Saida*** *» et «* ***Zahra*** *» qui m'ont donné l'exemple à suivre, ainsi que ma tante «* ***Fatima*** *».*

A mes deux chers frères « ***Zak*** *» et «* ***Abdou*** *» pour leur soutien dans la vie, ainsi que le petit bijou «* ***Mohamed Abdel Wahed*** *» qu'ALLAH le protège.*

A ma belle-famille qui m'a tant encouragé, j'ai vraiment eu la chance de vous avoir : à ***mes beaux-parents*** *ainsi que mes très chères belles sœurs «* ***Katia*** *» et «* ***Kahina*** *», leurs maris et leurs enfants, ainsi qu'à l'adorable «* ***Sabrina*** *».*

A mes collègues / amies « Sihem », « Karima », « Louiza », « Mounia », « Amel », « Kahina », « Batoul », « Hamida », « Ikram », « Sabira », « Hassina », « Wahiba ».

A notre chère Patrie et tout le monde musulman, qu'ALLAH les protège.

Que mes collègues de la promotion 2012-2013 de l'école doctorale trouvent ici mes estimes notamment mes collègues du CERIST.

A tous ceux qui me sont chers

Je leur dédie ce modeste travail.

Amina

Résumé

« Authentification Anonyme Adaptative dans un environnement Cloud »

Le Cloud Computing est devenu un concept majeur, faisant référence à l'utilisation des ressources et des serveurs répartis dans le monde entier et liés par un réseau comme Internet. Cependant, la confiance étant une notion floue et relative dans un tel environnement hétérogène, le but est de pouvoir utiliser les services offerts tout en étant indépendant de cette confiance. En effet, les préoccupations des utilisateurs quant à la manipulation de leurs informations personnelles, constituent l'obstacle principal lors de l'adoption des services Cloud. La protection des données personnelles permet de dissimuler les méta-données qui incluent les services Cloud consommés et les fréquences d'accès aux services. Dans ce contexte, nous avons proposé une approche afin de fournir une architecture complète et adaptative utilisant plusieurs technologies complémentaires, afin d'assurer une protection optimale des données personnelles des utilisateurs. Cela grâce à une authentification anonyme garantissant une consommation anonyme des services Cloud sur demande, tout en n'ayant aucune contrainte relative au niveau de confiance que prétend assurer le CSP.
Une première étude était d'identifier les différents types de menaces relatives à l'environnement Cloud par rapport aux données sensibles. Cela a permis de faire une classification des menaces/données sensibles, pour pouvoir offrir un système d'authentification anonyme dans lequel les utilisateurs pourront prouver qu'ils sont légitimes, sans révéler aucune information sensible qui pourra les identifier. Notre démarche pour concevoir et implémenter un tel système appelé «AnonCloud» comporte deux modèles:

- *Le premier étant le modèle de base, il s'appuie sur l'utilisation de tickets générés via la technique de signature en aveugle, proposant une nouvelle approche d'authentification des utilisateurs à partir de tickets d'accès anonymes.*
- *Le deuxième modèle étant le modèle étendu, conçu en combinant différentes technologies d'anonymat. Outre que la signature en aveugle, le routage en oignon assure un anonymat complet via l'encapsulation des informations d'identification (les tickets d'accès anonymes). Ce modèle offre donc une protection optimale notamment quant à l'adresse IP des utilisateurs qui présente un moyen potentiel de traçabilité.*

Le Cloud, avant d'être entièrement sûr, il devra intégrer des améliorations qui permettront de protéger au mieux les utilisateurs et ainsi leur garantir la confidentialité de leurs informations personnelles.

Abstract

« An Adaptive Anonymous Authentication for Cloud Environment »

Cloud Computing has become a major concept, that refers to the use of resources and servers located around the world, linked by a network such as the Internet. However, in the Cloud, trusting the Cloud Service Provider is blurred and relative concept in such a heterogeneous environment, the purpose is being able to use the services offered, while being independent of that trust. Indeed, an important barrier to the adoption of cloud services is user fear of privacy loss. One interesting issue from a privacy perspective is to hide user's usage behavior or meta-data which includes access patterns and frequencies when accessing services. In this context, we proposed an approach in order to provide a complete and adaptive architecture using complementary technologies to ensure maximum protection of sensitive user data. This objective is achieved via an anonymous authentication ensuring anonymous consumption of Cloud services and on-demand, with no constraint relative to the level of trust that claims to ensure the CSP.

A first study was to identify the different types of threats related to the Cloud environment and also different sensitive data. This helped us to classify threats / sensitive data to offer anonymous authentication system in which, users can prove that they are legitimate without revealing any sensitive information that could identify them. Our approach is to design and implement such an authentication system called «AnonCloud» which includes two schemes:

- *The first one is the basic scheme, it relies on the use of tickets generated via the blind signature technique which offers a new user authentication approach based on anonymous access tickets.*
- *The second model is the complete scheme, designed by combining different technologies of anonymity. In addition to the blind signature, the onion routing ensures complete anonymity via the encapsulation of credentials (the anonymous access tickets), providing so optimum protection particularly to the IP address of users which presents a potential way of traceability.*

The Cloud, before being entirely sure, it must integrates some enhancements to best protect its users and thereby, ensure the confidentiality of their personal information.

ملخص

« *مصادقة تكيفية مجهولة في عالم الحوسبة السحابية* »

اصبحت الحوسبة السحابية مفهوم واسع يشير الى استخدام الموارد الموجودة في جميع انحاء العالم، والمرتبطة بشبكة مثل شبكة الانترنت. الحوسبة السحابية توفر العديد من المزايا والفرص بالنسبة للمستخدمين، مع هذا تبقى مشكلة الثقة في مزود الخدمة السحابية مفهوم غير واضح ونسبى في مثل هذه البيئات غير المتجانسة. غرضنا هو إمكانية استخدام الخدمات المتوفرة مع الكون مستقلا عن هذه الثقة التي تشكل عائقا رئيسيا عند اعتماد خدمات الحوسبة السحابية خاصة عند فقدان الخصوصية من طرف المستخدمين.

النقطة الهامة من منظور الخصوصية هي اخفاء سلوك المستخدمين والبيانات الفوقية التي تشمل انماط وترددات الاستهلاك. في هذا السياق، ارتأينا الى اقتراح بروتوكول يوفر بنية كاملة وقابلة للتكيف تستخدم تقنيات مكملة لضمان اقصى قدر من الحماية لبيانات المستخدمين. هذا الهدف يتحقق عن طريق اقتراح مصادقة مجهولة للمستخدمين لاستهلاك الخدمات دون قيد على مستوى الثقة في مزود الخدمات ودون الكشف عن معلومات حساسة تمكن من التعرف عليهم. نظام المصادقة المجهولة المقترح يتبع نموذجين، النموذج الاول هو النموذج الأساسي، يعتمد على استخدام تذاكر مصنوعة عن طريق تقنية " التوقيع الاعمى" التي تمكن من توفير طريقة مصادقة جديدة للمستخدمين وذلك بطريقة مجهولة، النموذج الثاني هو النموذج الكامل، الذي يضيف على التذاكر المجهولة بتقنية " التوقيع الاعمى"، امكانية اخفاء العنوان الإلكتروني ا لذي يفتح الطريق للتعقب وذلك يتحقق بتغليف التذاكر وفق " تور بروتوكول" لتوفير شبكة اتصالات سرية وبذلك توفير الحماية المثلى للمستخدمين. الحوسبة السحابية قبل ان تصبح مضمونة كليا، يجب ان تدمج بعض التحسينات لضمان أفضل حماية للمستخدمين خاصة فيما يخص ضمان سرية المعلومات الشخصية الخاصة بهم.

TABLE DES MATIERES

TABLE DES FIGURES

LISTE DES TABLES

Introduction Générale

Contexte

L'essor de l'informatique dans tous les secteurs s'est fait conjointement avec son utilisation de plus en plus massive et son développement rapide. De nos jours, les environnements Cloud offrent aux utilisateurs l'illusion d'avoir une infinité de ressources informatiques à utiliser sans se préoccuper d'où viennent ces ressources, ni de comment elles sont maintenues. Le Cloud représente une plate-forme de l'externalisation et de traitement à distance des applications et des données qui se développe de plus en plus.
L'utilisation des serveurs informatiques dans les entreprises connait un changement radical. Le modèle de conception préconisé est de placer dans chaque entreprise un parc de serveurs pour répondre aux besoins. Le nouveau concept est de délocaliser les serveurs. La gestion de ces derniers est effectuée par un fournisseur ou prestataire de services spécialisé (CSP : Cloud Service Provider) via la location de services informatiques. Les entreprises s'abonnent donc à des services, plutôt que de devoir gérer leurs propres serveurs. C'est cette transformation qui est à l'origine de l'émergence du Cloud Computing connu comme «Everything-as-a-Service».

Pour les fournisseurs de services, le Cloud est défini par l'approche « 1-to-many »: ils doivent être en mesure de délivrer les services disponibles à un grand nombre d'utilisateurs. Pour les utilisateurs, le Cloud est vu comme un système de paiement à l'usage « pay-as-you-go » et des services à la demande: le Cloud peut faire gagner en efficacité de façon remarquable grâce à l'introduction de nouveaux modèles en libre-service informatiques et à la demande, ce qui n'était pas possible auparavant.
Le Cloud offre donc toute une série de services et est de plus en plus adopté pour fournir des applications et des ressources. Selon le cabinet Gartner[1], il faut s'attendre à une croissance avancée des utilisateurs dans l'environnement Cloud. D'ici la fin 2016, environ 30% des entreprises choisiront des services basés sur le Cloud, soit une progression de 16,5% du marché Cloud. Cette croissance sera, notamment, tirée par le Cloud d'infrastructure. La croissance globale du marché Cloud va se poursuivre en 2017 dans les mêmes proportions.

Problématique

Le Cloud étant une technologie à croissance rapide adoptant le principe de l'externalisation de l'infrastructure informatique, il demeure cependant des challenges à relever en termes d'outils d'administration, d'interopérabilité et notamment de sécurité. Ces challenges devront être réglés avant que les utilisateurs ne puissent profiter de tous les avantages du Cloud et y placer leur confiance absolue. En effet, le renforcement de la sécurité et les pratiques de confidentialité vont attirer plus d'utilisateurs et d'entreprises au monde de l'informatique dans les nuages. Le défi majeur en termes de sécurité est lié à la perte de contrôle sur certaines données personnelles voir sensibles, les fuites de données et la protection de l'identité lors de la migration des applications et des données sensibles dans le Cloud.
La sécurité, la protection des données personnelles « Privacy » et la confiance sont les principales préoccupations qui empêchent l'adoption massive du Cloud. Dans un sondage réalisé par l'institut de Recherche Fujitsu[2] sur les utilisateurs potentiels du Cloud, il a été constaté que 88% d'entre eux s'inquiètent à propos de qui possède l'accès à leurs données

[1] **Gartner:** http://www.gartner.com/technology/topics/cloud-computing.jsp.
[2] **Fujitsu Research Institute:** http://www.fujitsu.com/global/news/publications/dataprivacy.html.

et exigent plus d'intimité numérique. Les raisons sont entre autres que les utilisateurs ont à faire confiance aux mécanismes de sécurité et au fournisseur de services (CSP) lui-même.
Cependant, l'une des questions majeures à laquelle les utilisateurs Cloud doivent répondre est: est-ce qu'ils font confiance au CSP, de ne pas divulguer leurs données notamment personnelles, de ne pas les modifier ou les supprimer ?
De même, les utilisateurs s'inquiètent souvent d'une possible corrélation entre les services Cloud utilisés et leurs identités ce qui conduit à un mapping des identités et une utilisation souvent marketing (spam ciblé) : le CSP peut établir des profils à leurs insu (profilage) afin de réaliser des études de marché, car il est en mesure de lier des données et des informations sur le comportement et la consommation des ressources de ses utilisateurs leur permettant de construire de vastes rapports. Les utilisateurs peuvent ne pas vouloir que le CSP apprenne à quelles ressources ils accèdent et combien de fois ils utilisent un service. Du côté des entreprises, une telle transparence peut être trop intrusive et problématique si ces informations sont à la disposition de leurs concurrents. Il s'avère donc légitime que les utilisateurs cherchent à protéger leurs identités afin d'éviter ce genre de surveillance pouvant être nuisible et à réclamer leur droit à protéger leurs données personnelles.

La protection des données personnelles est une problématique importante et non négligeable dans un environnement Cloud que ce soit par rapport à la conformité législative, ou bien à la confiance que devraient avoir les utilisateurs envers le Cloud. L'impact que peut engendrer l'utilisation de ces informations peut être très important, il est donc devenu primordial d'introduire la protection des données personnelles des utilisateurs afin de leur garantir plus de sécurité. Le Cloud doit alors fournir des mécanismes forts pour bien authentifier ses utilisateurs et atténuer le plus possible les risques de divulgation. Un point capital et automatique lors de l'utilisation des services Cloud est la présence d'un bon mécanisme d'authentification.
La gestion sécurisée des identités étant essentielle dans tout environnement, elle prend une dimension plus complexe dans le cas du Cloud car il est plus difficile de gérer les utilisateurs à distance. De plus, l'accès du CSP aux informations d'identification présente une problématique d'un point de vue de la protection des données personnelles. Aussi, il existe un manque de transparence dans le Cloud empêchant les utilisateurs de surveiller leurs propres informations personnelles ce qui induit à un manque de confiance : les utilisateurs se soucient de : *Qui contrôle leurs données d'authentification dans le Cloud et qui possède les droits administratifs pour y accéder ?*
Etant donné que l'identité de l'utilisateur et des informations sensibles sont régulièrement utilisées dans le processus d'authentification lors de l'accès aux services Cloud, il devient important de les protéger. Autrement dit, comment assurer une authentification tout en gardant l'anonymat?
L'authentification et l'anonymat ont été largement étudiés. Le système doit avoir la possibilité de cacher les identités des deux parties communicantes vis-à-vis d'un tiers, en plus d'une procédure robuste et sécurisée pour pouvoir authentifier chacune vis-à-vis de l'autre.
« L'authentification anonyme » semble être généralement une déclaration contradictoire en elle-même, du fait que l'anonymat nécessite de cacher l'identité, en opposé à l'authentification qui exige de révéler l'identité pour pouvoir être vérifiée. L'utilisation des accréditations anonymes permet de prouver sa légitimité sans avoir à dévoiler explicitement son identité.

Objectif et Contribution

Dans cette optique, le présent travail s'inscrit dans le thème de recherche sur les challenges de sécurité notamment de protection des données personnelles lors du processus d'authentification, posés dans les environnements Cloud. Divers travaux de recherche ont été réalisés pour définir des mécanismes de sécurité pour la protection des données personnelles,

seuls quelques systèmes ont été conçus en intégrant l'anonymat comme élément de base. En outre, les travaux que nous avons pu rassembler lors de l'élaboration de l'état de l'art ont tous opté à assurer la confidentialité des données personnelles des utilisateurs Cloud via l'intégration d'une entité de confiance.

Notre but est de dissimuler le comportement des utilisateurs (qui inclut les services consommés et les fréquences d'accès aux services) et leurs méta-données : informations nécessaires au fonctionnement des systèmes informatiques et des réseaux, qui ne sont pas directement gérées par les utilisateurs mais sont susceptibles de les identifier directement ou indirectement. Cette manière de procéder va permette d'assurer la protection des données personnelles des utilisateurs Cloud notamment, leurs identités et leurs localisations contre toute divulgation non autorisée. Dans ce contexte, l'objectif de ce travail consiste à proposer un protocole d'authentification anonyme indépendant de la notion de confiance imposée dans les environnements Cloud afin de préserver au mieux la protection des données personnelles des utilisateurs (ce qui est équivaut à cacher au maximum les données personnelles vis-à-vis des fournisseurs). La protection des données personnelles constitue une propriété essentielle dans le protocole proposé, la particularité sera l'adaptabilité du protocole aux exigences des utilisateurs leur permettant d'affiner au mieux le niveau d'anonymat requis.

Structure du document

Dans le premier chapitre, nous allons présenter les problèmes de sécurité présents dans les environnements Cloud. Une classification des différentes attaques et des mécanismes de sécurité sera présentée. Un intérêt particulier sera accordé à la notion de protection des données personnelles dans le Cloud objet de notre travail.

Nous introduisons dans le second chapitre, les mécanismes d'authentification notamment dans les environnements Cloud puis ceux relatifs à l'authentification anonyme. Les travaux de recherche par rapport aux approches d'authentification alliant l'anonymat sont étudiés. A l'issue de ce chapitre, une synthèse et critiques des solutions existantes est présentée.

Le troisième chapitre présente la contribution. Il s'agit de proposer une approche afin de fournir une architecture complète et adaptative, utilisant plusieurs technologies complémentaires, afin d'assurer la protection des données personnelles de l'utilisateur. Ceci grâce à une authentification anonyme garantissant une consommation anonyme des services. En marge du protocole proposé, une classification des données sensibles à protéger dans le Cloud vis-à-vis des différents modèles d'attaquants a été proposée, après une étude détaillée des menaces présentes dans le Cloud afin de construire le modèle de l'adversaire.

Le quatrième chapitre est consacré à la validation du protocole. Cette dernière étant une étape primordiale lors de la proposition d'un protocole de sécurité pour garantir son bon fonctionnement, notamment en ce qui concerne le cheminement des étapes concrétisées via les différentes transitions allant de l'enregistrement jusqu'à l'accès aux services Cloud. Cette validation a été réalisée via un outil de validation de protocole de sécurité. Un prototype du protocole d'authentification a également été implémenté.

Nous achèverons ce mémoire par une conclusion générale et les perspectives.

Mots Clés: Cloud Computing, Sécurité, Protection des données personnelles, Anonymat, Authentification, Authentification anonyme, Signature en aveugle, Communication anonyme.

Chapitre 1: Sécurité et Privacy dans un environnement de Cloud Computing

1. Introduction

Comme toute avancée technologique, le Cloud Computing est confronté d'avoir ses risques, en matière de sécurité et de confiance quant à l'utilisation des différents services, qu'il convient de prendre en compte avant de pouvoir bénéficier de ses avantages. Les entreprises voient le Cloud Computing de différentes manières: la majorité possède une vision sceptique concernant le Cloud Computing, adoptant ainsi une attitude prudente. Ceci pousse les entreprises à se focaliser sur l'un des points les plus sensibles : la sécurité. Il existe une vision moins répandue, où l'entreprise voit le Cloud Computing comme étant un moteur d'innovation. Le personnel dédié au bon fonctionnement de l'infrastructure de l'entreprise sera ainsi libéré de ses tâches quotidiennes. Ceci permettra à l'entreprise de dépenser toute son énergie sur l'innovation et l'amélioration des services.

L'ample présence de l'informatique et son évolution continue ont toujours engendré des réflexions quant à la sécurité. Le premier niveau de sécurité à respecter est la norme : ISO 7498-2:1989 **[35]**, qui garantit que tout système doit assurer : l'authentification (l'identité), le contrôle d'accès, l'intégrité et la confidentialité des données (données accessibles uniquement par les personnes autorisées sous certaines conditions). En outre, la sécurité et le respect de la vie privée sont devenus des challenges techniques critiques pour les courantes et futures générations des systèmes de communication. Le développement rapide des transactions électroniques et la possibilité de collecte d'informations personnelles sur le Web ont contribué à accroître l'intérêt des utilisateurs à conserver le caractère privé et à réclamer le droit à la vie privée. La protection des données personnelles ou Privacy est une problématique importante dans un environnement de Cloud Computing, que ce soit par rapport à la conformité législative ou bien à la confiance que devraient avoir les utilisateurs envers le Cloud. Elle doit être considérée à chaque phase de la conception. Plusieurs tentatives ont été réalisées pour protéger les données personnelles des individus ou des organismes qui tentent d'utiliser les services fournis dans le Cloud. La tâche la plus difficile est de fournir des services aux utilisateurs, tout en préservant la confidentialité de leurs informations qu'ils s'agissent *de leur identité* ou de *leurs données*.

Dans ce chapitre, nous allons donc présenter d'une manière générale le Cloud Computing, la sécurité dans un tel environnement, ainsi que la notion de protection des données personnelles notamment dans un environnement de Cloud Computing.

2. Le Cloud Computing

Le Cloud Computing est devenu le mécanisme le plus émergent de l'utilisation d'Internet. La plupart des services tels que l'e-mail, les réseaux sociaux, les moteurs de recherche, les logiciels et beaucoup d'autres sont maintenant hébergés dans le Cloud. Pour comprendre la nature et la sécurité du Cloud Computing, nous devons comprendre d'abord son architecture afin de mieux assurer la sécurité contre les différentes menaces présentent dans ce type d'environnement.

2.1. Définition

Le Cloud Computing a été défini par l'Institut national américain des normes et de la technologie NIST «National Institute of Standards and Technology» comme suit:

« *Un modèle permettant un accès facile et à la demande, via le réseau, à un pool partagé de ressources informatiques configurables (par exemple : réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mises à disposition des utilisateurs ou libérées avec un effort minimum d'administration de la part de l'entreprise ou du prestataire de services fournissant les dites ressources* ». **[1]**

Le Cloud est donc un modèle qui permet l'accès à la demande. Les ressources sont partagées et l'utilisateur peut bénéficier d'une flexibilité importante avec un effort de gestion minimal.
La figure ci-dessous montre les huit éléments fondamentaux du Cloud Computing: **[2]**

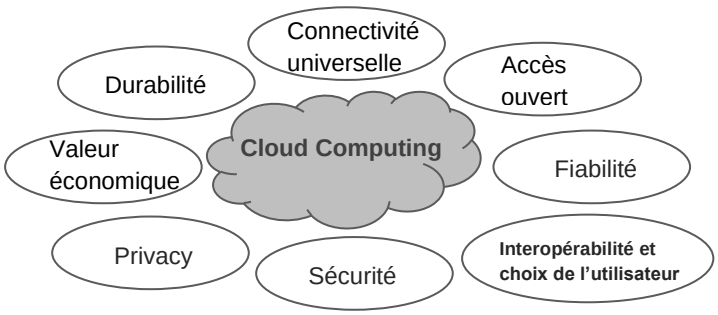


Figure 1.1 Eléments fondamentaux du Cloud Computing

Dans un environnement de Cloud Computing, les différents acteurs sont:

- **Le CSP** «**C**loud **S**ervice **P**rovider»: Le CSP est le fournisseur de services. Il gère les services Cloud (par exemple le stockage partagé) et donne l'accès via console ou API de gestion aux utilisateurs. Le CSP est généralement une compagnie qui se comporte comme une partie de confiance. Il fournit des services dans le Cloud et authentifie les utilisateurs lorsqu'ils accèdent à l'un de ses services. Il émet également des informations d'identification pour permettre l'accès à ses utilisateurs.

- **L'Utilisateur**: Un utilisateur est un client du CSP qui accède au Cloud et utilise ses services, par exemple, un service de stockage offert par un CSP. C'est une entité individuelle ou un groupe, qui est propriétaire de ses données stockées dans le Cloud.

- **Le TTP** «**T**rusted **T**hird **P**arty»: Un tiers est une entité facultative et neutre qui a la capacité de vérification de l'exactitude des fichiers logs des utilisateurs ou de réalisation d'un audit, etc.

- **Serveur Cloud:** Entité gérée par un CSP particulier ou par un opérateur d'application Cloud pour fournir un service de stockage des données ou des services de calcul. Le serveur Cloud est considéré comme une entité possédant un stockage illimité et une capacité de calcul importante.

2.2. Historique

Il est difficile de situer avec précision quand a été inventé le Cloud Computing. Selon certains, il faut remonter en 1960, avec les travaux de l'américain John McCarthy (1927-2011), un des pionniers de l'intelligence artificielle, qui considérait d'emblée l'informatique comme un service. Selon une autre source, c'est l'avènement des réseaux dans les années 1970 qui a rendu possible l'exécution déportée des tâches informatiques.
Enfin, Il est communément admis que le concept de Cloud Computing a été initié par Amazon en 2002 **[3]**. Ce leader avait investi dans le parc informatique afin de pallier les surcharges des serveurs dédiés au commerce en ligne. A cette époque, Internet comptait moins de 600 millions d'utilisateurs, mais la fréquentation de la toile et les achats en ligne étaient en pleine expansion. Amazon a eu alors l'idée de louer ses capacités informatiques à des clients pour qu'ils puissent stocker leurs données et utiliser les serveurs, même en dehors des périodes de fête (qui représentent en termes de commandes un pic temporel mais ponctuel d'utilisation).
Ces services étaient accessibles via Internet et avec une adaptation en temps réel de la capacité de traitement, le tout facturé à la consommation. Cependant, ce n'est qu'en 2006 qu'Amazon comprit qu'un nouveau mode de consommation de l'informatique et d'Internet faisait son apparition.
Bien avant la naissance du terme de « Cloud Computing », utilisé par les informaticiens pour qualifier l'immense nébuleuse du net, des services de Cloud étaient déjà utilisés comme le Webmail, le stockage de données en ligne ou les réseaux sociaux.
Dans les années 1990, un concept avait préparé le terrain au Cloud Computing. Il s'agissait de l'ASP: Application Service Provider, qui permettait aux clients de louer l'accès à un logiciel installé sur des serveurs distants d'un prestataire, sans installer le logiciel sur ses propres machines. Le Cloud Computing ajoute à cette offre la notion d'élasticité (caractéristique de base) avec la possibilité d'ajouter de nouveaux utilisateurs et de nouveaux services.
La virtualisation est un concept beaucoup plus ancien, elle constitue le socle du Cloud. La virtualisation regroupe l'ensemble des techniques matérielles ou logicielles permettant de faire fonctionner, sur une seule machine physique, plusieurs configurations informatiques (systèmes d'exploitation, applications,…) de manière à former plusieurs machines virtuelles qui reproduisent le comportement des machines physiques. **[3]**

La base essentielle de la création d'un Cloud étant la performance des réseaux. Par conséquent, le point de départ du Cloud Computing devrait être lié au développement de l'Internet. Les divers accès au Cloud, les idées et leurs origines respectives conduisent à une perception fortement divergente de la part du public. L'importance du Cloud est devenue évidente. La convergence vers le Cloud Computing est illustrée dans la figure 1.2. **[4]**

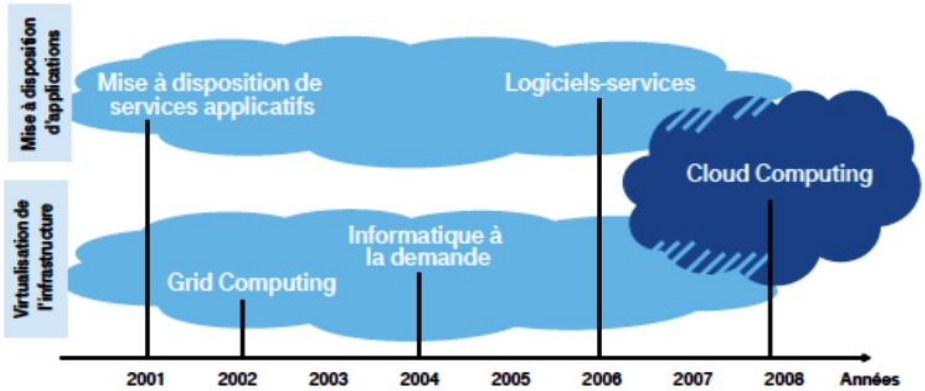


Figure 1.2 Convergence vers le Cloud Computing

Le fait de pouvoir formaliser une offre de services informatique dématérialisée et à la demande en direction des entreprises a été le moteur de développement du Cloud Computing en tant que tel **[3].** La transition des entreprises du système traditionnel vers le Cloud est motivée par le besoin d'une agilité et d'une vitesse plus importante, lorsqu'il s'agit d'apporter l'innovation nécessaire à l'entreprise. Le nouveau concept est de délocaliser les serveurs, ainsi, leur gestion est effectuée par un fournisseur de services Cloud spécialisé. La figure 1.3 montre cette transition. **[5]**

Figure 1.3 Transition des entreprises du système traditionnel au Cloud

2.3. Architecture du Cloud Computing

NIST définit l'architecture du Cloud Computing en décrivant cinq caractéristiques essentielles, trois modèles de service et quatre modèles de déploiement comme illustré dans la figure 1.4: **[6]**

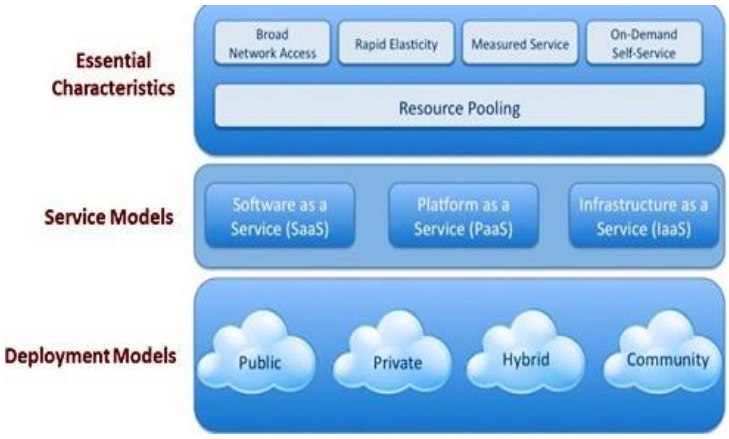


Figure 1.4 Modèle visuel du NIST pour la définition du Cloud Computing

2.4. Les modèles de déploiement dans le Cloud

Le Cloud Computing compte quatre modèles de déploiement, à savoir : **[6]**

- **Cloud Public:** Dans ce type, l'infrastructure du Cloud est à la disposition du grand public.
- **Cloud Privé:** C'est un type de Cloud qui est disponible uniquement pour une seule organisation.
- **Cloud Communautaire:** Dans ce type de modèle de déploiement, l'infrastructure Cloud est partagée par plusieurs organisations et maintenue par une communauté spécifique avec des préoccupations communes.
- **Cloud hybride:** Ceci est une infrastructure de Cloud qui est une composition de deux ou plusieurs Cloud i.e. privé, communautaire ou public.

2.5. Les modèles de services dans le Cloud «SPI MODEL»

Les produits du Cloud Computing sont souvent classés en une hiérarchie de termes **-as a service**, présentés comme: **[6]**

- **SaaS** « **S**oftware **a**s **a** **S**ervice »: Ce type de service fournit à l'utilisateur la capacité d'utiliser les applications du CSP installées dans le Cloud.

- **PaaS** « **P**latform **a**s **a** **S**ervice »: Dans ce type de service, l'utilisateur peut déployer, peut créer ou acquérir des applications en utilisant des langages de programmation ou des outils fournis par le CSP dans l'infrastructure Cloud.

- **IaaS** « **I**nfrastructure **a**s **a** **S**ervice »: Ce type de service fournit à l'utilisateur la capacité par laquelle il peut réaliser des traitements, un stockage, des réseaux et autres ressources informatiques fondamentales, où les utilisateurs peuvent déployer et exécuter des logiciels (systèmes d'exploitation, applications).

La figure ci-dessous présente les modèles de services Cloud en spécifiant au niveau de chaque couche les entités qui possèdent le contrôle : l'entreprise, le fournisseur de services ou bien un contrôle partagé.

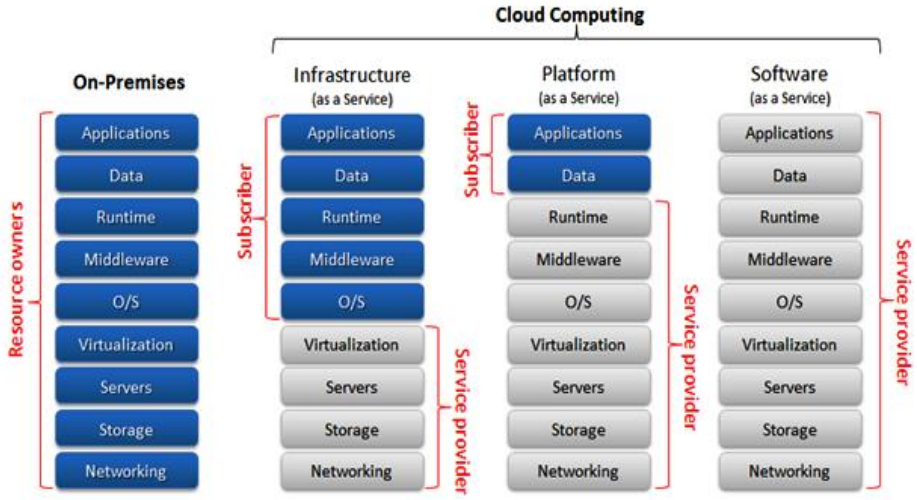


Figure 1.5 Les modèles de services dans le Cloud

2.6. Les caractéristiques du Cloud Computing

Les cinq caractéristiques essentielles d'un Cloud sont : **[6]**

- **Large accès réseau:** Les ressources du Cloud sont accessibles par Internet via les protocoles réseaux standards. Plusieurs clients peuvent alors accéder aux services à partir de plusieurs réseaux d'accès.
- **Elasticité rapide:** En quelques minutes, des ressources peuvent être approvisionnées en permettant le passage à l'échelle (la scalabilité). Par conséquent, l'élasticité des ressources est très rapide dans le Cloud, offrant ainsi un service évolutif avec une certaine souplesse dans la modification et le déploiement.

- **Service mesuré:** Le CSP effectue des mesures concernant généralement les frais dus à l'utilisation du CPU, de la mémoire, du disque, de la bande passante réseau, ou d'autres ressources. Le client payera ce qu'il a consommé selon le type et le temps d'utilisation du service « facturation à l'usage ».
- **Service à la demande:** Les ressources peuvent être approvisionnées par des mécanismes automatisés et au moment de leur demande. Le service sera donc fourni au client au besoin et à la demande.
- **Mise en commun des ressources (pooling):** Le même service et les mêmes ressources sont consommés par plusieurs clients.

2.7. Composants de base du Cloud Computing

Le Cloud Computing comporte divers composants. Ceux cités dans la figure 1.6 doivent être présents dans un Cloud de services afin de pouvoir être appelé ainsi : **[4]**

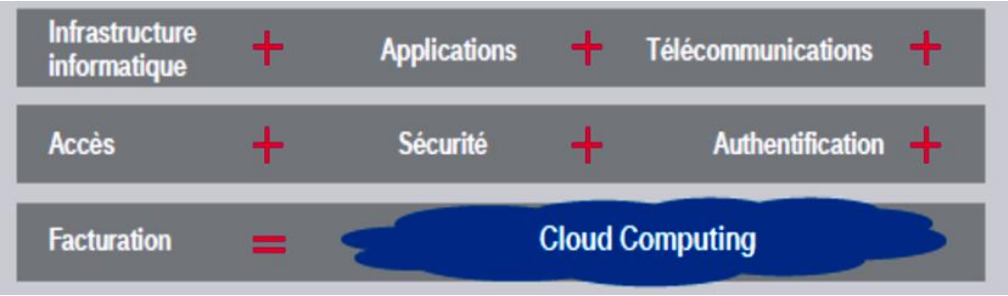


Figure 1.6 Composants de base du Cloud Computing

Les caractéristiques typiques de ces composants sont: la mise à disposition via Internet, le contrôle et le stockage en externe, la simplicité d'utilisation des interfaces, la simplicité d'implémentation, l'accessibilité par l'utilisateur à la demande et en temps réel, une grande extensibilité en termes de volume et durée de vie, en plus d'une intégration facile avec les autres systèmes. **[4]**

3. Questions clés à propos de la sécurité dans le Cloud Computing

La sécurité dans le Cloud Computing peut avoir des significations différentes selon le contexte, par exemple: avoir un Cloud sécurisé d'un point de vue du CSP n'implique pas qu'il soit sûr du point de vue des utilisateurs. Malheureusement, la plupart des utilisateurs considèrent le fait d'avoir un nom d'utilisateur et un mot de passe pour accéder à leur compte Cloud est une manière assez sécurisée. Pour les CSPs, les critères de sécurité, de protection des données personnelles et la confiance pourraient être un peu différents: d'un côté, ils ont tous comme objectif d'essayer de gagner la confiance de l'utilisateur, acquérir une bonne réputation dans le marché du Cloud tout en respectant les lois. D'un autre côté, le souci de chaque CSP est la possibilité de perdre le contrôle sur les données qu'il détient, comme la revente des données à d'autres organisations ou gouvernements, dans le but de les garder protégées dans leurs serveurs. Ces données peuvent être aussi supprimées ou faisant l'objet d'un back-up pour l'ensemble de leurs structures. Le tout doit être un choix fait par le CSP lui-même et sous son contrôle.

La sécurité du Cloud Computing constitue donc, un point très important en raison des trois faits suivants:

- Les fournisseurs Cloud forment une cible intéressante pour les pirates informatiques vu le nombre d'utilisateurs (passage à l'échelle).
- L'accès se fait via un réseau public : Internet.
- Les données ne se localisent pas en interne mais auprès d'un fournisseur externe.

En outre, la sécurité est généralement considérée comme l'obstacle principal lors de l'utilisation des services Cloud. Un niveau élevé de sécurité est généralement associé à l'accès aux données hébergées dans le Cloud. Cela est assuré grâce aux mécanismes d'authentification mis en place par les CSPs. Ces mécanismes peuvent éventuellement être renforcés. Malgré cela, les entreprises clientes se posent les questions suivantes:

- Quels types d'informations sont accessibles dans le Cloud, qui peut y accéder et comment sont-elles séparées des autres informations non sécurisées ?
- Comment les données sensibles doivent être envoyées et comment sont-elles accessibles: en clair ou en chiffrant certaines?
- Qui dispose des droits d'envoi et de réception des données sensibles en dehors l'entreprise elle-même?
- Quels sont les mécanismes de sécurité qui assurent la confidentialité des données de l'entreprise surtout dans un Cloud public?

Pour assurer la sécurité du Cloud Computing, le CSP doit faire face à la sécurité et la protection des données personnelles des utilisateurs, ainsi que le respect des règlements nécessaires.

Afin de développer un environnement Cloud sécurisé, les principes de base de sécurité suivants doivent être pris en compte : **[7]**

- **L'Intégrité:** L'objectif est d'assurer que les données protégées ne peuvent pas être modifiées par des tiers non autorisés.

- **La Confidentialité:** Le but est d'assurer la garantie de la protection de l'information pour ne pas qu'elle soit à la possession d'une personne non autorisée (l'information concerne les données stockées ainsi que les données en transit transférées via Internet).

- **L'Authentification:** L'authentification est le processus d'identification et de vérification de l'utilisateur. Elle fournit les droits d'accès aux services ou aux ressources du Cloud. L'authentification signifie généralement la vérification appropriée de l'identité de quelqu'un.

A ces trois principes, vient s'ajouter : **[8]**

- **La Disponibilité:** Le CSP doit s'assurer que les systèmes fonctionnent comme prévu et que les utilisateurs autorisés ne sont pas refusés. Les utilisateurs doivent être en mesure d'accéder à leurs données et aux services quand ils en ont besoin. Les ressources doivent donc être accessibles avec un temps de réponse acceptable.

  La figure suivante résume les principes de base de sécurité dans le Cloud dans chaque modèle de déploiement et par rapport à chaque modèle de service.

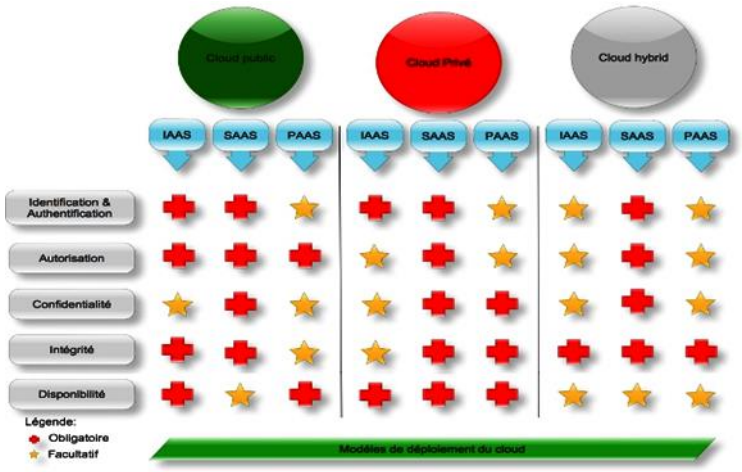


Figure 1.7 Cloud Computing / Principes de sécurité

3.1. Challenges introduits dans un environnement de Cloud Computing

Le Cloud Computing offre une alternative convaincante aux solutions IT internes. Cependant, l'externalisation de l'infrastructure informatique introduit un certain nombre de challenges en matière de sécurité. Plus précisément, le Cloud Computing étant une plate-forme informatique commune, il doit donc prévoir des mécanismes forts pour authentifier correctement les utilisateurs et atténuer le plus possible de vulnérabilités. Cependant, une attention particulière et un focus automatique lors de l'utilisation des services du Cloud Computing est la présence d'un bon mécanisme d'authentification. La puissance de ce mécanisme est relative au besoin de protection des données personnelles réclamé par les utilisateurs. Toutefois, une gestion sécurisée des identités est essentielle dans tout environnement, mais elle peut prendre une dimension plus complexe dans le cas du Cloud Computing.

Un tel environnement produit donc de nombreux challenges:

- Les exigences du Cloud: Garantir et veiller à ce que les informations confidentielles stockées dans le Cloud ne seront pas compromises.
- Questions liées à la sauvegarde des données dans des endroits différents à travers le monde, les utilisateurs n'ont aucune information concernant leur localisation.
- Les utilisateurs Cloud n'ont ni le droit d'accès ni de contrôle sur les infrastructures qu'ils utilisent (surtout dans le cas des services Cloud de haut niveau comme le SaaS). Ils ne peuvent donc pas vérifier les versions des logiciels utilisés, la mise à jours des codes, les mécanismes de sécurité, etc. ce qui peut générer des obstacles au niveau de la qualité et de l'utilisation des services Cloud.
- Sécurisation des applications pas uniquement sur sites mais également dans le Cloud.
- Comment intégrer plus de sécurité dans l'accès pour mieux se protéger.
- Qui contrôle les données d'authentification dans le Cloud? Et qui a les droits d'accès aux mots de passe des utilisateurs de l'entreprise cliente utilisés pour accéder aux services: qui dispose donc des droits d'administration?
- Comment protéger les données personnelles de l'utilisateur final: *comment lui assurer une authentification anonyme ?*

3.2. Les principales menaces de sécurité dans un environnement Cloud

Comme beaucoup d'entreprises choisissent d'adopter et de basculer vers le Cloud Computing en raison de ses caractéristiques et de ses avantages multiples, les pirates informatiques aussi suivent cette voie en essayant d'explorer et d'exploiter tout ce qu'ils trouvent dans le Cloud.
Les menaces de sécurité présentent dans un environnement Cloud peuvent être perçues en trois catégories : **[9]**

- **Menaces de sécurité conventionnelles :** Ceci inclut les intrusions et attaques informatiques qui sont plus néfastes lors du basculement vers le Cloud. Les CSPs répondent généralement à ces préoccupations en faisant valoir que leurs mesures et processus de sécurité sont bien installés, développés et suffisamment testés.

- **Problèmes de disponibilité :** Ces préoccupations portent sur des données et des applications critiques qui doivent être continuellement disponibles. Les pannes très médiatisées du Cloud Computing comprennent la journée de panne de Gmail en octobre 2008 (Gmail Extended Panne), Amazon S3 avec plus de sept heures de temps d'arrêt en juillet 2008 (Amazon S3 Availability Event), en mars 2012, le service Cloud de Microsoft Azure a connu une panne de grande envergure pendant près de 24 heures et quelques mois plus tard, c'est le Cloud d'Amazon qui tombait en rade pendant plusieurs heures, rendant indisponible des sites clients comme Pinterest. Le maintien de la disponibilité, la prévention des attaques par déni de service sont deux préoccupations majeures dans cette catégorie de menaces.

- **Contrôle de données par des tiers :** Diverses questions concernant la protection des données et la gestion de la sécurité incitent plusieurs entreprises à construire des Clouds, pour éviter ces problèmes et profiter de certains avantages de cet environnement. Toutefois, des préoccupations comme les obligations contractuelles, l'éventuel espionnage du CSP, les implications juridiques des applications et des données étant détenues par un tiers, doivent être abordées convenablement.

Les principales menaces de sécurité présentes dans un tel environnement et décelées par le **CSA** "**C**loud **S**ecurity **A**lliance" sont les suivantes: **[10]**

3.2.1. Technologie partagée

Cette menace de sécurité est en fait une vulnérabilité. Ceci est tout simplement dû au fait que l'infrastructure de services du Cloud Computing, les plateformes et les applications sont partagées. En conséquence, si un élément est compromis au sein du système de services Cloud, il existera une menace potentielle de violation de tout le système. Le CSA recommande comme moyen de défense une stratégie en profondeur, y compris par exemple un stockage et un monitoring constant, dans le cas où un problème est détecté.

3.2.2. Perte de contrôle et Perte de données

Probablement la raison la plus importante qui dissuade les entreprises et les utilisateurs des systèmes de Cloud Computing est que l'utilisateur perde le contrôle sur ses données. Sur ordinateurs traditionnels ou serveurs appartenant à une entreprise ou à un individu, il existe un contrôle sur : la manière de stockage des données, les restrictions mises pour définir qui peut y accéder et les politiques de sauvegarde établies.

Dans le Cloud Computing, les données sont stockées sur un serveur. Une tierce partie (fournisseur) est responsable de déterminer les détails par rapport au stockage de ces données. Il existe également un niveau de confiance requis entre l'utilisateur et le fournisseur. L'utilisateur doit suffisamment faire confiance au fournisseur pour stocker potentiellement des données notamment confidentielles, sensibles ou secrètes. La situation la plus probable est que les organisations et les individus ne veulent pas que leurs données soient extraites et utilisées à des fins publicitaires, surtout dans le cas de l'utilisation de services gratuits. Cela obligera les utilisateurs à opter pour des services qui incluent des frais, mais qui offrent un niveau de confidentialité plus élevé, ce qui impliquera la non vente de leurs données.

En outre, la perte de données provient de nombreuses sources, mais les principales sont les activités provenant d'un pirate informatique ou d'un désastre naturel. La deuxième situation peut être une conséquence inévitable comme dans le cas d'un incendie. L'entreprise doit donc effectuer une vérification approfondie de la stratégie concernant la perte de données établie dans les services Cloud et aussi établir ses propres contrôles internes dans l'entreprise avant de mettre en œuvre un service Cloud.

3.2.3. Usurpation d'identité

Les risques d'usurpation d'identité sont de deux natures :

- L'usurpation de service offert par le Cloud : Il s'agit de services similaires voire identiques, offerts au service des clients. Dans ce cas, les clients peuvent se retrouver confrontés à des risques tels que le phishing (hameçonnage).
- L'usurpation d'identité des utilisateurs : Il s'agit d'attaques liées au vol de l'identité des utilisateurs suite à des déficiences dans les mécanismes d'authentification. De faux clients utiliseraient de façon non autorisée des ressources, voire accèderaient aux données des utilisateurs légitimes.

Dans les deux cas, la faiblesse dans les mécanismes d'identification et d'authentification laisserait la porte ouverte à ces menaces et éventuellement aux attaques.

Le risque lié au détournement de compte « Account Hijacking », est que si un compte est piraté, l'attaquant peut accéder aux informations d'identification de l'entreprise, espionner ses activités et transactions, manipuler les données, falsifier les informations et rediriger les utilisateurs vers des sites illégitimes. Une façon de se défendre contre ce risque de sécurité selon le CSA, est d'interdire le partage des informations de compte entre les utilisateurs et les services et de disposer de techniques d'authentification à deux facteurs (authentification forte).

3.2.4. API non-sécurisée

Certaines organisations et tiers construisent des interfaces non-sécurisées, introduisant une nouvelle complexité aux couches de l'API. Cela augmente le risque que les entreprises divulguent des informations d'identification à ces tiers, exposent potentiellement des informations confidentielles ou pire, de risquer l'intégrité du système. Les conseils de la CSA pour les entreprises est de bien comprendre les mesures de sécurité quant à l'usage, la gestion et le monitoring des services.

3.2.5. Déni de service

Cette menace de sécurité a pour objectif de nuire à la disponibilité d'un ou de plusieurs services et engendrer des pannes pouvant provoquées une augmentation des prix. Les pirates informatiques peuvent réussir à pousser l'entreprise à consommer trop de ressources en termes de temps de calcul afin d'augmenter la charge et les frais.

3.2.6. Les intrus malveillants

Les entreprises ont tendance à être très préoccupées par cette violation de la protection des données. Dans le Cloud, l'intrus pourrait être un employé (actuel ou ancien), ou toute autre personne qui peut avoir accès au système, réseau ou aux données de l'entreprise. Les architectures Cloud étant gérées et exploitées par des personnes disposant de privilèges élevés ce qui implique donc un risque élevé et des dommages peuvent être causés. Les risques d'accès non autorisés aux données ou l'utilisation abusive doivent être prévenus. Les dommages causés par des administrateurs systèmes Cloud s'avèrent plus important que dans un environnement classique. Des procédures et des moyens sont nécessaires dans les phases de prévention et de détection, jusqu'aux phases de protection et de réaction.
Le chiffrement est éventuellement le meilleur moyen et la meilleure manière pour sécuriser les données (stockées ou en transit) pour dissuader les intrus malveillants. Cela est valable aussi longtemps que la clé restera protégée loin des potentiels intrus malveillants.

La forte croissance du Cloud constitue une arme à double tranchant. Ce dernier pouvant être utilisé à des fins malsaines, comme exemples significatifs l'utilisation du Cloud pour casser les clés de chiffrement ou l'utilisation des serveurs afin de propager des logiciels malveillants.

3.3. Les attaques dans un environnement Cloud

Il existe de multiples problèmes de sécurité quant à l'utilisation du Cloud Computing. Ces problèmes sont liés à l'informatique traditionnelle ainsi que ceux spécifiques au Cloud. En outre, il existe des problèmes de sécurité qui affectent les utilisateurs et les fournisseurs. Le Cloud Computing est en réalité concerné par divers risques, tels que les attaques ciblant l'environnement partagé et les logiciels malveillants ciblant les machines virtuelles etc. De plus, les méthodes de sécurité conventionnelles ne fonctionnent pas dans tous les cas dans le Cloud, ce qui le soumet à diverses attaques. Afin de bien traiter les vulnérabilités dans l'environnement Cloud, il est nécessaire de définir des procédures de sécurité bien structurées et bien déterminées. Dans le Cloud, la sécurité étant partagée entre le CSP et l'utilisateur Cloud, les deux entités doivent se faire confiance mutuellement afin d'améliorer la sécurité. En exploitant les vulnérabilités présentes dans un environnement de Cloud Computing, un adversaire peut lancer diverses attaques. Les utilisateurs Cloud sont confrontés à deux types d'attaques : attaques internes et attaques externes illustrées dans la figure 1.8 : **[11]**

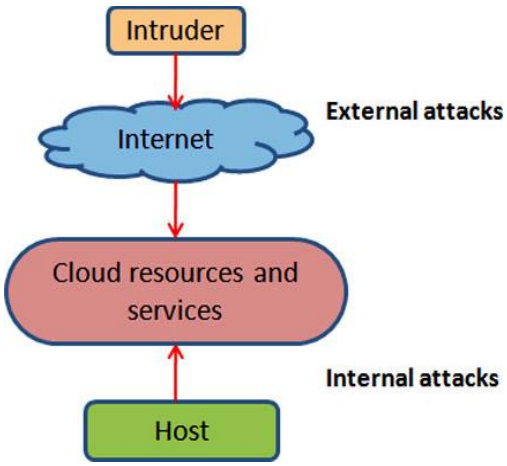


Figure 1.8 Attaques internes / externes dans un environnement Cloud

3.3.1. Les attaques externes

Les attaques externes augmentent à un rythme exceptionnel. Les attaques externes les plus importantes dans un environnement de Cloud Computing sont: **[11, 12]**

- **Attaque DoS** «**D**enial **o**f **S**ervice»

Grâce à Internet, un attaquant peut tenter d'inonder une victime en envoyant des requêtes à partir d'hôtes innocents connectés dans le réseau. Ces hôtes sont appelés machines zombies. Dans le Cloud, les demandes de machines virtuelles (VM) sont accessibles par chaque utilisateur à travers Internet. Un attaquant peut inonder le Cloud par un grand nombre de requêtes via les machines zombies. Une telle attaque interrompt le comportement attendu du Cloud et affecte la disponibilité de ses services. Le Cloud peut être surchargé à servir un certain nombre de demandes illégitimes émanant d'une seule machine ce qui causera l'attaque déni de service DoS « **D**enial **o**f **S**ervice » ou de plusieurs machines ce qui causera le DDoS pour déni de service distribué. Toutefois, une authentification forte, une autorisation et un système IDS / IPS peuvent fournir une protection contre une telle attaque. Certains professionnels de la sécurité ont fait valoir que le Cloud est plus vulnérable aux attaques DoS, car c'est un environnement partagé par plusieurs utilisateurs, ce qui rend une attaque DoS beaucoup plus dommageable.

Le Cloud étant cependant plus perméable aux attaques par déni de service, cela est dû au fait que de nombreux utilisateurs sont impliqués dans l'utilisation de ses services et ressources, les attaques DoS peuvent donc être plus néfastes dans un tel environnement. Il est important de considérer que des personnes malveillantes peuvent abuser du Cloud Computing pour créer des Botnets (réseaux de machines zombies) virtuels. Lorsqu'une attaque DDoS se produit contre un serveur virtuel hébergé, un grand nombre de paquets d'attaque sont générés par les Botnets et envoyés vers une file d'attente Q. Pour identifier ces paquets d'attaque et garantir une qualité de service QoS aux utilisateurs, une idée était d'investir davantage de ressources pour cloner multiples IPS «Intrusion Prevention System». Pour atteindre cet objectif comme illustré dans la figure 1.9, plusieurs IPS ont été cloné en parallèle. **[13]**

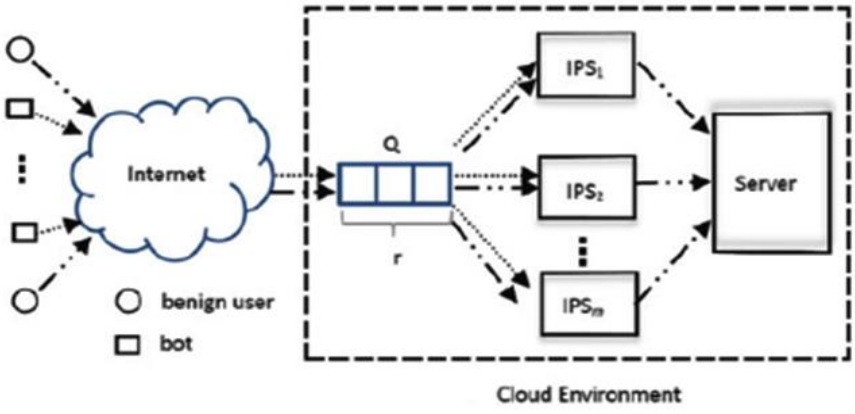


Figure 1.9 Parade contre l'attaque **DDOS** dans un environnement Cloud

- **Porte dérobée « Backdoor »**

C'est une attaque passive, qui permet aux adversaires d'accéder à distance au système compromis et cela, par l'utilisation de portes dérobées. L'adversaire peut être en mesure de contrôler les ressources de la victime et peut en faire un zombie pour tenter une attaque DDoS.

La porte dérobée peut également être utilisée pour divulguer les données confidentielles de la victime. Une meilleure authentification et l'isolation entre les machines virtuelles peut fournir une protection contre de telles attaques.

- **Attaque par injection de malwares**

C'est une attaque considérable qui tente d'injecter un programme malveillant ou de mettre en œuvre une machine virtuelle malveillante dans le Cloud. Le but d'insertion du logiciel malveillant est de modifier les données, induire des changements de fonctionnalité ou des blocages etc.
Dans cette attaque, l'adversaire crée son propre module de mise en œuvre de services malveillants (SaaS ou PaaS) ou l'introduit dans une instance de machine virtuelle (IaaS) et l'ajoute au système Cloud. L'adversaire va prétendre par la suite au système Cloud que sa nouvelle instance est valide. Si cette action réussit, le Cloud va rediriger automatiquement les demandes valides des utilisateurs vers le service malveillant, le code de l'adversaire sera ainsi exécuté. Le scénario principal derrière l'attaque d'injection de malwares dans le Cloud est qu'un attaquant transfère une copie manipulée de l'instance de service de la victime, de telle sorte que l'instance malicieuse puisse enregistrer les accès de la victime aux services. Pour atteindre cet objectif, l'attaquant doit prendre le contrôle des données des victimes dans le Cloud. Cette attaque est la principale menace exploitant les services Cloud.

- **Attaque par canal auxiliaire**

Un attaquant pourrait tenter de compromettre le système Cloud en plaçant une machine virtuelle malveillante à proximité d'un serveur Cloud cible, puis lancer son attaque par canal auxiliaire. Dans cette attaque, un attaquant tente souvent de placer son instance sur la même machine physique, qui jouera le rôle d'une instance cible et procédera à l'extraction et la collecte des informations sur les instances co-résidentes.
Au sein d'un même matériel comportant multiples machines virtuelles, des ressources sont partagées et peuvent être utilisées comme un moyen de canal auxiliaire de données d'une machine virtuelle à une autre. Ce type d'attaque se base alors sur les ressources partagées entre les machines virtuelles, un attaquant en cas de succès dans le voisin d'une cible, peut alors utiliser différentes méthodes afin d'intercepter les données envoyées et reçues des autres machines virtuelles.

- **Attaque sur l'authentification**

L'authentification est une question clé dans les services hébergés et virtuels et est très fréquemment ciblée. Le système d'authentification est souvent visé dans le but d'être contourner et bypasser. Il existe plusieurs façons pour authentifier les utilisateurs (qui seront détaillées dans le chapitre suivant). Les mécanismes et méthodes utilisés pour sécuriser le processus d'authentification sont principalement ciblés par les attaques. Une vulnérabilité provenant d'erreur/de faille dans le processus d'authentification peut être exploitée provoquant une attaque sur l'authentification. Celle-ci pourrait donner des accès de type administrateur dans le Cloud et entraîner une corruption de la plate-forme. La solution de base contre toute attaque réalisée sur l'authentification: la plupart des services utilisent encore aujourd'hui de simples noms d'utilisateurs et mots de passe, à l'exception de certaines institutions qui ont déployé diverses formes d'authentification secondaire (tels que des clés, des claviers virtuels, des questions secrètes partagées) pour rendre l'authentification plus solide notamment contre les attaques populaires de phishing.

- **Attaque par hameçonnage « Phishing »**

Les attaques de phishing sont bien connues par la manipulation des liens Web afin de rediriger un utilisateur à un faux lien dans le but d'obtenir des données sensibles. Dans le Cloud, il peut être possible qu'un attaquant utilise le service Cloud pour héberger un site d'attaque de phishing et de détourner les comptes et les services d'autres utilisateurs vers ce site malicieux. Dans ce genre d'attaque, les utilisateurs sont amenés à croire qu'ils sont en communication avec le serveur valide en créant une page Web ressemblant à la page du serveur valide. En 2007, un employé d'un SaaS Provider « SalesForce » a été victime d'une attaque de phishing qui a abouti à la révélation des informations de compte SalesForce de certains clients.

- **Attaque de l'homme du milieu MITM « Man-In-The-Middle »**

C'est l'attaquant lui-même qui va s'introduire dans une communication en cours entre deux utilisateurs du Cloud (ou de n'importe quel système), dans le but d'essayer d'injecter de fausses informations ou d'acquérir des connaissances à propos des données transférées entre eux. L'attaquant doit donc être capable de recevoir les messages des deux parties et leurs envoyer des réponses en se faisant passer pour l'autre. Depuis la création du Web 2.0, l'attaque MITM est devenue très populaire dans les environnements SaaS.

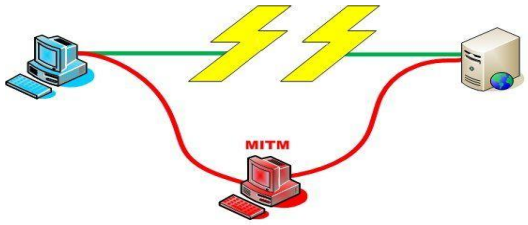


Figure 1.10 Attaque MITM

- **Attaque MITC « Man In The Cloud » [58]**

Nouveau type d'attaque spécifique, exploitant les principaux services de synchronisation de fichiers. Les services Dropbox, Box, OneDrive ou Google Drive, permettent à un individu (et donc potentiellement un employé d'une entreprise) de conserver sur le Cloud, des copies synchronisées de ses fichiers et les rendre accessibles par ses multiples équipements (PC, smartphone, tablette). A la création du compte, le CSP effectue l'authentification de l'utilisateur, puis lui remet un jeton de synchronisation, qui est stocké sur les divers équipements de l'utilisateur. Toute modification d'un des fichiers par quelconque des équipements de l'utilisateur est rapidement synchronisée, puis propagée vers les autres équipements.

Conformément à la figure 1.11, l'attaque consiste à : **(1)** Convaincre l'utilisateur de cliquer sur un e-mail fictif contenant un jeton infecté. **(2)** Le code de l'e-mail va discrètement copier le bon jeton dans un fichier du dossier de synchronisation et remplacer le bon jeton par un jeton infecté. **(3)** Ce jeton infecté va provoquer la prochaine synchronisation des fichiers de l'utilisateur sur un compte possédé par l'attaquant au lieu du compte de l'utilisateur. **(4)** Parmi les fichiers que va récupérer l'attaquant se trouve le fichier qui contient le bon jeton de l'utilisateur. **(5)** Avec ce bon jeton, l'attaquant pourra accéder au compte de l'utilisateur sans provoquer aucune alerte particulière. Ce dernier peut aller récupérer/modifier des fichiers ou ajouter un malware qui sera téléchargé sur les équipements de l'utilisateur à la prochaine synchronisation.

Enfin, **(6)** il ne suffit plus à l'attaquant que d'effacer ses traces en détruisant le jeton infecté du registre et en remettant en place le bon jeton déjà récupéré. Seule une analyse minutieuse des logs peut le révéler sauf si l'attaquant a également effacé ses traces des logs.

Figure 1.11 Attaque MITC

- **Attaque sur la virtualisation**

Il existe principalement deux types d'attaque effectués sur la virtualisation: « évasion de la machine virtuelle» et « présence de Rootkit dans l'hyperviseur ».

- Evasion de la machine virtuelle: Dans ce type d'attaque, le programme d'un attaquant opérationnel dans une machine virtuelle va casser la couche d'isolation afin d'exécuter les privilèges root de l'hyperviseur à la place des privilèges machine virtuelle. Cela permet à un attaquant d'interagir directement avec l'hyperviseur. Par conséquent, l'évasion de la machine virtuelle à l'isolement est assurée par la couche virtuelle. Par le biais de cette attaque, un attaquant obtient l'accès au système d'exploitation de l'hôte et aux autres machines virtuelles en cours d'exécution sur la machine physique.
- Rootkit dans l'hyperviseur: Les Rootkits présents dans la machine virtuelle lancent un hyperviseur afin de compromettre le système d'exploitation de l'hôte. Le nouveau système d'exploitation est supposé en cours d'exécution en tant que système d'exploitation de l'hôte avec le contrôle correspondant aux ressources. L'hyperviseur de l'attaquant va également créer un canal secret pour exécuter du code non autorisé dans le système. Cela va lui permettre d'acquérir le contrôle sur tout le fonctionnement de l'hôte, des machines virtuelles en cours d'exécution et des activités présentent dans le système.

- **Attaque d'usurpation des méta-données**

Dans ce type d'attaque, un adversaire va modifier ou changer la description des services Web du langage WSDL où des descriptions sur les instances des services sont stockées. Si l'adversaire réussit à interrompre le code d'invocation d'un service de WSDL, cette attaque peut être possible. Pour surmonter une telle attaque, les informations sur les services et les applications doivent être conservées sous forme chiffrée. Un mécanisme d'authentification forte et d'autorisation devrait être appliqué pour renforcer l'accès à cette information critique.

- **Attaque d'espionnage**

L'espionnage implique l'acte d'écouter un canal de communication établi entre deux utilisateurs autorisés. Dans un environnement Cloud, un espion de trafic intercepte passivement les données transférées au sein du Cloud en chargeant un code dans le serveur Cloud, ou écoute les données échangées entre l'utilisateur et le CSP, il peut réaliser alors une copie non autorisée des messages. L'attaquant peut utiliser les informations recueillies illégalement pour obtenir les informations d'identification valides d'un utilisateur autorisé

pour lancer des attaques. L'attaque d'espionnage dans un environnement Cloud, se traduisant par la divulgation d'informations, peut être minimisée par l'application des procédures d'autorisation appropriées et en transmettant les données via une connexion sécurisée HTTPS : chiffrer les données transmises et joindre une signature pour aider le destinataire à assurer l'intégrité et l'authenticité des données. Les protocoles d'authentification qui protègent les secrets, assurent l'anonymat de l'utilisateur et les protocoles PAKE « **P**assword **A**uthenticated **K**ey **E**xchange » sont préférés dans les environnements Cloud.

- **Attaque par rejeu**

Dans cette attaque, le message d'authentification contient les mêmes jetons d'authentification préalablement échangés entre un utilisateur autorisé et le prestataire de services. Ce jeton va être sniffé et rejoué par un attaquant. La solution pour empêcher l'attaque par rejeu (ce qui implique l'usurpation d'identité) est de veiller à ce que quelque chose dans le message doit changer à chaque instant. Compte tenu de cet aspect, de nombreux protocoles utilisent des estampilles temporelles ou des valeurs générées aléatoirement (les nonces) pour résister à ce type d'attaque, ce qui permet au vérificateur de vérifier la fraîcheur ou l'authenticité du message. L'utilisation des estampilles temporelles exige la synchronisation des temporisations à la fois de l'utilisateur des services Cloud et du vérificateur, qui peut ne pas être facilement réalisable dans un environnement Cloud distribué. Par conséquent, les nonces sont plus préférables dans un tel environnement et étant donné que ces valeurs sont uniques pour chaque session, le récepteur sera en mesure d'identifier une rediffusion du message envoyé au préalable contenant une ancienne valeur de nonce.

- **Attaque de détournement de session « Session Hijacking »**

Le détournement de session est possible, si les identifiants de session émis aux utilisateurs authentifiés ne sont pas protégés correctement. Ces identifiants seront peut être utilisés pour l'usurpation d'identité. Ces attaques utilisent des outils de sniffing de paquets pour capturer une séquence de login et ainsi accéder à la clé de session de l'utilisateur. Ces attaques exploitent les failles présentent dans les protocoles de communication non sécurisés ou les données ne sont pas chiffrées. Ces attaques peuvent être contrecarrées en utilisant un protocole de communication sécurisé tel que le HTTPS, en chiffrant les fichiers qui contiennent les informations d'identifications des utilisateurs. Un mécanisme d'authentification forte qui exclut la possibilité d'authentification non autorisée et des mécanismes qui protègent les secrets, tels que des clés de session, sont nécessaires dans un environnement Cloud afin de prévenir de telles attaques. L'attaque peut être atténuée en évitant le transfert des clés de session à travers le canal de communication. Un mécanisme d'échange de clés, qui implique le calcul de la clé de session par le client et le serveur séparément, ayant pour résultat la même valeur de clé, peut être adopté.

- **Attaque de réflexion**

Cette attaque est effectuée sur les systèmes d'authentification mutuelle. Elle se réalise généralement en créant des sessions parallèles lancées par un attaquant (utilisateur non autorisé), dans le but d'établir une session valide avec le serveur. L'attaquant usurpe l'identité d'un utilisateur valide et demande l'ouverture d'une session avec le serveur. Le serveur, dans le cadre de l'authentification du demandeur, lui envoie un challenge et demande donc à l'attaquant de renvoyer sa réponse secrète. Comme l'attaquant n'est pas un utilisateur légitime, il ne saura pas trouver ce secret. Il crée alors une autre session et envoie au serveur, le secret reçu du serveur dans la première session. En réponse, lorsque le serveur répond avec un autre secret, l'attaquant l'utilisera à la première session qui sera une session valide pour

le serveur. L'attaquant peut alors gagner l'accès aux ressources du système avec les privilèges d'un utilisateur légitime. En 2013, le fournisseur de spam, Spamhaus a été affecté par l'attaque de réflexion menant à une des plus grandes attaques par déni de services jamais vu, produisant plus de 300 gigabit de trafic.
Dans le Cloud, le fait de garder la trace des sessions et des secrets utilisés pour chaque session, ainsi que de limiter le nombre de sessions établies, peuvent aider à minimiser ces attaques.

3.3.2. Les attaques internes

Ces d'attaques ont lieu quand une personne/une équipe, un partenaire d'une organisation, un employé (actuel ou ancien), etc. possédant des connaissances de la façon dont le système Cloud fonctionne, du client au serveur, utilisent à mauvais escient et abusent de leurs droits pour accéder aux ressources sensibles de l'organisation. Ceci va affecter négativement la confidentialité, l'intégrité ou la disponibilité du système. Ils peuvent par conséquent, implanter des codes malveillants pour tout détruire ou détruire une partie du système Cloud. Cette attaque est alors lancée par une personne se trouvant à l'intérieur du périmètre de sécurité dont le but est délibérément de compromettre la sécurité sans être détectée.
Généralement, l'attaque interne peut provenir d'un administrateur Cloud malintentionné, ou des employés qui exploitent les faiblesses du Cloud pour acquérir des accès non autorisés, ou plus, utiliser les ressources du Cloud pour mener des attaques contre l'infrastructure informatique locale de l'organisation. Le CSP doit donc avoir des politiques de contrôle d'accès de sécurité solubles et des solutions techniques mises en place empêchant une éventuelle escalade de privilèges par les utilisateurs. Le CSP doit également activer un audit des actions des utilisateurs, supporter la séparation des tâches et le principe du moindre privilège attribué aux utilisateurs afin de prévenir et de détecter les activités malveillantes. **[14]**

Par conséquent, les attaques internes sont plus faciles à lancer par rapport aux attaques externes, étant donné que l'attaquant interne possède des privilèges plus élevés et des connaissances liées au réseau, aux mécanismes de sécurité déployés et aux ressources, par rapport à l'attaquant externe. Ce dernier a besoin d'investiguer et de collecter différents types d'information avant de pouvoir exécuter son attaque.

3.4. Mécanismes de sécurité dans le Cloud

La sécurité dans le Cloud est partagée en sécurité physique, sécurité logique et sécurité des données. Etant donné que dans notre travail, nous nous focalisons sur l'authentification et les accès aux services dans le Cloud, cela implique que c'est la sécurité logique qui nous intéresse le plus. La section suivante va donc donner un bref aperçu sur la sécurité physique et la sécurité des données et le détaille de la sécurité logique dans le Cloud. **[15]**

3.4.1. La sécurité physique dans le Cloud

Le Cloud Computing, par nature, est associé à une dématérialisation de l'hébergement : un nuage. En conséquence, les lieux d'hébergement sont multiples et répartis sur plusieurs centres de données « Data Center ». Dans le Cloud public, le client ne connaît pas avec exactitude le ou les lieux d'hébergement. La sécurité physique concerne alors:

- *L'accès physique*
  L'accès physique d'une personne malintentionnée possédant une bonne connaissance de l'implémentation physique du Cloud et de ses points importants/névralgiques, peut être suffisant pour mettre le Cloud hors service. Cela va engendrer une rupture dans la continuité du service et empêchera tout accès externe au Cloud. Les conséquences peuvent être néfastes telles que l'isolement complet ou partiel du service, perte des données en production, des données sauvegardées, risque d'incendie, etc.

- *Contrôle et traçabilité des accès*
  Le contrôle des accès doit être maitrisé dans le contexte du Cloud, car il constitue un point délicat de la sécurité physique. Il convient de bien délimiter les zones les plus sensibles, telles que les serveurs et le réseau. L'accès à ces zones doit être interdit ainsi que la limitation du passage à ces zones. Le personnel autorisé devra être informé du caractère sensible de ces zones. Au-delà des contrôles d'accès, il est aussi important de porter attention à la conception sécurisée des datacenters d'hébergement.

- *Redondance matérielle*
  L'architecture Cloud doit assurer une très haute disponibilité lors de l'accès aux services, avec des performances optimales. La défaillance d'un équipement matériel peut causer une dégradation ou une coupure du service, allant jusqu'à la perte de données. Pour limiter ces risques, il est nécessaire d'implémenter la redondance d'équipements. Une réplication des configurations entre les équipements peut faciliter la bonne prise en charge de la redondance. Elle peut ainsi augmenter la haute disponibilité du service, en plus de la redondance des connexions par la multiplication des liaisons, des opérateurs et des chemins d'accès permettant une accessibilité supérieure aux services.

- *Résilience*
  Une architecture de secours doit exister, sur un site géographiquement éloigné, avec des équipements redondants permettant de réaliser un plan de continuité, sans interruption de service. Cette précaution est nécessaire dans le cas d'une catastrophe de provenance humaine ou naturelle, qui peut avoir des conséquences vitales sur le fonctionnement du Cloud, engendrant une panne totale ou partielle du service. La perte totale de l'infrastructure Cloud pourrait donc entrainer une interruption de service d'une durée indéterminée et une perte de données irréparable sans possibilité de remise en service de l'infrastructure.

3.4.2. La sécurité des données dans le Cloud

La sécurité des données comporte:

- *Responsabilité juridique de la sécurité et de la confidentialité des données*
  Les données et leur utilisation sont la responsabilité juridique du client. Le prestataire lui, a des obligations techniques et organisationnelles. Ce dernier doit également garantir l'intégrité et la confidentialité des données, en empêchant notamment tout accès ou utilisation fraudeuse et en prévenant toutes altérations, pertes ou destructions de ces données. Sa responsabilité juridique peut être retenue dans le cas d'un transfert des données de ses clients sans les prévenir. Généralement, plus l'infrastructure

est livrée au CSP, plus sa responsabilité est importante. Dans le cas du PaaS et du SaaS, le client ne contrôle que le contenu de ses données.

- *Protection et récupération des données*
  Deux métriques permettent de mesurer l'efficacité d'un processus de protection des données. Le premier est le RTO « **R**ecovery **T**ime **O**bjective » : qui mesure le temps toléré de rétablissement du service lors d'une panne. Le second est le RPO « **R**ecovery **P**oint **O**bjective » : qui mesure la quantité de données tolérée à perdre suite à une panne ou au processus de restauration.
  Pour les entreprises, une phase d'analyse est indispensable afin d'identifier les applications et données critiques pour mettre en place une politique de protection adaptée. Plus les données sont critiques, plus la fréquence des copies doit être élevée avec un besoin d'accès et de performances plus important. Le Cloud étant basé sur une infrastructure, il faut tenir compte de cette spécificité en termes d'évolutivité, flexibilité, migration, mobilité et colocation sécurisée. Après la mise des données dans le Cloud, quelle garantie à propos de l'intégrité et de la disponibilité de ces données? Faut-il continuer à sauvegarder et restaurer ces données ?
  En réalité, il s'agit d'un déplacement des responsabilités vers le CSP. Les SLAs (**S**ervice **L**evel **A**greements) définissent, pour chaque groupe de consommateurs Cloud, les niveaux de services attendus. L'infrastructure doit donc être en «Always On» sans arrêt de service.

- *Intégrité des données*
  Un Cloud sûr implémente un contrôle d'accès, c'est la fonctionnalité du RBAC «**R**ole **B**ased **A**ccess **C**ontrol»: méthode permettant de définir un certain nombre d'actions à réaliser par un utilisateur/un administrateur au sein du Cloud. Le but est de définir plusieurs rôles où chacun possèdera des permissions et des privilèges différents.

- *Chiffrement lié à la donnée*
  Les challenges du chiffrement dans le Cloud sont difficiles, surtout quand il s'agit de protéger les données hébergées contre des accès non-autorisés de la part de l'hébergeur ou toute tierce partie. Des travaux sont en cours chez la communauté IT, pour mettre en œuvre un chiffrement adéquat à ces situations afin de fournir un équilibre entre sécurité et efficacité. Ceci permettra de manipuler et d'effectuer des recherches sur des données chiffrées sans les déchiffrer, tout en vérifiant leur intégrité.

- *Données du Cloud accessibles aux autorités d'un autre pays*
  Tout pays a le droit légal d'avoir l'accès, dans les conditions juridiques qui lui sont propres, aux données qui sont stockées sur son territoire, ou qui transitent par lui. Il faut donc s'assurer contractuellement du ou des pays où seront physiquement installés les éléments d'infrastructures et de connaître les juridictions, avant de s'engager dans un contrat de service Cloud avec le CSP.

- *Réversibilité : changer de Cloud*
  Lors de l'engagement dans une solution Cloud, il faut savoir, a priori, comment pouvoir la quitter. Il faudrait également savoir comment avoir l'assurance du premier prestataire, que les données, après récupération, seront bien effacées. Pour faciliter la migration entre Cloud, il existe plusieurs APIs Cloud émergentes utilisées par un nombre significatif de CSP.

3.4.3. La sécurité logique dans un environnement Cloud

La sécurité logique dans un environnement Cloud englobe:

- *Sécurité des serveurs virtuels*
  Dans le Cloud, les technologies d'abstraction de services constituent le point d'appui. Dans l'IaaS, la virtualisation de serveurs assure cette abstraction. L'élément de base étant une machine virtuelle sur un hyperviseur. Ce dernier héberge également une machine virtuelle particulière appelée partition de gestion. Elle permet d'administrer l'hyperviseur, de gérer le matériel et les ressources virtualisées. La sécurité liée à la virtualisation se divise en deux familles. Il s'agit en premier, de sécuriser les systèmes, en fournissant une gestion des mises à jour de sécurité. Il s'agit également de restreindre les accès aux services de la partition de gestion afin de minimiser les surfaces d'attaque. Les fichiers des disques virtuels sont également protégés par le contrôle d'accès, l'audit, voire le chiffrement. La seconde famille concerne la notion d'isolation: isolation des machines virtuelles et isolation des flux réseaux.
  L'infrastructure Cloud, pour être efficace et rentable, doit automatiser la plupart des contraintes évoquées, en plus des processus liés à l'administration, la supervision et l'allocation automatique de ressources.

- *Colocation sécurisée*
  Cette propriété comporte l'hébergement des applications et données sur le Cloud provenant de multiples clients au sein d'une seule infrastructure physique, mutualisée, avec respect de la sécurité, notamment la confidentialité. Les entreprises clientes du Cloud doivent être rassurées que leurs données et traitements sont bien isolés et protégés des autres sur l'infrastructure partagée. C'est généralement une obligation légale, par exemple lorsqu'une entreprise stocke des numéros de cartes bancaires ou des données personnelles notamment médicales. Ceci est assuré en appliquant les bases de la sécurité d'un système d'information mutualisé : planification des droits d'accès, des privilèges administrateurs, sécurisation des mots de passe en plus d'un chiffrement: méthode sécurisée (selon la taille de la clé) et sélective (choisir de chiffrer que ce qui le requiert).

- *Segmentation réseau*
  Les mêmes règles doivent être appliquées dans la virtualisation que dans une architecture physique: Cloisonner les différents rôles sur des machines virtuelles différentes via des VLANs différents (réseau dédié à une machine virtuelle ou à un rôle) entre le serveur physique et l'infrastructure du client, mettre en place les firewalls, reverse proxy, etc.
  Les risques accentués par le Cloud, liés à la multi-location: la colocation et le partage de l'infrastructure entre plusieurs clients augmentent les risques et nécessitent un renforcement de la politique de sécurité, chiffrement des sauvegardes, conflits et usurpation d'adressage. Ainsi, une attention particulière doit être portée à la liste des personnes ayant un droit d'administration sur le Cloud.

- *Sécurisation des accès*
  Pour maitriser la sécurité de bout en bout, il faut sécuriser les éléments constituant la plate-forme Cloud, mais aussi, l'accès à cette plate-forme. Dans le cas d'un accès aux services hébergés sur le Cloud via Internet, le serveur (la machine virtuelle)

est nativement vulnérable puisqu'il est directement exposé sur la toile. Deux solutions de sécurisation peuvent être appliquées:

• Inclure les briques de sécurité type firewall (ouvrir que les ports applicatifs nécessaires), IPS ou IDS (détection et protection d'intrusions) entre l'infrastructure Cloud et le client.

• Sécuriser chaque serveur virtuel par un firewall applicatif installé sur l'OS (ou IPS, IDS applicatif).

Ce type d'accès n'est envisageable que pour des serveurs hébergeant des données publiques (serveur FTP public, site web…) peu sensibles pour l'entreprise. Si le serveur héberge des services privés de l'entreprise (ERP, CRM, Intranet…) et constitue alors une extension du SI, le serveur ne doit pas être visible d'Internet et des solutions de connexions dédiées doivent impérativement être envisagées, telles que la connexion VPN privée ou connexion VPN Internet.

- *Accessibilité*

  Il faut s'assurer que le service hébergé reste accessible par les utilisateurs, quel que soit le type de connexion au Cloud (connexion dédiée ou via Internet). L'accessibilité aux serveurs doit être ajustée au niveau de la disponibilité de ceux-ci. Tout comme la redondance offerte par les offres Cloud, l'accessibilité doit donc être renforcée par une redondance à tous les niveaux. En effet, une infrastructure Cloud ultra disponible ne servira pas s'il n'y a pas d'accès.

- *Adaptabilité aux pics de charge*

  Une forte charge non prévue sur un des services hébergés sur l'infrastructure Cloud risque d'entrainer une dégradation des performances du service. Pour éviter cela, la mise en œuvre d'un mécanisme de flexibilité des ressources s'avère nécessaire pour permettre d'adapter la plate-forme aux besoins en un temps minimum.

- *Impact de la gestion des mises à jour de sécurité sur la certification*

  La gestion des mises à jour de sécurité est essentielle pour certains types de certification, car ne pas les installer est égal à perdre une telle certification. Par exemple, les solutions d'IaaS privées incluent obligatoirement une gestion automatisée des mises à jour. Pareil aux offres de SaaS publics, l'avantage étant de déléguer au Provider la gestion des mises à jour.

- ***Authentification***

  Une personne malintentionnée accédant aux interfaces d'administration du Cloud peut provoquer une coupure de service ou altérer les données hébergées. Si l'accès authentifié n'est pas sûrement identifié, il sera alors impossible de tracer la connexion et la modification engendrée des données ou du service. L'authentification doit apporter une preuve de l'identité pour pouvoir enquêter sur d'éventuels accès étranges. Les bonnes pratiques sont :

  • L'identification pour avoir une traçabilité des accès.

  • Mise en place de mécanismes d'authentification forte (reposant sur deux facteurs ou plus) : identifiant, mot de passe, accès par jeton, certificat électronique, contrôle biométrique.

  • Journalisation des authentifications réussies et échouées.

  • Application d'une politique de sécurité: changement des mots de passe tous les mois, politique de mots de passe complexes, etc.

Notre étude se base sur le mécanisme d'authentification qui est un élément très important de la sécurité logique dans le Cloud. Ce mécanisme fera l'objet du chapitre suivant. L'identification ainsi que la gestion des identités étant un élément de base qui précède l'authentification, il sera détaillé dans la section suivante.

4. Gestion des identités et des accès dans le Cloud

Les points suivants demandent à être étudiés lors de : l'évaluation, l'implémentation, la gestion et la maintenance des solutions de Cloud Computing: **[16]**

- ***Gestion des identités et des accès* :** Les fournisseurs de services doivent fournir des identités à leurs clients. Ces fournisseurs doivent ensuite pouvoir gérer les accès aux services Cloud en se basant sur les identités préalablement attribuées.
- *Gestion de la conformité et des risques* : Les organismes/entreprises ayant une partie de leurs activités sur le Cloud sont responsables de la conformité, de la sécurité et des risques liés à leurs opérations.
- *Intégrité des services* : Les services basés sur le Cloud doivent être conçus et exécutés avec comme première priorité la sécurité. Les processus opérationnels doivent par contre être intégrés au système de gestion de la sécurité de l'organisme/entreprise.
- *Intégrité des points de terminaison* : La sécurité, la conformité et l'intégrité des sites utilisateurs doivent être soigneusement étudiées.
- *Protection des informations* : Les services Cloud nécessitent des processus fiables de protection des informations manipulées avant, pendant et après l'utilisation.

Des stratégies bien définies autour des cinq points susmentionnés, ainsi qu'une infrastructure solide de services peut garantir que ces services fournissent des fonctions de Cloud Computing qui respectent les exigences de sécurité.

Comme discuté ci-dessus, la gestion des identités constitue une question importante qui doit être bien étudiée dans tout environnement de Cloud Computing, afin d'offrir des services sécurisés aux utilisateurs légitimes. Pouvoir accéder aux ressources d'un Provider représente la condition initiale pour pouvoir les exploiter. Mis à part les failles, toute la sécurité tient dans la manière dont est conçue l'identification des utilisateurs autorisés et leur niveau d'accès, la sécurité commence donc par l'identité. Pour bien comprendre la notion d'identité (et relativement les attributs de l'identité) ainsi que sa gestion, les définitions suivantes sont adoptées : **[17]**

- **L'identité :** C'est l'ensemble de données qui définit de manière unique un utilisateur et le distingue des autres. Tous les utilisateurs d'un système doivent posséder une identité afin qu'ils puissent avoir un accès sécurisé aux ressources et aux services au sein du système.

- **Les Attributs de l'identité :** Constituent les pièces individuelles à propos d'un utilisateur qui le définissent, ainsi que ses interactions avec les autres utilisateurs.
  Les attributs de l'identité peuvent être quelque chose que l'utilisateur possède, comme un nom, quelque chose que l'utilisateur connaît, comme un code PIN[3], ou quelque chose que l'utilisateur est comme un scan de la rétine ou les empreintes digitales. Dans le cas de la plupart des systèmes de Cloud Computing, les attributs de l'identité peuvent être classés dans les deux premières catégories.

[3] **PIN** « **P**ersonal **I**dentity **N**umber »: Numéro d'identification personnel

Les attributs de l'identité contiennent souvent des informations qui peuvent identifier personnellement un utilisateur, comme le numéro de sécurité sociale, le nom ou l'adresse. Cette information est appelée informations personnellement identifiables: PII « **P**ersonally **I**dentifiable **I**nformation ». La Protection des PIIs de la diffusion non désirée ou non autorisée est souvent une obligation légale et appartient au domaine de la protection des données personnelles.

- **La Gestion de l'identité :** Se réfère à la création, la modification et la suppression des objets de l'identité. Elle fournit la première ligne du contrôle d'accès de tout système. Avant de pouvoir donner l'accès à un utilisateur, le système doit d'abord être en mesure de l'identifier et de déterminer s'il doit lui accorder l'accès. Pour ce faire, l'utilisateur doit avoir obtenu au préalable des informations d'identification, sous la forme d'un objet d'identité. Les informations d'identification associées à l'objet de l'identité pourraient être n'importe quelle combinaison des attributs de l'identité. Le but d'un système de gestion d'identité est de permettre à un organisme de créer un objet d'identité pour chaque utilisateur, de gérer les identités et leurs propriétés (par exemple à quel groupe un utilisateur appartient, quand le mot de passe d'un utilisateur expire automatiquement, etc.) et supprimer les identités une fois que l'utilisateur n'ait plus besoin d'accéder au système.

Selon **[16]** « Tout système de gestion des identités numériques dans le Cloud doit être interopérable entre plusieurs entreprises et prestataires et doit reposer sur des processus fiables ».
Un système de gestion des identités numériques, qui offre une authentification forte et des fonctions interopérables, peut largement améliorer la sécurité et l'intégrité des données. Les systèmes de certification et de réputation jouent un rôle important dans la gestion des identités. Les services basés sur le Cloud nécessitent donc un système de protection contre l'utilisation abusive des identités des utilisateurs, notamment le vol d'identité. Les systèmes de contrôle des identités et des accès, doivent se baser sur une infrastructure qui utilise des informations d'identification personnelles et à chiffrement fort. Les noms d'utilisateur et mots de passe habituellement utilisés dans les systèmes de gestion des accès doivent être remplacés par des informations d'identification robustes. **[16]**

Le transfert de services vers le Cloud engendre plusieurs questions quant à l'identité:

- Qui est le détenteur de l'identité ?
- Quels contrôles encadrent la gestion des identités et des accès ?
- L'entreprise peut-elle changer de prestataire de déclarations d'identité ?
- Quelles sont les différences entre les méthodes de gestion des identités adoptées par chaque prestataire de services?
- De quelle manière l'authentification et l'autorisation sont-elles liées à l'identité ?
- Comment la collaboration avec un partenaire tiers, utilisant un fournisseur d'identité différent, est-elle possible ?

5. Notion de protection des données personnelles ou « Privacy[4] »

5.1. Aperçu et définition

Il demeure rare dans Internet que l'on puisse vraiment cacher son identité. En effet, en accédant à des contenus/services (sites web, transactions en ligne, courrier électronique,

[4] Le terme en anglais « **Privacy** » sera adopté pour la suite du document.

réseaux sociaux, au Cloud, etc.), l'utilisateur peut révéler intentionnellement ou à son insu des informations sur son emplacement, ses intérêts et ses habitudes de navigation. Les informations sur les habitudes et les préférences des utilisateurs revêtent beaucoup d'intérêt à des fins de marketing. Il existe des outils de repérage qui permettent de recueillir automatiquement ces informations en ligne à l'insu des utilisateurs. Généralement, il s'agit d'indications anodines : adresse IP, site web et fichiers consultés, temps passé sur chaque page etc. Une fois rassemblées, ces bribes d'informations anodines peuvent aboutir à la création d'un profil descriptif que les utilisateurs ne tiendraient pas à divulguer notamment le fait que le profil en ligne puisse être rattaché à leur véritable identité. **[33]**
La protection des données personnelles est une propriété changeante selon les circonstances, les personnes concernées et les valeurs d'une société ou d'une communauté. Généralement, elle concerne la vie personnelle (identité, origine raciale,...), le secret professionnel, le secret médical, la protection de l'identité et de l'image, la protection de la correspondance et la réglementation des écoutes téléphoniques, la vie familiale et le domicile **[18]**. La protection des données personnelles sur Internet prend une dimension plus importante que celle habituellement admise dans la vie de tous les jours. Il est indispensable de bien comprendre que toute information non sécurisée mise en ligne peut être accessible par n'importe qui. Cela étant dû à l'universalité d'Internet et de sa propension à diffuser rapidement une information importante.
Dans le contexte des consommateurs, la protection des données personnelles implique la protection et l'utilisation appropriée de leurs informations personnelles et les attentes des utilisateurs au sujet de leurs utilisations : au sujet de la collecte, l'utilisation et la divulgation de ces informations personnelles et d'autres informations contextuelles. Pour les organisations, la protection des données personnelles entraîne l'application des lois, des politiques, des normes et des processus par lesquels l'information personnelle est gérée. Une manière de percevoir la protection des données personnelles est «l'utilisation appropriée des informations personnelles dans les circonstances où elles se trouvent». **[19]**

La sécurité est une condition nécessaire mais non suffisante pour assurer la privacy. La privacy diffère de la sécurité, en ce qui concerne les mécanismes de manipulation des informations personnelles, portant sur les droits individuels et les aspects tels que l'équité de l'utilisation, le choix, l'accès et la responsabilité. De nombreuses lois sur la privacy limitent également la transfrontière des flux de données d'informations personnelles. Les mécanismes de sécurité, d'une autre part, se concentrent sur la fourniture de mécanismes de protection qui incluent : l'authentification, les contrôles d'accès, la disponibilité, la confidentialité, l'intégrité, le stockage, la sauvegarde, la réponse aux incidents et la récupération. La privacy concerne les informations personnelles uniquement, tant dis que la sécurité et la confidentialité peuvent se rapporter à toutes les informations.

La notion de « Privacy » étant un concept relatif, sa définition a souvent engendré une certaine controverse. En général, toutes les définitions l'associent au besoin des personnes à garder leurs informations sensibles secrètes, sûres et sous contrôle. La privacy est :

« *L'aptitude d'un système à protéger l'identité et la localisation de ses utilisateurs contre la divulgation non autorisée* ». **[21]**

La privacy est vue également comme étant le droit des individus de déterminer comment et quand leurs données personnelles sont partagées avec d'autres parties **[17]**.

Les données à caractère personnel comprennent toutes les informations relatives à une personne physique, qu'elles se rapportent à sa vie privée, professionnelle ou publique. Il peut s'agir d'un nom, d'une photo, d'une adresse de courrier électronique, de coordonnées bancaires, de messages postés sur Internet, de données médicales etc.
Les données à caractère personnel peuvent constituer des informations sensibles, à titre d'exemples, les informations sur la religion ou la race, l'appartenance syndicale, les informations de santé (enregistrements médicaux), les données biométriques et toute autre information considérée comme sensible. Ces informations, d'un point de vue de la protection des données personnelles, exigent des garanties supplémentaires quant à leur manipulation, leur sauvegarde etc. **[22]**
Les informations qui peuvent identifier directement ou indirectement une personne, sont appelées informations personnelles identifiables PII **«P**ersonally **I**dentifiable **I**nformation». La protection des données personnelles impose des normes pour la collecte, l'entretien, l'utilisation et la divulgation des PII.
« *Le PII inclut toute information qui peut être utilisée pour identifier ou localiser un individu (par exemple le nom, l'adresse) ou toute information qui peut être corrélée avec d'autres informations pour identifier un individu (par exemple, le numéro de carte de crédit, le code postal)* ». **[22]**

Une atteinte à la privacy se produit lorsque des données personnelles relativement confidentielles sont révélées à un adversaire. Dans ce contexte, l'adversaire est toute entité collectant des traces numériques d'un individu. L'adversaire peut être un individu, une organisation ou une compagnie. Les données collectées peuvent être des :
- sources d'informations publiques.
- traces récupérées de manière passive.
- données récupérées par l'exploitation d'une vulnérabilité du système.

Chaque individu laisse continuellement des traces numériques qui peuvent être reliées à son identité. Le danger peut provenir de toute entité non autorisée, qui peut mener une action malveillante après l'utilisation des traces numériques collectées d'un individu : déduire un *profil de ses intérêts*, ou encore plus, *usurper l'identité de l'individu ciblé*.
Les données collectées par un adversaire sont généralement des sources d'informations publiques (réseaux sociaux, blogs, images, e-mail, agrégateurs de données : moteur de recherche spécialisé dans la collection et la fusion de données à caractère personnel). **[20]**
Exemple d'utilisation de traces numériques:

- Adresse IP => Localisation
- Historique => Centre d'intérêts
- Connaissance du réseau social => Inférences sur opinions politiques, religion, loisirs.

Le but principal de la privacy est de permettre aux individus de minimiser et de contrôler leurs traces numériques.

5.2. Propriétés principales de la privacy

Quatre propriétés principales relatives à la notion de privacy sont définies dans **[23]**: l'anonymat, le pseudonymat, la non-chaînabilité et la non-observabilité.

- **Anonymat:** implique que d'autres utilisateurs sont incapables de déterminer la véritable identité associée à un sujet, une opération ou un objet.

- **Pseudonymat:** garantie qu'un utilisateur puisse utiliser une ressource ou un service sans révéler son identité, mais peut être tenu « responsable » de ses actes.
- **Non-chaînabilité:** c'est l'impossibilité pour d'autres utilisateurs d'établir un lien entre les différentes opérations faites par un même utilisateur.
- **Non-observabilité:** consiste à ce que les utilisateurs ne puissent pas déterminer si une opération est en cours. La non-observabilité assure la protection de l'activité d'un utilisateur contre un tiers qui ne peut pas présumer qu'une ressource ou un service est utilisé.

5.3. Privacy dans le Cloud

Les consommateurs de services de Cloud Computing (utilisateurs) ont peu de connaissances sur le fonctionnement interne du système du fournisseur (CSP). Ce manque de transparence induit à un manque de confiance entre les utilisateurs et les fournisseurs de services Cloud. **[17]**.

De nombreuses lois existent à propos de la privacy imposant des normes pour la collecte, l'entretien, l'utilisation et la divulgation des informations personnelles identifiables (PII) et qui doivent être respectées même par les CSPs dans les environnements Cloud **[24]**.
Le modèle « Utilisateurs + Cloud » propose à moindre coût plus de choix, de flexibilité et d'efficacité opérationnelle aux différentes entreprises, institutions et particuliers. Pour tirer pleinement parti de tous ces avantages, des garanties doivent être apportées en matière de confidentialité et de sécurité notamment quant à la protection des données personnelles. De ce fait, en raison de la nature du Cloud Computing, il existe peu ou pas d'informations disponibles pour préciser où les données sont stockées, comment elles sont sécurisées, qui en a accès et si elles sont transférées à un autre hôte (et surtout si ce hôte est de confiance). Un Cloud ne peut pas être utilisé pour le stockage et le traitement des données s'il est non sécurisé.
La mise à disposition des données sensibles à une entité externe constitue une sérieuse préoccupation. Les problèmes majeurs concernant la confidentialité des données personnelles dans le Cloud sont :

- Comment sécuriser le PII afin d'éviter toute exploitation par des utilisateurs non autorisés.
- Comment empêcher les attaques contre la divulgation des données personnelles (le vol d'identité) même si le CSP n'est pas de confiance.
- Comment maintenir le contrôle sur la divulgation des informations personnelles.
- Les données conservées quelque part dans le Cloud sont-elles aussi sûres que les données protégées dans les ordinateurs et les réseaux contrôlés par l'utilisateur ?

Dans notre contexte de travail, nous définissons la privacy dans un environnement de Cloud Computing comme étant :
« La capacité d'une entité à contrôler les informations qu'elle révèle sur elle-même au Cloud (ou au CSP) et la possibilité de contrôler qui peut accéder à ces informations ». **[24]**

Quand une entreprise externalise la gestion de ses données personnelles à une autre entité, il existe une certaine responsabilité pour s'assurer des utilisations externes «sécurité raisonnable» afin de protéger ces données. Dans le cas du Cloud Computing, le CSP doit mettre en œuvre la sécurité raisonnable lors de la manipulation des informations personnelles.

Toute organisation crée, maintien, utilise ou diffuse des données personnelles, doit s'assurer que les données n'ont pas été altérées et doit prendre des précautions pour prévenir l'utilisation abusive d'une telle information. Spécifiquement, pour assurer la sécurité du traitement de ces informations, des mesures techniques et organisationnelles appropriées doivent être mises en œuvre afin de les protéger contre tout accès ou divulgation non autorisés, destruction: accidentelle, illicite ou perte, modification inappropriée ou utilisation non autorisée (toutes autres formes de traitement illicite). **[26]**

6. Conclusion

Le Cloud étant une technologie à croissance rapide qui offre une vaste gamme d'avantages aux utilisateurs ainsi qu'aux entreprises. Cependant, la sécurité, la confidentialité des données personnelles et la confiance restent les principales préoccupations qui empêchent l'adoption massive du Cloud vu que la plupart des méthodes employées sont vulnérables à de nombreuses attaques, ce qui engendre l'insécurité des utilisateurs. Un environnement Cloud qui fournit des services variés et héberge plusieurs ressources peut être sécurisé exclusivement en permettant qu'aux utilisateurs légitimes d'accéder aux ressources.
En outre, l'autorisation des processus et la gestion des données appartenaient autrefois aux utilisateurs et malgré le fait que les données soient stockées du côté du CSP, l'autorisation doit demeurer toujours du côté des utilisateurs à la place des fournisseurs, surtout que leurs intérêts divergent souvent. Si la confidentialité des données est importante, le service Cloud basé sur l'architecture IaaS sera la solution la plus appropriée, offrant des mesures de protection et un chiffrement des données. Il est impératif que les entreprises comprennent pleinement l'environnement Cloud avec lequel elles envisagent de s'engager et ces risques associés « diligence raisonnable ». Non seulement les questions contractuelles sont importantes, mais aussi celles opérationnelles et architecturales. Il faut s'assurer que le service Cloud dispose de ressources suffisantes pour les besoins relatifs à l'entreprise notamment ceux liés à la sécurité.

Les mécanismes d'authentification forte offrent par conséquent une limitation des accès illégaux, ils représentent la condition principale pour sécuriser le Cloud. Un mécanisme d'authentification conçu pour le Cloud doit être suffisamment solide afin de le protéger des diverses attaques possibles. Etant donné que l'identité de l'utilisateur et des informations sensibles sont régulièrement utilisées dans le processus d'authentification lors de l'accès aux services Cloud, un besoin primordial est de protéger et empêcher les utilisateurs de révéler leurs informations personnelles au Cloud Service Provider.

Le chapitre suivant s'intéressera alors à l'authentification qui représente un mécanisme de base de la sécurité informatique. Il faut noter que les autres propriétés de la sécurité (l'intégrité et la confidentialité) dépendent fortement de l'authentification, vu que si celle-ci est compromise, cela impliquerait que les données à caractère privé peuvent être divulguées.

Chapitre 2: Authentification et Authentification anonyme dans le Cloud

1. Introduction

Pour pouvoir tirer parti de tous les avantages offerts par le Cloud Computing, plusieurs éléments de sécurité doivent être analysés: les processus, les technologies et les mécanismes de contrôle. Le but étant d'arriver à l'informatique de confiance « Trustworthy Computing », initié par Microsoft dans le but de rendre l'informatique plus sûre, mais aussi de rendre les services plus fiables et disponibles, tout en assurant la confidentialité des données des utilisateurs.

Actuellement, le Cloud Computing attire beaucoup d'attention à la fois dans le milieu universitaire que dans l'industrie. Avec sa scalabilité, sa collaboration, son agilité, sa disponibilité et sa réduction des coûts, le Cloud Computing offre une alternative convaincante aux solutions IT en interne. Toutefois, par l'externalisation de l'infrastructure informatique, il introduit un certain nombre de questions de sécurité. Plus précisément, le Cloud étant une plate-forme informatique commune, il doit fournir des mécanismes forts pour bien authentifier ses utilisateurs et atténuer le plus possible de vulnérabilités. Un point primordial et automatique lors de l'utilisation des services du Cloud Computing est la présence d'un bon mécanisme d'authentification. La puissance de ce système d'authentification est relative au besoin de confidentialité requis par les utilisateurs. Cependant, la gestion sécurisée des identités est critique dans tous les environnements, mais peut prendre une dimension plus complexe quand il s'agit de Cloud Computing. Cela engendre également de nouveaux défis, notamment quant à l'authentification en ligne qui doit être convenable, incluant une protection exhaustive, à la fois pour l'utilisateur et pour les données sensibles.

Dans ce contexte, ce chapitre va présenter les mécanismes d'authentification, notamment dans le Cloud, puis ceux relatifs à l'authentification anonyme. Aussi, en plus d'un mécanisme fiable et robuste, le but étant de préserver la privacy des utilisateurs Cloud via l'anonymisation de leurs identités et de leurs diverses communications. Un ensemble d'approches conçues dans cette même optique va être exposé. Enfin, une conclusion de l'étude sera le point de départ pour la proposition d'une nouvelle approche d'authentification anonyme dans un environnement de Cloud Computing.

2. Mécanisme d'authentification

L'authentification est en général, le mécanisme permettant de vérifier l'identité d'un utilisateur et d'assurer que l'utilisateur qui tente d'accéder à un système ou à un pool de ressources pour une éventuelle utilisation, est un utilisateur légitime. Un autre aspect de l'authentification est d'empêcher l'accessibilité à un utilisateur non autorisé. Le mécanisme d'authentification peut être classé en deux types: authentification de message et authentification de l'entité. L'authentification de message concerne la vérification de l'auteur d'un message par le destinataire du même message, tandis que l'authentification de l'entité assure l'identification d'une entité lors d'une communication. La différence est que l'authentification de message n'est pas limitée par une période de temps, contrairement à l'authentification d'entité qui est limitée par la durée de la communication. **[27]**

2.1. Définitions

« *L'authentification est le processus d'établissement de confiance dans l'identité des utilisateurs. C'est le processus qui consiste à vérifier si l'entité est celle qu'elle prétend être. L'authentification est la clé pour assurer la sécurité* » **[31]**

L'Identification est le moyen par lequel une ressource demande un identifiant spécifique et unique (la ressource peut être identifiée par d'autres moyens autre qu'un identifiant). **[28]**

L'objectif du mécanisme d'authentification est de permettre l'accès qu'aux utilisateurs autorisés. Il fournit la manière selon laquelle l'identifiant obtenu préalablement est vérifié.

L'Autorisation détermine les privilèges d'accès associés à l'identité authentifiée. Le processus d'autorisation suit l'authentification. L'autorisation est source de préoccupation pour les Services Providers et typiquement basée sur le niveau d'assurance qui émerge de la phase d'authentification. **[28]**

Le Contrôle d'accès est la discipline dans laquelle les mécanismes et les politiques sont établis pour restreindre l'accès aux ressources, uniquement aux utilisateurs légitimes **[28]**. L'authentification représente la base du contrôle d'accès.

2.2. Classification des approches d'authentification

Il existe différentes approches d'authentification, allant des mots de passe jusqu'à l'authentification par clés publiques. Le choix d'une telle ou telle technique dépend en grande partie de l'usage souhaité: authentification de l'expéditeur d'un email, authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, etc.
Les approches courantes d'authentification sont basées sur des mots de passe (statiques ou dynamiques générés par un outil logiciel ou matériel), des certificats électroniques ou des données biométriques sauvegardées dans une base de données. **[29]**
La qualité d'une approche d'authentification ne se mesure pas uniquement à ses avantages et inconvénients généraux ou à sa robustesse théorique face aux attaques, mais surtout à sa capacité de répondre aux besoins de sécurité requis. **[30]**

Le paradigme classique des systèmes d'authentification identifie trois facteurs (appelés aussi méthodes) comme la pierre angulaire de l'authentification **[31].** Toute approche d'authentification se base sur l'un des trois facteurs suivants illustrés dans la figure 2.1:

- **Authentification à base de quelque chose que l'utilisateur connait:** Méthode qui permet de vérifier l'identité des utilisateurs en se basant sur des informations mémorisées par le système lors de la phase d'inscription, par exemple : un mot de passe, une question secrète ou un numéro d'identification personnel PIN. Ce sont les méthodes d'authentification les plus populaires et classiques, puisque les données d'authentification sont faciles à mémoriser par les utilisateurs.

- **Authentification à base de quelque chose que l'utilisateur possède:** Méthode selon laquelle les utilisateurs sont authentifiés par les informations contenues dans un objet physique en leur possession. Ceci se réalise généralement grâce à une clé USB, un certificat numérique, une carte à puce, un passeport ou une carte d'identité.

- **Authentification à base de quelque chose que l'utilisateur est**: Ensemble de méthodes permettant la vérification automatique de l'identité des personnes sur la base des caractéristiques personnelles : physiologiques et/ou comportementales, par exemple, reconnaissance des empreintes digitales, faciale ou vocale.

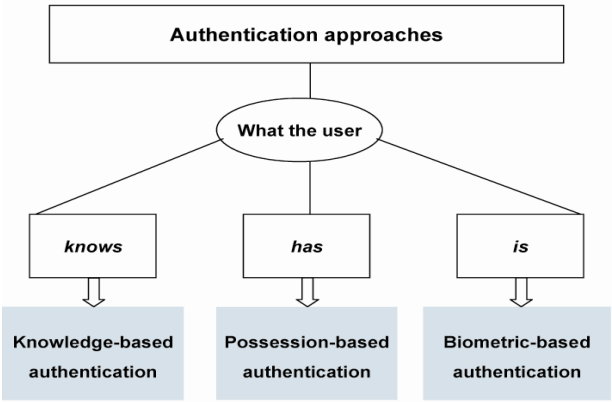


Figure 2.1 Classification des approches d'authentification selon les facteurs

Une authentification simple « Single-factor authentication » est une authentification qui ne requiert qu'un seul facteur d'authentification parmi les trois classes déjà présentées : facteur connu, possédé ou caractéristique personnelle. L'authentification à deux facteurs « Two-factor authentication » ou l'authentification multi-facteurs est basée sur deux ou plusieurs facteurs. Le terme authentification à deux facteurs (ou plus, authentification à trois facteurs) est utilisé lorsque deux (ou trois) facteurs sont nécessaires pour l'identification. Les éléments doivent être choisis parmi les trois classes déjà définies.
Les deux éléments de l'authentification à deux facteurs pourraient par exemple être une combinaison de quelque chose que l'utilisateur possède, par exemple une carte à puce ou un téléphone mobile et quelque chose que l'utilisateur connaît, par exemple un mot de passe. Lorsque l'authentification à deux facteurs ou plus est utilisée⇔ l'authentification est forte.

Parmi les différents protocoles proposés dans le cadre de l'authentification à deux facteurs, le «T-FA» populaire et censé être utilisé et adopté par de nombreux fournisseurs de services de Cloud Computing à l'avenir **[32]**. Certains services Web célèbres implémentent l'authentification à deux facteurs. La plupart de ces services offrent ce type d'authentification pour enregistrer un nouvel utilisateur. Une fois enregistré, l'authentification du service est transférée à l'authentification à un seul facteur.

Service	1er facteur d'authentification	2ème facteur d'authentification
Amazon Web Services	Mot de passe	Matériel (Hardware) ou Logiciel (Software) générateurs de Jeton
Google/ Facebook/ Dropbox	Mot de passe	Logiciel (Software) générateur de Jeton ou Message envoyé vers le téléphone mobile

Table 2.1 Authentification a deux facteurs des Providers Cloud populaires

2.3. Protocoles d'authentification

Par analogie, un protocole d'authentification électronique est le langage à utiliser pour l'authentification voir figure 2.2: **[30]**

- Les transactions d'authentification peuvent être considérées comme les phrases nécessaires pour transmettre des éléments de discussion entre les parties à authentifier.
- La structure de la phrase est dictée par les méthodes d'authentification employées qui fournissent la sémantique.
- Le facteur d'authentification, qui se réfère au secret qui doit être démontré et vérifié, peut être considéré comme le sujet de la phrase.
- La protection du secret représente le moyen pour protéger la communication de ce secret.
- Enfin, les éléments clés utilisés pour soutenir le secret représentent les adverbes et les adjectifs. Ces éléments incluent les nonces, estampilles temporelles et les identifiants de sessions utilisés afin d'assurer une meilleure protection du secret en question.

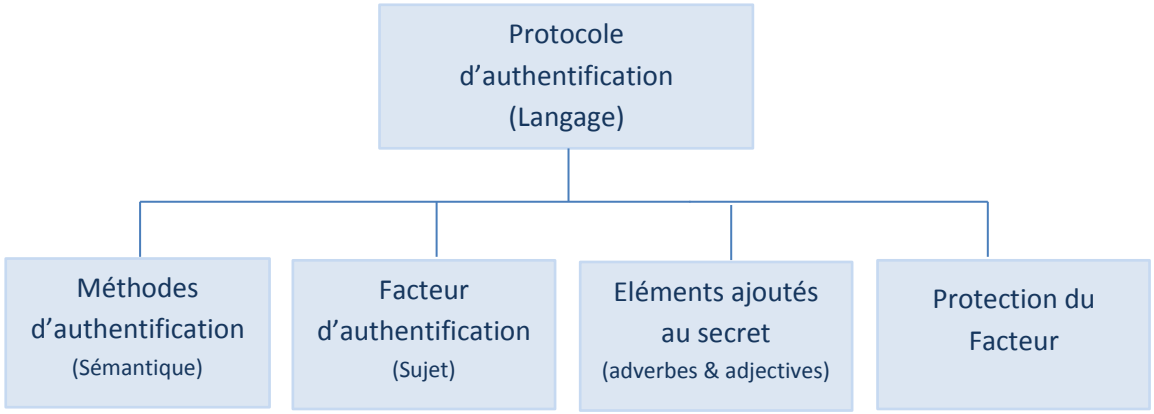


Figure 2.2 Protocole d'authentification

Selon **[30]** « *Un protocole d'authentification comporte une séquence de messages échangés entre deux parties permettant l'utilisation/la possession d'un secret, dans le but d'être confirmé*».
Un protocole d'authentification est également défini comme un type de protocole cryptographique, dont le but est l'authentification des parties qui souhaitent communiquer en toute sécurité.

Le but d'établir un protocole d'authentification entre les parties communicantes, est de pouvoir prouver un secret qui sera créé et/ou transféré et utilisé pour le reste de la session, afin d'assurer la confidentialité de toutes les données communiquées. Un protocole d'authentification étant souvent un protocole cryptographique, car il exige que les données échangées entre les parties d'authentification soient sécurisées contre la divulgation des secrets, ou toute attaque ultérieure d'usurpation d'identité. Les primitives cryptographiques les plus déployées dans les protocoles d'authentification comprennent : les signatures électroniques, le hash, les mécanismes de chiffrement / déchiffrement.

Il existe plusieurs protocoles d'authentification et méthodes disponibles. Chaque protocole d'authentification emploie certaines méthodes pour réaliser l'authentification, bien que la mise en œuvre puisse différer en termes de robustesse et des processus impliqués.

Presque tous les protocoles d'authentification ont la particularité d'utiliser des secrets, soit pré-partagés ou dérivés pour mener le processus d'authentification d'identité. Ils exploitent habituellement des nombres aléatoires, des fonctions de hachage, des défis, des nonces et des estampilles temporelles pour améliorer la robustesse ou ajouter des fonctionnalités au protocole. Comme exemple de protocoles d'authentification, nous avons le protocole **P**assword **A**uthentication **P**rotocol (PAP), **C**hallenge **H**andshake **A**uthentication **P**rotocol (CHAP), **E**xtensible **A**uthentication **P**rotocol (EAP), SSL/TLS, IPSec, RADIUS, kerberos, etc.

Les méthodes d'authentification employées dans les protocoles d'authentification gèrent dans l'ensemble un secret. La protection des secrets montre les différentes manières dont les secrets peuvent être transportés dans une session d'authentification, comme le montre la figure 2.3. Le secret peut être transmis en clair (pas de protection), protégé par l'intermédiaire de moyens cryptographiques symétriques ou asymétriques, protégé par hachage, ou encapsulé dans un tunnel à l'intérieur d'un canal de communication sécurisé (VPN)[5]. **[30]**

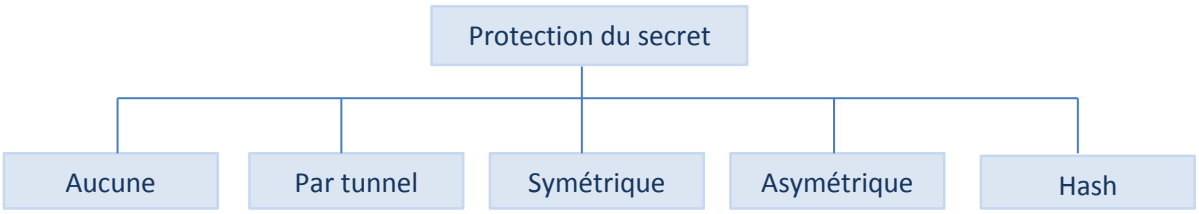


Figure 2.3 Protection du secret lors de l'authentification

Un mécanisme d'échange de ce secret doit être défini dans le protocole d'authentification spécifiant les diverses façons dont l'authentification est effectuée, pour transmettre la preuve de possession du secret PoP «Proof of Possession».
Un mécanisme d'échange d'authentification constitue un processus clé dans chaque protocole d'authentification électronique. Il fournit les moyens de communication entre les parties d'authentification et facilite les échanges de données nécessaires à l'accomplissement de l'authentification. Le mécanisme d'échange d'authentification détermine les transactions requises et les données qui devraient être transmises au sein du processus d'authentification pour établir son succès ou son échec, comme par exemple le mécanisme challenge-réponse.
Les protocoles d'authentification peuvent être divisés selon le mécanisme d'échange employé par la méthode d'authentification utilisée, à ceux qui sont fondés sur un secret pré partagé et ceux qui ne nécessitent pas un secret pré partagé. **[30]**

- **Présentation directe «Direct Presentation»:** Méthode dans laquelle l'authentification peut avoir lieu par une présentation directe du secret. La faiblesse cependant se caractérise par les attaques par rejeu ciblant le secret qui est trivialement soumis à être rejoué en étant présenté directement.

- **Challenge-Réponse «Challenge-Response»:** Une série d'échanges de messages, en termes d'un mécanisme de challenge-réponse, empêche l'observation directe du secret par un observateur en ligne. Dans les protocoles d'authentification électronique, le mécanisme de challenge-réponse est généralement mis en œuvre avec l'une des techniques cryptographiques:

[5] VPN : **V**irtual **P**rivate Network: Réseau privé virtuel.

cryptographie à clé symétrique/asymétrique et fonctions de hachage, afin de protéger le secret d'authentification contre une attaque d'observation directe.
Le challenge-réponse est l'un des mécanismes d'échange d'authentification les plus utilisés dans lequel un Vérificateur enverra un challenge au Demandeur. Ce dernier, doit fournir une réponse valable afin d'être authentifié. La forme la plus simple du challenge-réponse est lorsque le défi est une demande de mot de passe et la réponse valable est de fournir le bon mot de passe.

- **Preuve à divulgation nulle de connaissance «Zero Knowledge Proof»:** Mécanismes d'échange d'authentification qui implémentent la preuve à divulgation nulle de connaissance. Ces mécanismes sont également en mesure de prouver la possession de secrets, sans la nécessité de transmettre préalablement le secret au Vérificateur. Par conséquent, la présence d'un secret est nécessaire et est stocké à la fin. Cette manière de procéder permet efficacement de maintenir la confidentialité du secret. Cependant, pour que le Vérificateur puisse effectuer une vérification sur la possession du secret par le Demandeur, un Vérificateur de mot de passe par exemple, doit être fourni par le Demandeur au Vérificateur à l'avance. Le Vérificateur de mot de passe peut être généré sur la base de calculs mathématiques. Dans l'exemple simpliste connu, Un Vérificateur doit être convaincu qu'un Demandeur connaisse le mot de passe secret de la porte reliant les chemins A et B. Si le Demandeur est capable d'entrer à partir de la voie A et sortir par la voie B, le Vérificateur sera convaincu qu'il connaisse en effet le mot de passe secret. Il ne sera alors nécessaire au Vérificateur que de spécifier le chemin d'entrée au Demandeur. Ce dernier, doit être en mesure de suivre le protocole et déverrouiller la porte avec le mot de passe secret, sans le révéler au Vérificateur. Le Demandeur connait certainement le mot de passe secret s'il est capable de faire cela de manière répétée. Dans les protocoles d'authentification électronique, la mise en œuvre de ce type de mécanismes repose sur un certain modèle de calcul mathématique. Les protocoles sont basés sur des problèmes mathématiques durs, tels que le calcul du logarithme discret, factorisation des nombres, le calcul du produit de nombres premiers grands, etc.

3. Authentification dans le Cloud

L'authentification est un besoin pour chaque organisation. De plus elle est devenue primordiale pour toute organisation, non pas parce qu'elle fait face aux menaces de sécurité seulement, mais parce qu'elle développe des politiques, des procédures et des mécanismes qui assurent la sécurité des données, la sécurité physique et logique.

L'industrie informatique a créé une gamme de technologies d'identification et d'authentification pour les différentes entreprises, afin de répondre aux exigences de sécurité, par exemples : la paire « ID utilisateur / mot de passe », **O**ne **T**ime **P**assword «OTP», authentification biométrique, cartes à puce, protocole Kerberos, **S**ecure **S**ocket **L**ayer « SSL », **L**ightweight **D**irectory **A**ccess **P**rotocol « LDAP », **S**ecurity **A**ssertion **M**arkup **L**anguage «SAML», OpenID et CardSpace, etc. Chaque organisation adopte une ou plusieurs de ces technologies pour sécuriser les informations contre les abus et les accès non autorisés.
Dans un système d'authentification, les utilisateurs bénéficient d'un accès uniquement lorsqu'ils fournissent leurs informations d'accès en toute sécurité pour vérifier et valider leur identité. Si une personne peut prouver son identité, qu'elle connait quelque chose qu'elle seule pourrait savoir, il est raisonnable de penser que cette personne est bien celle qu'elle prétend être. L'authentification fait en sorte que les services produits soient accessibles uniquement par les utilisateurs légitimes, notamment dans le cas d'un environnement de Cloud Computing où les utilisateurs sont distribués.

3.1. Aperçu du processus d'authentification dans le Cloud

Dans le Cloud Computing, la sécurité des services est relative à chaque modèle : dans le cas du modèle SaaS, un utilisateur s'appuie sur le CSP pour accomplir toute la sécurité. Dans le modèle PaaS, l'utilisateur assume presque toutes les fonctions de sécurité sauf la disponibilité. Concernant le modèle Iaas, l'utilisateur dépend du CSP pour maintenir l'intégrité des données et la disponibilité, les utilisateurs se chargent alors de la confidentialité et le contrôle de la privacy.
Etant donné que l'industrie IT et l'ensemble de ses activités basculent leurs informations sensibles vers le Cloud, les CSPs doivent fournir un support solide aux données présentent dans le Cloud, en adoptant des mesures de sécurité consistantes. L'authentification dans le Cloud est différente de celle propre à une organisation. La vérification de l'utilisateur est différente de celle dans un réseau d'entreprise car dans le Cloud, les utilisateurs ne sont pas nécessairement connectés par un réseau, tel le réseau local de l'entreprise. La sécurité des applications Cloud dépend fortement d'un mécanisme fort d'authentification. Les entités qui répondent à un certain niveau de confiance auront l'accès au Cloud.

Lorsque les organisations utilisent les services Cloud, l'authentification des utilisateurs d'une manière fiable et flexible présente une exigence vitale. Les organisations doivent répondre aux défis liés à l'authentification, tels que la gestion des informations d'identification, l'utilisation d'une authentification forte et la confiance dans l'ensemble des services Cloud. En outre, l'authentification forte est obligatoire pour tout déploiement de Cloud. Dans un environnement de Cloud Computing, l'authentification et le contrôle d'accès sont les deux aspects les plus importants, puisque le Cloud et toutes ses données sont accessibles par tous sur Internet.

3.2. Méthodes d'authentification de base dans un environnement Cloud

Lors de l'authentification dans un environnement Cloud, les sessions Cloud doivent être bien sécurisées. Les entreprises hésitent à rejoindre le Cloud, parce qu'elles n'ont pas la certitude que ce soit un système 100% sécurisé par rapport à toutes les activités malveillantes existantes. Les sessions Cloud peuvent être sécurisées par *le chiffrement* et *un bon mécanisme d'authentification.*
De nombreux systèmes d'authentification ont été introduits pour traiter des données secrètes sur des réseaux non sécurisés ou des connexions distantes, tel le Cloud Computing. L'authentification constitue l'étape principale lors de la sécurisation des systèmes de communication, en particulier lors d'une large diffusion réseau comme le cas du Cloud Computing. Elle permet de protéger l'information partagée contre les personnes non autorisées. L'authentification détermine «Qui est l'utilisateur légal» et «L'utilisateur est-il vraiment celui qu'il prétend être». En outre, la vérification de l'identité de l'utilisateur est l'objectif le plus important derrière l'authentification. Les méthodes d'authentification dans un environnement Cloud sont généralement utilisées pour améliorer la sécurité de celui-ci, un aperçu est montré dans la figure 2.4. **[36]**

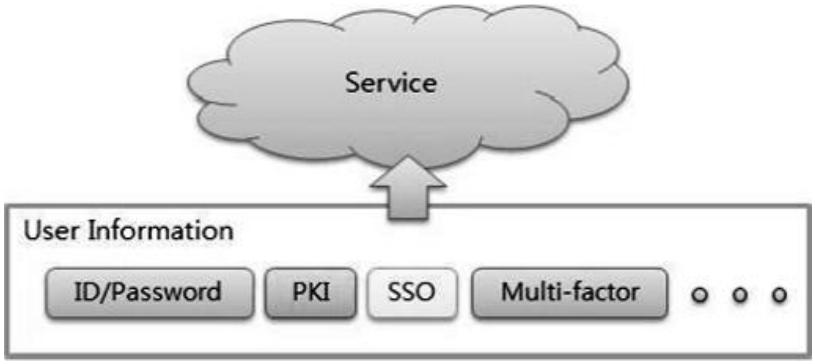


Figure 2.4 Aperçu des méthodes d'authentification pour l'accès aux services Cloud

Le point le plus important dans l'authentification est de protéger les données contre les éventuels accès des personnes non autorisées. Ceci revient à rejeter les demandes des utilisateurs inconnus et de bien gérer l'accès des utilisateurs authentifiés. Dans un environnement Cloud, les méthodes d'authentification déployées sont illustrées dans la figure 2.5: **[37]**

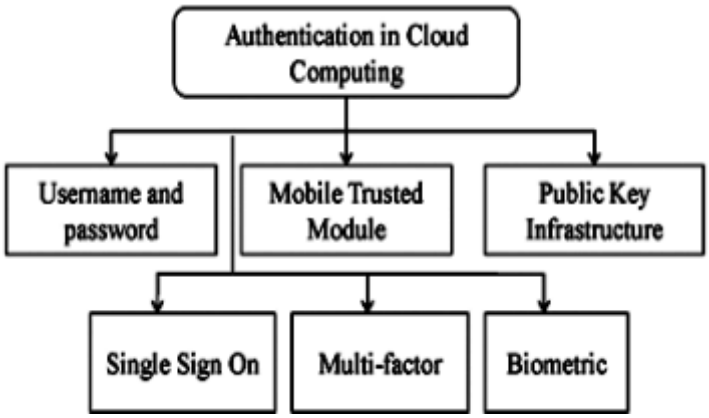


Figure 2.5 Méthodes d'authentification dans le Cloud

3.2.1. Nom d'utilisateur / Mot de passe

Mécanisme qui se base sur le partage d'un secret commun entre le Demandeur (utilisateur) et le Vérificateur (CSP). L'authentification réussit si les informations d'identification et le secret fourni par le Demandeur correspondent à ceux du Vérificateur. Dans cette méthode d'authentification, l'utilisateur doit introduire un nom d'utilisateur et un mot de passe pour se connecter au système Cloud et accéder aux services du CSP. Par unanimité, il est admis que le mécanisme de nom d'utilisateur / mot de passe est un mécanisme d'authentification qui n'est pas très sûr, car il est difficile de confirmer que la demande provient du propriétaire légitime de ces informations. En outre, les utilisateurs choisissent des mots de passe faciles et même le meilleur mot de passe peut être volé ou deviné via les attaques de dictionnaire et par brute force **[38, 39]**, le sniffing du réseau, le rejeu, l'attaque man-in-the-middle et l'ingénierie sociale. Dans le Cloud, il y a l'emploi de mots de passe courts et de gestionnaires de mots de passe à la place de mots de passe complexes qui sont difficiles à retenir pour les utilisateurs. De plus, les utilisateurs réutilisent leurs mots de passe pour l'authentification dans différents serveurs et utilisent des mots de passe faibles qui ne font qu'augmenter les risques de sécurité. Les caractéristiques de cette méthode d'authentification peuvent être énumérées comme suit: **[40]**

- Facile à utiliser et à implémenter.
- Pratique et ne nécessite pas de configuration particulière.
- Ne requiert aucun équipement spécial.
- Possibilité de perte ou d'oubli du secret.
- La sécurité se base sur la force du mot de passe.
- Familière avec beaucoup d'utilisateurs.
- Possède un certain niveau de complication quant au renouvèlement régulier des informations d'identification.

L'augmentation de la force du mot de passe est une solution pour éviter les attaques, étant donné que la longueur du mot de passe détermine le niveau de sécurité qu'il procure. Les gestionnaires de mots de passe est l'une des solutions les plus courantes permettant d'atténuer ces problèmes de sécurité. En général, les gestionnaires de mots de passe fonctionnent en sauvegardant les mots de passe introduits en ligne et, plus tard, faire l'auto-remplissage des formulaires de connexion. Par conséquent, le bénéfice et la raison principale derrière la conception de nombreux gestionnaires de mots de passe est que les utilisateurs ne doivent plus s'en souvenir. Les auteurs dans **[39]** et **[41]**, ont présenté des protocoles qui peuvent permettre à un utilisateur d'utiliser un mot de passe unique pour s'authentifier dans de multiples services et en toute sécurité. Ces protocoles aident à protéger les utilisateurs contre les attaques Cross-Site Scripting, par dictionnaire, le phishing et les logiciels malveillants. De plus, pour augmenter la sécurité, les mots de passe à usage unique sont recommandés à être utilisés plutôt que ceux statiques.

- **Mots de passe statique**

Les mots de passe statiques sont la forme la plus ancienne et la plus répandue comme informations d'identification des utilisateurs. Ce sont des secrets partagés entre l'utilisateur et le serveur d'authentification qui ne changent pas souvent. Le serveur d'authentification stocke le mot de passe statique dans sa base de données, où il doit être solidement protégé. Pratiquement, n'importe quelle application, plate-forme, ou système d'exploitation peut prendre en charge cette authentification. Leur inconvénient majeur est qu'ils peuvent être une cible facile pour les attaquants. Contrairement aux humains ou de nombreux facteurs les influent lors du processus de prise de décision, les machines se comportent toujours exactement de la même manière prévisible. Les ordinateurs peuvent utiliser la date courante et l'heure, ou le contenu d'une cellule mémoire, pour générer un mot de passe. Cependant, aucun de ceux-ci n'est certainement aléatoire. Quelqu'un qui possède des connaissances de l'environnement peut deviner le mot de passe pseudo-aléatoire. Les mots de passe statiques forment une méthode d'authentification commune très répandue, largement soutenue et pratique, mais fournit de faibles niveaux de sécurité. **[42]**

- **Mots de passe à usage unique OTP « O**ne **T**ime **P**assword **»**

Les mots de passe à usage unique sont des secrets qui peuvent être utilisés pour s'authentifier uniquement une fois ou un certain nombre de fois. Techniquement, cela signifie que l'utilisateur doit avoir un nouveau mot de passe à chaque fois qu'il aura besoin de s'authentifier. La génération des mots de passe à usage unique nécessite un logiciel spécial ou un matériel du côté du serveur d'authentification et du côté de l'utilisateur. Une des approches possibles est d'avoir une liste de mots de passe et une stipulation que chacun de ses mots de passe sera utilisé uniquement une fois. Ce mécanisme assez simple n'a pas trouvé beaucoup de soutient. Les mots de passe à usage unique sont générés par un algorithme. Ils sont différents des mots de passe typiques, car ils ne se répètent pas.

L'algorithme de génération utilise un secret sous-jacent. Ce secret est partagé entre le Demandeur et le Vérificateur. Au cours du processus d'authentification, le Demandeur et le Vérificateur génèrent chacun le mot de passe à usage unique. L'utilisateur envoie le mot de passe à usage unique au Vérificateur qui le compare avec celui généré en local. Le Demandeur est donc authentifié si les deux mots de passe correspondent. Les OTPs peuvent être distribués par logiciel, matériel et même sous forme de papier. Cette technologie ouvre de nouvelles opportunités pour les solutions d'authentification à deux facteurs notamment dans les environnements de Cloud Computing. Le RSA SecurID[6] est un exemple de mécanisme de mot de passe à usage unique. **[42]**

3.2.2. MTM « **M**obile **T**rusted **M**odule »

Standard proposé par le TCG « **T**rusted **C**omputing **G**roup » dont : Nokia, Samsung, France Télécom, Ericsson, y font partie. Ce dernier a présenté un ensemble de spécifications de sécurité pour mesurer et préserver l'intégrité des logiciels à travers un matériel-de-confiance. C'est principalement appliqué pour authentifier les terminaux de télécommunication et accomplir des fonctions de sécurité, telles que les fonctions de hachage, les schémas de signature, ainsi que le chiffrement asymétrique. Cependant, il a été considéré comme une méthode d'authentification de Cloud Computing avec SIM « **S**ubscriber **I**dentity **M**odule », en raison de la généralisation des smartphones.

3.2.3. Infrastructure à clé publique

Le système traditionnel d'authentification basé sur la clé secrète supporte principalement le déploiement des algorithmes cryptographiques asymétriques, tel que le RSA. Il utilise une clé privée pour prouver l'identité de l'utilisateur. Le PKI à son tour, a été utilisé dans la conception des protocoles de sécurité tels que **S**ecure **S**ocket **L**ayer (SSL / TLS) et **S**ecure **E**lectronic **T**ransaction (SET), dont l'objectif principal est de fournir l'authentification sur la base d'un certificat, sans avoir à partager une information secrète. Le succès du PKI, comme un autre type de système cryptographique, dépend du contrôle des accès aux clés privées. Ce mécanisme doit fournir la confidentialité et l'intégrité des données, la non-répudiation, une forte authentification ainsi que l'autorisation.
Les auteurs dans **[43]** proposent d'assurer les caractéristiques de sécurité de l'environnement Cloud en utilisant une combinaison de PKI, SSO, des techniques cryptographiques ainsi que le LDAP pour garantir l'authentification, l'intégrité et la confidentialité des données et des communications. Le principal avantage du PKI est de fournir aux utilisateurs une authentification dans les systèmes répartis comme le Cloud, le Cloud mobile et les réseaux de capteurs sans fil. C'est la source de beaucoup de progrès réalisés dans l'évolution des solutions de sécurité pour l'authentification, l'autorisation, la confidentialité, l'intégrité et la comptabilisation **[44]**.

3.2.4. SSO

Le **S**ingle **S**ign **O**n est un système de gestion d'identité, qui peut authentifier l'utilisateur une fois vis-à-vis d'une seule autorité d'authentification. Il permet à l'utilisateur par la suite d'accéder à d'autres ressources confinées sans se ré-authentifier. SSO est donc un moyen d'accès à de multiples applications indépendantes de manière à ce que les utilisateurs se connectent et gagnent l'accès sans se ré-identifier pour chaque application.

[6] RSA SecurID : Mécanisme d'authentification par mot de passe à usage unique développé par RSA Security.

Cette méthode permettant aux utilisateurs d'accéder à plusieurs services, améliore l'efficacité, en empêchant l'utilisateur de se rappeler de nombreux mots de passe.
Le SSO permet de diminuer le temps de la saisie des mots de passe différents lors de l'ouverture des sessions. En outre, il permet de contrôler les droits des utilisateurs. Les avantages du SSO sont:

- Réduire le nombre de nom d'utilisateur / mot de passe et donc leur gestion.
- Accroître la sécurité du système.
- Aider l'administrateur en contrôlant une information d'identification unique au lieu de plusieurs.
- Accroître la productivité de l'organisation.

3.2.5. Authentification biométrique

L'authentification biométrique maintient trois facteurs importants de la sécurité de l'information, à savoir : l'authentification, l'identification et la non-répudiation. Ce mécanisme est basé sur l'identification physiologique de l'individu vivant ou sur des attributs comportementaux. En outre, les objectifs de l'authentification biométrique sont la sécurité, le coût, la vitesse de calcul, la précision, l'acceptation de l'utilisateur et les contraintes de l'environnement. L'authentification biométrique présente certains avantages :

- Extrêmement difficile à copier, à partager et à distribuer.
- Exige que la personne soit présente pour s'authentifier.
- Difficile à forger (nécessite plus de temps, de coût, de l'expérience et des privilèges d'accès).

Par conséquent, l'authentification biométrique est un mécanisme approprié pour remplacer l'authentification traditionnelle basée sur des clés cryptographiques PKI, authentification par nom d'utilisateur / mot de passe. Cependant, toutes ces techniques biométriques ont leurs propres avantages et inconvénients de par leur acceptation par les utilisateurs, le coût et la performance. Les systèmes biométriques sont généralement des systèmes d'authentification statique. Dans une authentification statique, l'identité de la personne est vérifiée au début de la session, en utilisant par exemple une empreinte digitale, pour obtenir l'accès à un ordinateur ou à l'aide d'une analyse de l'iris pour obtenir un accès à une pièce. Deux vulnérabilités majeures qui nécessitent plus d'attention sont présentes dans le contexte de la biométrie qui sont : "l'attaque spoof" du côté de l'interface utilisateur, ainsi que "les fuites dans la base de données". Une attaque spoof consiste à présenter une imitation de la caractéristique biométrique. Les fuites dans la base de données impliquent que la caractéristique biométrique d'un utilisateur tombe entre les mains d'un adversaire.

3.2.6. Authentification forte / multi-facteurs

L'authentification traditionnelle par mot de passe ne fournit pas suffisamment de sécurité dans les environnements Cloud contre la plupart des attaques. Il y a eu alors la nécessité d'introduire un système plus sécurisé employant une authentification multi-facteurs, qui doit vérifier une paire : nom d'utilisateur / mot de passe, mais doit également employer un deuxième facteur comme l'authentification biométrique, etc. Toutefois, la faisabilité de l'authentification à deux facteurs est limitée par la complexité du déploiement et du coût élevé. Cette technique utilise une combinaison entre les trois facteurs d'authentification (connaissance, possession ou caractéristiques personnelles). C'est une technique solide d'identification de l'utilisateur, en effet, la confiance d'authenticité augmente de façon exponentielle, lorsque plusieurs facteurs sont impliqués dans le processus de vérification. Cette méthode accroît l'intensité de la sécurité.

Le choix de la méthode d'authentification appropriée dans un Cloud dépend principalement du type d'entités, du modèle de déploiement public, privé ou hybride ainsi que du degré de confiance des entités.

3.3. Solutions industrielles d'authentification dans le Cloud

3.3.1. Principe de l'identité fédérée

L'authentification et la gestion des identités sont assez complexes. Divers types de services nécessitent l'utilisation d'un ou de plusieurs mécanismes d'authentification, comme le montre la figure 2.6. Le fait que les mécanismes d'authentification soient généralement fournis dans la base des services (i.e. : un ensemble d'informations d'identification pour chaque service spécifique), augmente la complexité apportée à cette situation. **[47]**

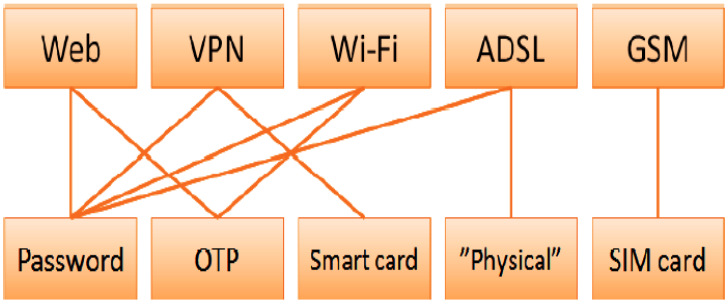


Figure 2.6 Authentification et gestion des identités: gestion de plusieurs identités

En utilisant *les Frameworks de gestion des identités*, le premier avantage supplémentaire offert par ces solutions de gestion des identités est qu'ils ne soient pas dans cette situation et permettent, par la même occasion, à plusieurs Services Providers d'utiliser des mécanismes d'authentification plus avancés et plus sûrs. Le deuxième avantage est que plusieurs services, fournis par le même Services Provider ou différents Services Provider, peuvent permettre une authentification unique « **S**ingle **S**ign **O**n » à l'utilisateur où il pourra se déplacer entre certains Services Providers sans se ré-authentifier. Ceci est illustré dans la figure 2.7, où plusieurs services sur le World-Wide-Web (WSn) ont accès à des mécanismes d'authentification communs, grâce à l'utilisation d'un Framework de gestion d'identité.

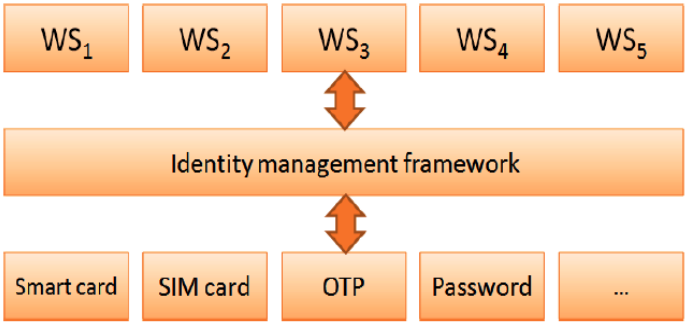


Figure 2.7 Utilisation de la même authentification

Pour résumer, l'utilisateur devait s'authentifier à chaque fois pour accéder à une ressource, la question qui se pose dans ce cas : combien de mots de passe différents ou d'une manière générale, d'informations d'identifications différentes doit-il retenir, ou plutôt, doit-il retenir un mot de passe unique pour toutes ses applications ?

Des solutions d'identités fédérées ont été alors proposées, offrant la possibilité d'accéder à diverses ressources du Cloud en utilisant une seule fois l'étape d'authentification. Elles s'appuient sur des protocoles standards d'identité (SAML, OpenID, WSFed).
La solution de l'identité fédérée met en œuvre des outils automatisés qui permettent d'importer les comptes utilisateurs. En conséquence, avec une seule requête d'authentification via une interface, l'utilisateur peut accéder à toutes les applications en mode SaaS (Office, Salesforce,...). Les applications les plus familières de ces normes sont présentent dans les services SaaS comme Google et Facebook. Ces normes ont aussi souvent un rôle implicite dans plusieurs domaines techniques.

Cependant, le Cloud en permettant d'avoir un service d'authentification réutilisable chez plusieurs Providers, cette option peut s'avérer contraignante du côté des utilisateurs désirant préserver au mieux leur privacy dans le Cloud.

Les normes industrielles « Open Standards » pour la gestion des identités centralisées et fédérées, dans les environnements Cloud, seront présentées dans les deux sections suivantes: **[47]**

3.3.2. Frameworks d'Authentification et d'Autorisation

- **OATH «Open Authentication»**

  OATH est une initiative pour l'authentification ouverte, une collaboration à grande échelle ayant pour but le développement d'une architecture de référence utilisant des normes ouvertes, afin de promouvoir l'adoption de l'authentification forte. OATH propose des normes pour une variété de technologies d'authentification, cherchant à offrir une utilisation simplifiée et à coût inférieur. OATH fournit donc une feuille de route et des spécifications ouvertes pour l'industrie afin d'opter pour les mécanismes d'authentification forte. Voici trois exemples majeurs des méthodes d'authentification proposées dans OATH:
  • Authentification basée sur un module d'identité d'abonné SIM «**S**ubscriber **I**dentity **M**odule» en utilisant les réseaux GSM / GPRS SIM.
  • Authentification fondée sur une infrastructure à clé publique PKI, en utilisant les certificats X.509.
  • Les mots de passe à usage unique OTP «One Time Password».

  OATH représente un effort de collaboration des leaders de l'industrie informatique visant à fournir une architecture de référence pour une authentification forte et universelle, entre tous les utilisateurs et tous les périphériques sur tous les réseaux.

- **OAuth «Open Authorization»**

  OAuth est un protocole ouvert, qui permet le partage du contexte de sécurité sans la nécessité de partager une identité / informations d'identification. Par exemple, les utilisateurs peuvent partager des ressources privées telles que des contacts, photos et vidéos stockées chez un CSP avec un autre, sans avoir à introduire leur nom d'utilisateur / mot de passe. OAuth est complémentaire à OpenID (voir section Frameworks de gestion des identités), sauf que c'est un service séparé. OAuth a été créé après une étude menée sur d'autres protocoles propriétaires tels que Google AuthSub, AOL OpenAuth, Yahoo BBAuth, API Flick, dont chacun fournit un procédé

d'échange des informations d'identification de l'utilisateur, par le biais d'un jeton d'accès, afin de fournir une alternative d'accès ouvert. OAuth n'est pas un protocole d'authentification, mais plutôt de délégation d'autorisation.
OAuth définit trois rôles : le client, le serveur et le propriétaire de ressources. Ces rôles sont présents dans toute transaction OAuth. Dans certains cas, le client est aussi le propriétaire de la ressource. Les propriétaires de la ressource accordent l'accès à une ressource protégée sur un seul site (serveur) à un autre site (client). Une ressource protégée est une ressource stockée sur le serveur, qui requiert une authentification afin d'y accéder. Cette ressource est contrôlée par son propriétaire. Toute personne demandant l'accès à une ressource protégée doit être autorisée par le propriétaire des ressources.

- **RADIUS**

RADIUS pour « **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice » est un protocole réseau qui fournit l'authentification centralisée, l'autorisation et la comptabilisation assurant la journalisation des accès et la facturation. RADIUS est un protocole dénommé AAA: Authentication/Authorization/Accounting. Les principales fonctions de RADIUS sont d'authentifier les utilisateurs avant de leur accorder l'accès à un réseau, d'autoriser ces utilisateurs à accéder à certains services du réseau et de comptabiliser l'utilisation de ces services.
Diameter est le successeur de RADIUS. Il étend le protocole de base en ajoutant de nouvelles commandes / attributs, tels que ceux pour l'utilisation du protocole EAP «**E**xtensible **A**uthentication **P**rotocol».

- **Kerberos**

Kerberos est un protocole d'authentification utilisé afin d'authentifier des clients vis-à-vis d'un serveur dans une architecture client-serveur. Le Cloud Computing peut également être vu comme une architecture client-serveur distribuée, où le CSP représente le serveur et les utilisateurs Cloud les clients. Ces entités communiquent généralement par le moyen d'un intermédiaire, nommé le Cloud Broker. **[46]**
L'objectif de Kerberos est la mise en place de serveurs d'authentification (AS : Authentication Server) pour permettre d'identifier des utilisateurs distants et des serveurs qui délivrent des tickets de service (TGS : Ticket Granting System), afin de les autoriser à accéder à des services réseaux. La plupart du temps, les deux types de services sont regroupés sur un même serveur, appelé Centre de Distribution de Clés (KDC : Key Distribution Center).

3.3.3. Frameworks de gestion des identités: IAM «**I**dentity **A**ccess **M**anagement»

- **Initiative SSO « S**ingle **S**ign **O**n»

Le SSO désigne les technologies permettant aux utilisateurs de mutualiser la phase d'authentification entre plusieurs services. Concrètement, il s'agit de ne solliciter le processus d'authentification qu'une seule fois et leur permettre d'accéder à de multiples applications. C'est un processus nécessitant une authentification unique, en introduisant les informations d'identification une seule fois.

L''utilisateur va donc s'authentifier d'abord vis-à-vis d'une autorité d'authentification de confiance et aura ensuite l'accès à toutes les applications de cette autorité. Les applications ne reçoivent que des informations leurs permettant de savoir si elles peuvent autoriser l'accès à l'utilisateur ou non.
Puisque l'utilisateur s'authentifie une seule fois, l'exposition de ses informations sensibles sur le réseau est limitée. Un avantage supplémentaire est que les systèmes SSO redirigent souvent les utilisateurs vers des canaux de communication sécurisés. Les systèmes SSO conservent généralement l'état de l'utilisateur pour une certaine période de temps, de sorte que ce dernier puisse accéder à plusieurs reprises aux applications sans s'authentifier à chaque fois. Dans le Cloud, le SSO est une extension du Web SSO existant dans les applications sur site, à titre d'exemple, l'authentification Google est partagée entre les différents services Gmail, YouTube, Google Apps etc. Dans ce mode, Google est le fournisseur d'identité (IdP) pour ses propres services. Cette initiative est une coopération réalisée entre Microsoft et Sun.

Figure 2.8 Accès à de multiples services via le SSO

- **Oasis SAML et Shibboleth**

SAML pour **« S**ecurity **A**ssertion **M**arkup **L**anguage » est un standard basé sur le langage XML qui assure l'échange des données d'authentification et d'autorisation entre les domaines de sécurité, plus précisément, entre un fournisseur d'identités « Identity Provider » : producteur d'assertions et un fournisseur de services « Service Provider » : consommateur d'assertions. SAML a été créé par OASIS, sa mission principale est de résoudre les problèmes du Web SSO. Shibboleth est une architecture et une implémentation open-source pour la mise en œuvre de l'authentification basée sur l'identité fédérée ainsi que l'autorisation. Cette architecture se base sur le langage SAML, utilisée pour accomplir le Web SSO. Shibboleth est constitué de deux parties:
• Identity Provider : Software géré par une organisation comportant des utilisateurs qui souhaitent accéder à un service restreint.
• Service Provider : Software géré par le prestataire qui gère le service restreint.

- **OpenID**

OpenID est un standard ouvert, décentralisé pour l'authentification et le contrôle d'accès. Il permet aux utilisateurs de se connecter à de nombreux services avec la même identité numérique, tel le cas de l'utilisateur SSO avec des services supportant l'OpenID. En tant que tel, il remplace le processus d'ouverture de session commune qui utilise un nom d'utilisateur et un mot de passe, en permettant à un utilisateur de se connecter une fois et d'avoir accès aux ressources de multiples systèmes. OpenID est principalement disponible sur les services offerts par les compagnies de l'Internet. L'adoption de l'OpenID pour une utilisation en entreprise est presque inexistante en raison du problème de confiance.

Certains chercheurs ont révélé que l'OpenID pourrait accentuer les attaques de phishing qui peuvent conduire à compromettre les informations d'identification des utilisateurs.
L'OpenID se base sur des technologies existantes (URI, HTTP, SSL, Diffie-Hellman) et permet aux utilisateurs de créer leurs identités eux-mêmes, que ce soit pour leur blog, flux de photos, page de profil, etc. Avec OpenID, ils peuvent facilement transformer une de ces URI existante sur un compte qui peut ensuite être utilisée dans des sites qui supportent les connexions OpenID. Les identités dans OpenID sont des URIs, à savoir, une courte chaîne de caractères identifiant une ressource sur un réseau. Parmi les avantages d'utiliser les URIs, c'est le fait qu'elles soient relativement simples, elles sont omniprésentes (utilisation fréquente) et faciles à retenir. Le processus d'authentification dans la pratique implique de vérifier que l'utilisateur possède une certaine URI.

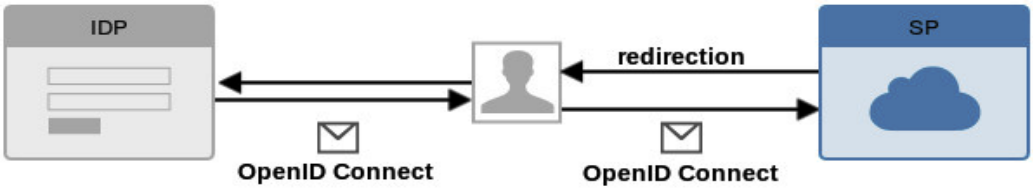


Figure 2.9 Principe de l'OpenID

4. L'Authentification anonyme dans le Cloud Computing

4.1. Aperçu et définition

Selon **[48]** « *L'Authentification Anonyme semble être un oxymore car l'Authentification représente le moyen de prouver l'identité de quelqu'un vis-à-vis d'une autre partie, tandis que le but de l'Anonymat est de cacher l'identité de quelqu'un* ».

Cependant, l'authentification anonyme réalise ces objectifs contradictoires en demandant par exemple aux utilisateurs de prouver uniquement l'appartenance à un groupe de telle sorte que l'identité de l'utilisateur ne peut pas être déterminée par le Vérificateur : Partie qui réalise la vérification (*généralement c'est le Service Provider dans le cas du Cloud Computing*).

Si U est l'ensemble des utilisateurs autorisés à être authentifiés auprès d'un vérificateur V, ce dernier devra accepter toute demande d'authentification d'un utilisateur légitime $u_i \in U$. Même si V est malhonnête, il ne doit pas être en mesure de savoir quel utilisateur particulier a effectivement réalisé la preuve.

Ceci étant les principes de base de l'authentification anonyme. Cette dernière s'accomplit mieux avec les conditions suivantes:

- **L'Anonymat** « Anonymity » : Le vérificateur « The Verifier », peu importe qu'il y ait une fraude ou non, ne doit pas avoir les moyens d'identifier un demandeur d'authentification : le Prouveur « The Prover » ⇔ Anonymat Complet. Cette condition peut être décontractée, la probabilité d'identification peut être légèrement supérieure ⇔ Anonymat Probabiliste. De plus, le Prouveur devrait être en mesure de choisir le degré d'anonymat (la taille de l'ensemble d'anonymat U'), i.e. : chaque authentification unique est indépendante des authentifications antérieures ⇔ Anonymat Adaptatif.

- **Exactitude** « Correctness » : Un Prouveur honnête (Membre de l'ensemble des Prouveurs autorisés) doit toujours effectuer son authentification de façon anonyme.

- **Inforgeabilité «** Unforgeability **»** : Toute partie qui n'appartient pas à l'ensemble des utilisateurs autorisés ne doit pas être en mesure d'exécuter un protocole d'authentification anonyme avec le Vérificateur, de telle sorte que le Vérificateur l'accepte. Cela inclut des ensembles arbitraires d'utilisateurs révoqués.

- **Non chaînabilité ou Inassociabilité** « Unlinkability » : Les Vérificateurs ne doivent pas être en mesure de relier les exécutions du protocole d'authentification anonyme à un autre, si elles ont été réalisées par le même Prouveur inconnu

- **Traçabilité** «Traceability » : Il peut être nécessaire qu'un tiers de confiance «Trust Third Party» soit en mesure de révoquer l'anonymat d'un ensemble d'utilisateurs en question, étant donné la transcription du protocole d'authentification anonyme.

- **Pas de fausse attribution** « No misattribution » : Les protocoles d'authentification anonyme devraient fournir des mécanismes de telle sorte que les Prouveurs peuvent signaler de manière plausible les Vérificateurs en fraude. D'un autre côté, ils ne peuvent pas accuser des Vérificateurs honnêtes de fraude.

- **Retrait d'adhésion** « Membership withdrawal » : Les protocoles d'authentification anonyme doivent fournir des mécanismes efficaces pour exclure des utilisateurs de l'ensemble des utilisateurs autorisés.

4.2. Mécanismes d'authentification anonyme

Comme l'authentification repose généralement sur des secrets : tels que les mots de passe, il est courant de mesurer sa qualité par la difficulté de deviner le secret d'authentification. Cette difficulté est mesurée en termes *d'entropie* : une mesure statistique de l'incertitude. Étant donné que les éléments sont sélectionnés au hasard à partir d'un ensemble
$X = \{X_1, . . ., X_n\}$ avec des probabilités $p_1, . . ., p_n$, l'entropie h: c'est à dire, l'incertitude à propos de quel élément est choisi, est calculée comme suit :

$$h := -\sum_{i=0}^{n} p_i \log p_i$$

Avec la convention que $0 \cdot \log 0 := 0$. Son unité est généralement bits si le logarithme est base-2. Une entropie de h bits signifie un besoin moyen de deviner correctement h bits pour découvrir le secret (complet). Par ailleurs, si un secret de n bits possède $h < n$ bits d'entropie, alors les n-h bits peuvent uniquement être dérivés des h bits connus.

Les techniques traditionnelles d'authentification peuvent être utilisées pour garantir un certain niveau d'anonymat. Dans cette section, divers mécanismes pour réaliser l'authentification anonyme seront présentés. Ils peuvent généralement être divisés en deux classes:

- La première classe couvre les protocoles d'authentification anonymes, qui requièrent aux utilisateurs de se rappeler d'un secret à faible entropie relativement court: comme un mot de passe mémorable. Ces techniques sont appelées protocoles d'authentification anonymes par mot de passe, ou plus généralement, **A**nonymous **P**assword-based **A**uthenticated **k**ey **E**xchange **« APAKE »**.

- La deuxième couvre les protocoles d'authentification anonymes, qui requièrent aux utilisateurs de se rappeler d'un secret à forte entropie relativement long (comme une clé secrète).

4.2.1. Authentification anonyme par mot de passe

C'est l'authentification anonyme qui utilise seulement une chaîne de caractère à faible entropie, afin de prouver qu'un individu actif appartient à un groupe d'utilisateurs autorisés, sans révéler son identité.

Avec cette technique, les utilisateurs peuvent accéder anonymement aux ressources du Cloud, la machine de l'utilisateur a besoin seulement de se souvenir d'un mot de passe.

Cette technique, proposée dans **[49]** et formalisée plus tard dans **[50]**, est une méthode populaire d'authentification dans un environnement où l'utilisateur et le serveur partagent un secret court à faible entropie (mot de passe). Cette technique a connu un intérêt considérable et, à partir de **[51]**, de tels protocoles ont également été considérés dans le cadre de l'authentification anonyme via des mots de passe courts. Cependant, le secret peut être deviné, par exemple, via des attaques de dictionnaire divisées en attaques online et offline. Dans le cas online, l'adversaire a besoin de l'assistance du serveur, c'est à dire, il s'engage dans le protocole d'authentification avec le serveur en utilisant un mot de passe deviné. La contre mesure côté serveur est le verrouillage des comptes après un certain nombre de tentatives d'authentification consécutives échouées dans le cadre traditionnel. Dans le cas de l'authentification anonyme par contre (surtout quand la non chaînabililité est souhaitée) de telles attaques sont inévitables. Dans le scénario d'attaque offline, l'adversaire tente d'extraire ou de deviner le mot de passe en se basant sur les transcriptions des exécutions du protocole d'authentification, sans interaction avec le serveur. Par conséquent, les protocoles d'authentification anonymes par mot de passe doivent être conçus d'une manière à ce que les attaques offlines par dictionnaire ne soient pas efficacement réalisables.
De ce fait, un protocole d'authentification anonyme a été proposé dans **[34]**, où un utilisateur se sert de son identité en tant qu'indice pour récupérer le mot de passe correspondant stocké dans le serveur. Les mots de passe stockés dans le serveur sont organisés sous forme de matrice. L'indice de l'identité envoyé par l'utilisateur ainsi que les données récupérées sont chiffrés (à savoir le mot de passe correspondant est sous forme chiffrée). Le serveur ajoute une valeur aléatoire aux données récupérées avant de les envoyer à l'utilisateur. Ainsi, seul un utilisateur valide peut utiliser son mot de passe et la valeur aléatoire est nécessaire pour le calcul d'une clé de session Diffie-Hellman.

Le problème général de toute authentification par mots de passe est que le serveur hébergeant les secrets (mots de passe), ou une valeur dérivée d'eux (une valeur de hash du mot de passe) est une entité centralisée. Par conséquent, ce serveur est la cible la plus précieuse pour les attaquants.

4.2.2. Authentification anonyme via PKE « **P**ublic **k**ey **E**ncryption»

C'est l'authentification anonyme qui utilise seulement le chiffrement à clé publique comme une boîte noire, afin de prouver qu'un individu actif appartient à un groupe d'utilisateurs autorisés, sans révéler son identité.

Grace à cette technique, les utilisateurs Cloud peuvent accéder anonymement aux ressources, la machine de l'utilisateur a besoin seulement d'être dotée d'un mécanisme classique de chiffrement à clé publique.

Puisqu'il existe des protocoles d'authentification challenge-réponse bien connus basés sur le chiffrement à clé publique (par exemple, le protocole Needham-Schroeder-Lowe), il est naturel de se demander s'il est également possible de construire une authentification anonyme en utilisant ces protocoles comme éléments de base. L'idée est la suivante:
Soit U un groupe de n utilisateurs, dont les clés publiques sont PK_1,..., PK_n authentiquement connues par un serveur S (le Vérificateur).
Si un membre u ∈ U (Un Prouveur) souhaite s'authentifier anonymement, alors S sélectionne un challenge aléatoire r et chiffre r avec toutes les clés publiques et envoie les textes chiffrés C_1, . . ., C_n à u. Le Prouveur u déchiffre le texte chiffré se référant à sa propre clé publique PK_i et répond avec la valeur correcte de r. Puisque S ne peut pas déterminer quel texte chiffré a été déchiffré, le Prouveur u reste anonyme.

Dans ce schéma, il est également important que l'anonymat ne soit valable que si le Vérificateur utilise le même challenge r pour chaque texte chiffré. Si le serveur S chiffre des challenges différents pour chaque utilisateur, alors l'identité de u est trivialement découverte.

4.2.3. Signature de groupe « Groupe signature »

Ce sont des signatures numériques qui lient une signature à un groupe de signataires potentiels, plutôt qu'à un individu. Le but est de créer une signature numérique dont la vérification ne révèle rien, sauf le fait qu'un message / document ait été signé par une personne appartenant à un groupe spécifique, tant dis que le signataire réel ne peut être identifié.
La signature de Groupe dans le Cloud permet à chaque utilisateur de soumettre ses informations d'identification au nom d'un groupe, sans montrer son identité au CSP. Les utilisateurs peuvent ainsi s'authentifier de façon anonyme vis-à-vis du CSP.

Les protocoles d'authentification challenge-réponse basés sur les signatures anonymes permettent à tout utilisateur U_i d'un groupe U = {U_1, . . ., U_n} de produire une signature au nom du groupe U, de telle sorte que toute personne qui vérifie la signature soit incapable d'identifier le signataire. Par conséquent, le Vérificateur apprend uniquement que quelqu'un appartenant à l'ensemble U a produit la signature, mais ne sait pas exactement qui.
Le concept de signature de groupe a été introduit par Chaum et Van Heyst dans **[52]**. Dans ce type de signatures, il existe une partie désignée gestionnaire de groupe GM: Group Manager, qui est responsable de gérer le groupe des utilisateurs c'est à dire, les utilisateurs ont besoin d'exécuter un protocole de join avec GM afin de se joindre au groupe, GM quant à lui, est responsable de révoquer les utilisateurs. En outre, GM est en mesure d'ouvrir une signature c'est à dire, de révéler l'identité du membre du groupe qui a anonymement signé un message. Chaque membre du groupe peut émettre anonymement des signatures pour des messages arbitraires au nom du groupe, tandis que GM est en possession de certaines informations de trappe, lui permettant de révéler l'identité du membre du groupe qui a signé anonymement un message en cas de suspicion. Chaque partie en possession de la clé de vérification publique du groupe est en mesure de vérifier qu'une signature pour un message donné est valide et d'être convaincue que quelqu'un des membres du groupe a émis la signature, sans être en mesure d'identifier un signataire particulier.

4.2.4. Signature en aveugle « Blind signature »

La Signature en aveugle est une méthode dont l'objectif est d'obtenir l'autorisation d'accès pour consommer anonymement des services. Le but étant de fournir des tickets anonymes en usage unique ou en multi-usages.

Dans le contexte Cloud, cette méthode va permettre aux utilisateurs d'effectuer des requêtes anonymes lors de la consommation des services vis-à-vis du CSP. Les signatures en aveugle peuvent être utilisées pour autoriser une transaction via un ticket. Le ticket lui-même est signé numériquement par le Provider. L'aveuglement « The blinding » assure que le Provider ne peut pas reconnaître les tickets pour établir des profils sur ses utilisateurs ou les lier à une identité.

L'idée générale est que certaines parties (le CSP ou une entité de confiance) émettent des jetons (également appelés informations d'identification ou tickets) aux utilisateurs afin d'être utilisés pour consommer les services de manière anonyme. Habituellement, il est souhaitable que : l'émission et l'usage d'un jeton assurent la non chaînabilité et que le jeton ne révèle aucune information sur son propriétaire (anonymat).
En parlant du nombre d'usage, certains systèmes sont conçus pour un usage unique des jetons et d'autres pour offrir des jetons en multi-usages. Ce dernier cas peut être réalisé par un nombre illimité où un entier k, c'est à dire, l'utilisateur est capable de montrer un jeton au plus k fois d'une façon anonyme et non chaînable. Le montrer à la k + 1 fois permet la traçabilité de l'utilisateur.
La signature en aveugle est un concept introduit par David Chaum en 1983 **[53]**. Une signature en aveugle « Blind signature » est une signature numérique dans laquelle, le signataire ne voit pas le document qu'il signe numériquement. Contrairement à une signature conventionnelle qui est créé par une seule entité, une signature en aveugle est un processus interactif entre deux parties, à savoir *le Propriétaire du document* et *le Signataire.*

Soit m le document à signer, ou plus précisément sa valeur de hash (pour contrecarrer toute falsification existentielle). Une simple construction d'une signature en aveugle est basée sur le système RSA:

1- Soit **p, q** deux grands nombres premiers appelés Facteurs premiers RSA.
2- n = p · q appelé le Modulo RSA.
3- φ (n) = (p-1). (q-1) appelée l'indicatrice d'Euler: fonction arithmétique de la théorie des nombres, qui à tout entier naturel n non nul associe le nombre d'entiers compris entre 1 et n et premiers avec n.
4- e, **d** deux entiers appelés respectivement exposant RSA public et exposant RSA privé, satisfaisant : e · d ≡ 1 (mod φ (n)).
e est choisi tel que : 1< e < φ (n) et **e** est premier avec φ (n) tandis que **d=** e^{-1} (mod φ (n)).
5- Pk = (n, **e**) est la clé publique du signataire. Elle est authentiquement connue par le propriétaire du document à signer.
6- SK= (n, **d**) la clé privée du signataire.

Une signature en aveugle pour un document m peut être obtenue comme suit:
1. Le propriétaire du document sélectionne un nombre entier aléatoire **r** premier avec **n** et calcule le message aveuglé $\tilde{\mathbf{m}}$ = H(m) · r^e (MOD n), où H est une fonction de hachage cryptographique sécurisée utilisée pour contrecarrer la falsification existentielle. Il transmet le message aveuglé au signataire.

2. Le signataire calcule la signature numérique pour $\tilde{\mathbf{m}}$ comme d'habitude: **S'** = $\tilde{m}^{d}$ (MOD n) noter que: $\tilde{m}^{d} \equiv (H(m) \cdot r^{e})^{d} \equiv H(m)^{d} \, r^{ed} \equiv H(m)^{d} \cdot r$ (MOD n).
Etant donné que r est inconnu du signataire et choisi au hasard, le document original m reste parfaitement secret.
3. Le propriétaire reçoit S' = $H(m)^{d} \cdot r$ (MOD n) et peut le multiplier par r^{-1}. La signature résultant **S**= **S'** $\cdot \; r^{-1} = H(m)^{d}$ (MOD n) est alors valide pour le document m.

Par analogie, considérons qu'une entité «A» possède une lettre qui doit être signée par une autorité «B», mais A ne veut pas révéler le contenu de sa lettre à l'autorité B. A peut placer la lettre dans une enveloppe couverte de papier carbone et l'envoyer à B. B va signer l'extérieur de l'enveloppe de carbone sans l'ouvrir, puis la renvoyer à A. A peut alors l'ouvrir pour trouver sa lettre qui a été signée par B, mais sans que B n'est pu visualiser son contenu. **[53]**

4.3. Anonymat et approches d'authentification dans le Cloud

4.3.1. Anonymat et Authentification dans les environnements classiques

L'anonymat a été souvent considéré comme un moyen idéal pour assurer la privacy des utilisateurs. Cependant, la majorité des protocoles n'offrent pas la notion d'anonymat. L'attaque possible dans de tels protocoles est la présence d'un sniffer réseau situé sur la route des messages. L'adversaire a seulement besoin de lire les messages interceptés pour connaître l'émetteur et le destinataire d'un message. L'anonymat des systèmes « source rewriting systems » englobe les Mixs de chaum **[96]** et l'Onion Routing **[55]** qui assure que les messages soient envoyés dans le réseau via un chemin aléatoire pour obscurcir leurs origines.
Un Proxy (serveur mandataire) ou l'utilisation des réseaux anonymes pour assurer la privacy des utilisateurs ont été largement discutés **[54]**. Le principal objectif est de garder l'anonymat même dans un réseau à conditions complexes. L'Onion Routing et son successeur Tor « **T**he **O**nion **R**outing » **[56]** fournissent un scénario sophistiqué de protection des utilisateurs, ce qui rend difficile aux attaquants de retracer les utilisateurs via l'analyse du trafic réseau. L'anonymat au niveau du réseau a été considéré comme un sujet de recherche important depuis la conception des Mixs. Le système à faible latence Tor étant la seconde génération de l'Onion Routing. Tor constitue une amélioration par rapport au premier projet, il est utilisé et testé par une communauté dédiée. Il présente une technique appropriée assurant l'anonymat au niveau des réseaux, permettant aux utilisateurs d'effectuer des communications anonymes.
O. Berthold et al **[57]**, proposent un Framework pour générer un accès Internet anonyme en temps réel via l'utilisation du concept de Mix. Hawkey **[59]** expose le besoin de garantir l'anonymat de l'identité pour assurer la privacy dans le Web 2.0.
Un certain nombre de protocoles d'authentification anonyme ont été proposés par Rivest et al **[91]** sur la base de signature de groupe. Slamanig **[92]**, a mené une étude à base de chiffrement à clé publique, dont le concept principal derrière l'authentification anonyme était la création d'un anonymat fixé pour tous les utilisateurs, leur permettant de prouver leur identité en envoyant n challenges différents chiffrés avec n clés publiques différentes, plutôt que d'envoyer un seul challenge r. Ce modèle est mis à profit des réseaux ad-hoc.

4.3.2. Anonymat et Authentification dans le Cloud

Quant au Cloud, un groupe de protocoles d'authentification déployé dans un tel environnement a été discuté **[45]**.

Une analyse des différents modèles de confiance dans un tel environnement distribué a été effectuée par Li et Ping **[93]**, qui proposent un nouveau modèle de confiance qui divise le Cloud en domaines ou un ensemble d'agents de confiance permet d'atteindre une authentification par laquelle la relation de confiance peut être construite. Concernant l'assurance de la privacy dans le Cloud, des travaux de recherche ont été réalisés notamment Siani **[22]**, qui expose la privacy comme problématique de base dans un environnement Cloud et propose de l'intégrer lors de la conception des services. Les auteurs dans **[24]**, proposent un système de gestion des identités orienté utilisateur permettant à l'utilisateur de contrôler ses données. Govinda et al **[94]**, ont utilisé la technique de signature de groupe afin d'assurer la privacy des utilisateurs dans un Cloud privé. Slamanig **[95]**, introduit la consommation anonyme des services Cloud en spécifiant une limite quant aux ressources consommées. Le modèle proposé « anonymous yet authorized and bounded cloud resource » emploie la technique de signature en aveugle partielle afin de rajouter une limite de ressources à consommer pour chaque utilisateur.

Trois travaux de recherche seront présentés dans la section suivante, proposant l'intégration de la privacy dans un environnement de Cloud Computing.

Approche 1: Cloud Anonyme « Anonymous Cloud »

Dans cette approche **[60]**, le but est de préserver la privacy du propriétaire des données stockées dans le Cloud. Ceci est réalisé grâce à un ensemble de ressources appartenant au Cloud et mis à profit pour construire des circuits anonymes, basés sur le principe du réseau Tor, à travers lesquels les clients peuvent soumettre des données et des jobs à exécuter.
L'authentification anonyme proposée se base sur la cryptographie à clé publique pour relier en toute sécurité les jobs et les données aux utilisateurs à des fins de facturation et de gestion. Ceci se fait sans révéler l'identité de l'utilisateur aux nœuds qui ne sont pas de confiance «Untrusted Nodes». Ce mécanisme est réalisé à travers un «Manager Node» qui manipule des méta-données concernant les utilisateurs pour pouvoir les facturer convenablement.

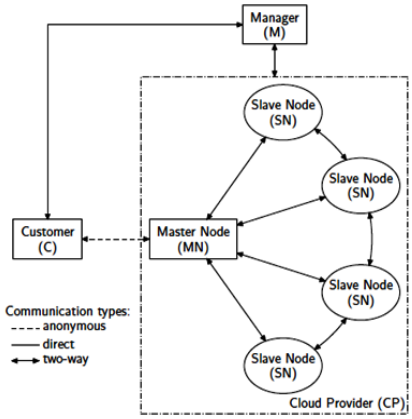


Figure 2.10 Architecture du Cloud anonyme

Dans l'architecture précédente, le Manager est supposé comme un nœud de confiance et ne doit pas communiquer avec les autres nœuds dans le but de porter atteinte à la privacy. Les autres nœuds (le Master et un pourcentage P des nœuds Salves) sont potentiellement des nœuds malicieux et peuvent s'entendre pour essayer de divulguer l'anonymat. Dans l'architecture, nous remarquons la présence d'un Cloud Provider et d'un Manager indépendant. Toutes les entités (C, CP, M, MN, SNs) sont équipées de paires de clés publique/privée utiles dans la construction du circuit Tor.

- Cloud Provider « CP » : Offre les services de calcul aux clients qui envoient des jobs. Les clients accèdent aux services via un mode « pay-as-you-go » dont le paiement est géré par un Manager indépendant « M ». Dans cette architecture, les jobs sont soumis via un Master Node centralisé « MN » qui les partitionne et les schedule à travers une collection de Slave Nodes « SNs ».
- Manager « M » : Il est séparé de l'infrastructure CP, il permet l'authentification du client et la facturation, il :
  - Stocke les clés publiques de MN et SNs.
  - Maintient l'ensemble des SNs, pour faciliter la construction des circuits.
  - Fournit à chaque client C: Un jeton d'accès **t** et des informations d'identification **c**, par exemple : un mot de passe.

Les fonctionnalités de facturation, révocation des clés, mise à jour des certificats, étant dépendantes du déploiement, elles n'ont pas été détaillées.
Un Client C commence par communiquer avec le Manager en lui envoyant **<t, c, k>**K_M, le Manager vérifie l'information d'identification **c** et le jeton **t** et voit s'il y a au moins k SNs disponibles (k étant le nombre de SNs demandé par C pour construire son circuit).
M renvoie une réponse à C contenant **SN list,** K_{SN}**,** K_{MN} : la liste des SNs choisis, leurs clés publiques ainsi que celle de MN.

Le client C envoie une requête de construction de circuit aux SNs fournis. Puis, C peut envoyer sa requête vers MN via le circuit anonyme. Le client C envoie: **< < t, <t, c>** K_C **>** K_M**,** data> K_{MN}. MN peut voir la partie data mais ne peut pas voir la partie m=**< t, <t, c>** K_C > K_M qui est la métadonnée. Il l'envoie vers M pour vérification. Une fois la réponse valide reçue, MN fait un «job dispatche» du calcul relatif à la requête vers les SNs. Une fois les résultats reçus, il les transmet à C.
La manière de faire communiquer MN avec M pour la facturation est que MN peut tagguer un rapport par la métadonnée m et l'envoyer à M qui connaitra la quantité de ressources consommées afin de facturer convenablement C.

Approche 2: PCCP « **P**reserving **C**loud **C**omputing **P**rivacy »

Dans ce travail **[25]**, le modèle présenté intègre une architecture à trois niveaux (trois couches) et vise à préserver la confidentialité des informations relatives aux utilisateurs du Cloud. Les trois couches du modèle sont illustrées dans la figure 2.11 :

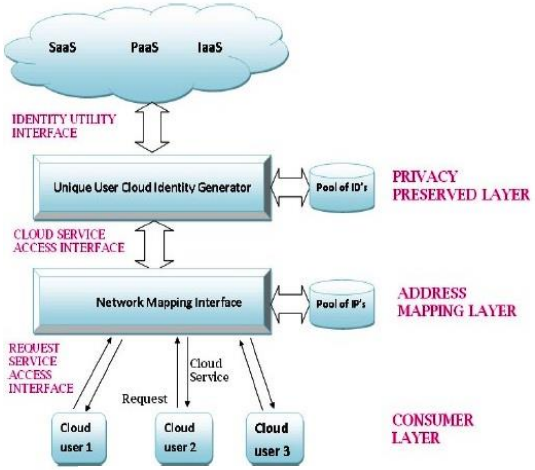


Figure 2.11 Modèle PccP

Les couches comprennent : *la couche utilisateur*, *la couche mapping d'adresses* et *la couche Préservation de la privacy*. Toute demande de service par un utilisateur Cloud devra être traitée par ces trois couches, puis en conséquence, la requête de l'utilisateur sera servie.

- Couche utilisateur: Concerne l'utilisateur du service Cloud. Ce dernier peut être une organisation ou un individu qui envoie une demande de service à la couche mapping d'adresses. La couche de l'utilisateur traite tous les aspects qui permettent à l'utilisateur Cloud d'accéder aux services fournis par le fournisseur de services CSP.

- Couche mapping d'adresses: La requête au service arrive à l'interface d'accès «Request Service Access Interface» : (R-sa-I). La R-sa-I interagit ensuite avec l'interface mapping réseau «Network Mapping Interface» : (N-map-I) disponible à la *couche mapping d'adresses*. La N-map-I maintient un pool d'adresses IP. Elle crée alors un mapping approprié entre l'adresse IP d'origine de l'utilisateur et une adresse IP modifiée : OTIP « Owned Translated IP». Dans ce processus, la protection de l'adresse IP d'origine de l'utilisateur est assurée. Une fois le mapping d'adresse fait, la *couche mapping d'adresses* va transmettre la requête du service à la *couche de Préservation de la privacy*. La requête du service arrivera à la *couche Préservation de la Privacy* en utilisant OTIP.

- Couche Préservation de la privacy: La requête arrive de la Couche mapping d'adresses à l'interface d'accès aux services Cloud (C-sa-I) de la couche Préservation de la privacy. Cette dernière possède un générateur d'identité unique. Ce générateur assure la génération d'une identité unique pour chaque utilisateur afin de garantir la protection de ses informations sensibles. Toutes les communications à partir de / vers le Cloud passant par l'interface utilitaire d'identité « Identity Utility Interface »: (Id-UI) sont faites en utilisant l'adresse OTIP.
La fonctionnalité du générateur d'identité unique étant de générer une identité unique « Unique Service-dependent Identity » : USID, en suivant les mesures suivantes:

(i) L'identité doit être unique pour tous les utilisateurs.
(ii) La durée de vie de cette identité est le temps où l'utilisateur utilise ce service. Une fois que l'utilisateur termine son utilisation, son identité doit être détruite.
(iii) L'utilisateur peut utiliser des services Cloud différents. Dans ce cas, des identités multiples vont être allouées à l'utilisateur se basant sur le type de service. Une liste de toutes les différentes identités devra être maintenue et mise à jour de temps à autres.
(iv) L'identité générée doit être en fonction de l'adresse IP modifiée. L'USID ainsi généré est renvoyé dans un pool d'USIDs déjà généré en utilisant une logique de matching. Si une correspondance est trouvée, l'USID est simplement écarté.

Cet USID généré par la couche Préservation de la privacy sera ensuite utilisé pour accéder au service Cloud à travers l'interface utilitaire d'identité. Les données résultantes de l'utilisation du service fourni par le Cloud, sont ensuite envoyées à travers la couche Préservation de la privacy et la couche de mapping d'adresses à destination de l'utilisateur Cloud.
Une fois une réponse reçue, la liste des USID peut être mise à jour / étendue. Une traduction sera également faite de l'adresse OTIP à l'IP l'originale au niveau de l'interface mapping réseau. Les fonctionnalités de mapping d'adresses réseau et ID utilisateur permettent et assurent à l'utilisateur une plus grande capacité de contrôle sur ses identités.
USID : User ID généré et attribué à chaque utilisateur. C'est la concaténation de trois informations qui sont:

- OTip: Owned Translated IP reference
- TS <req>: Time Stamp de la requête relative au service Cloud
- CS <type> : Code du type du service Cloud
  tel que: USID = Concat {OTip,TS<req>,CS<Type>}

OTIP a été incorporé dans l'USID afin d'assurer la privacy de l'adresse IP. Le but principal de l'ajout du code du type de service est de s'assurer que les identités générées aux utilisateurs correspondent aux différents services demandés : différents USID seront générés.

Approche 3: Consommation anonyme des services Cloud SaaS

Dans cette proposition **[61]**, une architecture d'un Framework assurant la consommation anonyme des services SaaS a été discutée. C'est une conception multicouche permettant la combinaison de différentes techniques d'anonymat: chaque couche utilise une technologie d'anonymat spécifique visant à améliorer la privacy. La proposition utilise une entité courtier appelé **TPB «T**hird **P**arty **B**roker**»**, qui sert d'intermédiaire pour réaliser les contrats entre les utilisateurs et le CSP. Il s'occupe également des questions relatives aux informations d'identification anonymes qui les génèrent, en utilisant la technique de signature de groupe pour la consommation anonyme des services. A propos de l'anonymat du réseau, ils proposent l'utilisation du réseau Tor réel. Dans cette architecture, chaque couche emploie alors une technique d'anonymat pour assurer la privacy de l'utilisateur Cloud, ceci étant réalisé comme suit:

- Distribution des informations d'identification aux consommateurs: chaque consommateur a ses propres informations d'identification qu'il utilise pour s'authentifier anonymement pendant la consommation de services. Lors de l'authentification d'un message signé avec la signature de groupe, le fournisseur est capable de reconnaître le consommateur (signataire) comme un membre légitime du groupe, à savoir un utilisateur du service approprié. Pourtant, il ne possède pas d'informations sur l'identité du membre qui vient de signer le message. TPB étant le groupe Master, il émet plusieurs informations d'identification: l'ensemble des informations d'identification forme un groupe. Les signatures de groupe dictent si le groupe est statique, ou s'il permet des jointures dynamiques.
Les informations d'identification anonymes sont donc fournies par le TPB et sont placées dans la partie métadonnée du message. Le fournisseur utilise les informations d'identification pour authentifier le consommateur et savoir si c'est un utilisateur autorisé. Cependant, le fournisseur ne pourra pas identifier le consommateur qui a demandé le service. Le service sera fourni si l'authentification est valide.

- Anonymat des données: pour assurer l'anonymat des données, il y a eu comme proposition une combinaison appropriée des techniques d'anonymisation des données, comme la technique « k-anonymat ». L'anonymat des données peut être difficilement appliqué dans les services du Cloud Computing, parce qu'il existe beaucoup de types différents de données et de structures de données. Une analyse service par service peut être nécessaire pour établir la technique d'anonymat des données la plus appropriée, en vue d'assurer une protection efficace des données.

- Anonymat du réseau: Pour assurer l'anonymat du réseau, il y a eu la proposition de l'utilisation du réseau Tor réel. Cependant, aucune discussion à propos de la latence due à l'utilisation des nœuds du réseau Tor réel n'a été procurée.

Ces trois caractéristiques sont résumées dans la figure 2.12.

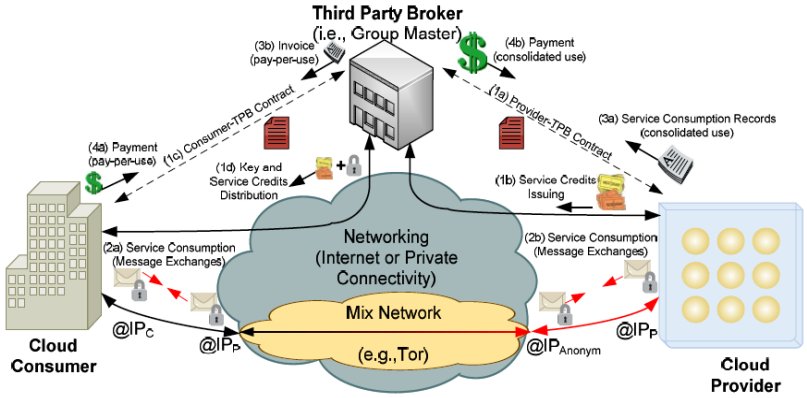


Figure 2.12 Design de la consommation anonyme des services SaaS

4.4. Discussion et Comparaison

Dans la première approche, les nœuds esclaves, ou un pourcentage d'entre eux, peuvent ne pas être de confiance et peuvent même communiquer avec le nœud Master pour faire de la chaînabilité (essayer de lier tous les services utilisés par un client C). De même, tous les nœuds esclaves ainsi que le nœud Master appartiennent au CSP, qui même étant honnête peut être curieux. Le fait qu'il contrôle toute cette structure, il pourra déduire des informations sur ses clients, ce qui implique que la privacy ne soit pas totalement assurée. A ces suppositions, vient s'ajouter l'hypothèse qui exige que le nœud Manager doit être de confiance et ne doit en aucun cas communiquer avec le nœud Master ainsi que les nœuds esclaves. Ainsi, le problème de confiance est toujours présent et l'architecture n'est pas totalement indépendante de ce concept qui exige un certain niveau de confiance et de loyauté pour l'assurance de l'anonymat des utilisateurs.

Dans le deuxième modèle, les différentes couches proposées sont également fournies par le CSP lui-même. Il pourra alors contrôler toute la structure et divulguer les identités relatives aux utilisateurs, en faisant un chainage de chaque information contenue dans chaque couche. Cela est dû non pas parce que le CSP n'est pas de confiance (implique qu'il suit bien les spécifications du protocole) mais il peut être parfois curieux et le fait de tout contrôler cela lui permet d'avoir la trace de tous ses utilisateurs.

Dans la troisième approche, le TTB « **T**hird **P**arty **B**roker » doit être une entité de confiance. Cela étant mentionné dans la proposition, cette confiance doit être vis-à-vis du CSP et des utilisateurs. Le TTB gère le groupe d'utilisateurs et peut à tout moment tracer un utilisateur dans le but de le révoquer du système. Ceci pourrait se faire via la technique de signature de groupe où le TTB joue le rôle du groupe Master, avec possibilité de remonter à un élément du groupe (remonter à l'utilisateur qui a signé le message). Cette traçabilité et révocation sont réalisées dans le cas d'un utilisateur à comportement suspect (membre malhonnête du groupe). L'approche proposée était une approche de consommation anonyme des services SaaS avec traçabilité possible.

Pour résumer, dans les approches décrites, les auteurs intègrent l'utilisation d'une entité de confiance TTP « **T**rusted **T**hird **P**arty » qui possède les informations concernant les autres entités notamment les utilisateurs.

Dans la première approche AnonymousCloud, c'était le Manager qui devait impérativement être de confiance et qui ne devait en aucun cas communiquer avec les autres nœuds (le Master et les nœuds esclaves). Dans le modèle en couche PccP, les différentes couches proposées dans ce modèle sont fournies par le CSP lui-même qui doit donc être de confiance et ne jamais essayer de divulguer l'identité de ses utilisateurs ce qui n'est pas évident. Dans la troisième, le Framework était complet et l'entité TPB proposée agissait comme un intermédiaire entre le CSP et ses utilisateurs mais ce TPB devait également être de confiance.

Pour récapituler, la majorité des solutions proposées assurant la privacy des utilisateurs Cloud, possèdent comme caractéristique commune l'utilisation d'un TTP pour vérifier et approuver le PII « **Pe**rsonally **I**dentifiable **I**nformation ». Dans le cas où le TTP est lui-même le CSP donc ils forment la même entité, le CSP supposé de confiance, peut également être curieux et peut inférer des informations à propos de ses utilisateurs ce qui implique que la privacy n'est pas complètement assurée. Un autre danger existe, la présence d'une seule entité TTP, engendre une approche centralisée permettant de compromettre tous les PIIs des utilisateurs si cette dernière est compromise.
Enfin, un CSP est un tiers qui maintient des informations sur d'autres entités (ses utilisateurs). Faire confiance à un tiers nécessite de prendre le risque d'assumer que ce tiers de confiance agira comme il est prévu (ce qui ne peut pas être vrai tout le temps). Donc, à chaque traitement de données relatives à une entité dans le Cloud, la question de privacy ou de confidentialité peut se poser. La plupart des solutions proposées utilisent le TTP pour vérifier ou approuver le PII. Les problèmes majeurs rencontrés dans ces approches notamment, dans un environnement de Cloud Computing sont:

- Le TTP pourrait être un service du Cloud, donc le CSP pourrait être lui-même le TTP et par conséquent, le TTP n'est pas dans tous les cas une entité de confiance indépendante du CSP.

- Aussi, en utilisant un seul TTP, cela conduit à une approche centralisée qui engendre le danger d'essayer de compromettre ce TTP et donc de compromettre tous les PIIs.

5. Conclusion

Ce chapitre a abordé le processus d'authentification et l'authentification dans un environnement de Cloud Computing notamment l'authentification anonyme. Des travaux réalisés afin d'assurer la privacy des utilisateurs Cloud ont été discuté. Ceci étant notre but majeur « Pouvoir utiliser les services Cloud tout en étant anonyme et tout en prouvant sa légitimité vis-à-vis du CSP ».

De plus, l'originalité sera d'assurer ce niveau d'anonymat et de respect de la vie privée des utilisateurs Cloud tout en étant indépendant du CSP et de n'avoir aucune contrainte relative au niveau de confiance qu'il prétend assurer. Dans le prochain chapitre, notre contribution sera présentée, consistant en la proposition d'un nouveau protocole d'authentification anonyme assurant la privacy des utilisateurs indépendamment du concept de confiance imposé dans un tel environnement.

Chapitre 3: Nouvelle Approche d'Authentification Anonyme Adaptative dans le Cloud

1. Introduction

L'évolution technologique pose de nouveaux défis en matière de protection des données à caractère personnel. Le développement des activités en ligne tels que l'échange d'e-mails, l'accès aux sites web et aux réseaux sociaux, facilite l'échange des informations personnelles et permet de les rendre publiques et accessibles à l'échelle mondiale. De plus, l'expansion des services Cloud offre une dimension plus importante de partage et de mutualisation des ressources. Cependant, le recours au Cloud peut signifier une perte de contrôle sur les informations potentiellement sensibles, car les données sont externalisées.

Dans les environnements Cloud, la confiance reste une notion floue et très difficile à estimer dans un tel environnement hétérogène. De plus, le fait de limiter la visibilité de la surveillance (monitoring) aux utilisateurs, induit à un manque de confiance important entre les utilisateurs et les fournisseurs Cloud, outre le fait que ces derniers peuvent être en sous-traitance à l'insu des utilisateurs. Le traitement des données en dehors des organisations pose un niveau de risque inhérent et un sérieux problème de confiance. Dans le Cloud, il devient alors nécessaire de bénéficier des services offerts et de les utiliser d'une manière sûre sans se soucier du niveau de confiance qu'offre le Cloud Service Provider. Etant donné que le problème de sécurité entre le CSP et les utilisateurs du Cloud est principalement un problème de confiance, il est par conséquent utile d'arriver à un compromis entre tout avantage offert par le CSP et le niveau de confiance requis.
De nombreuses lois existent à propos de la protection des données personnelles, imposant des normes pour la collecte, l'entretien, l'utilisation et la divulgation de ces données. Ces lois doivent être satisfaites par les fournisseurs Cloud. La nature du Cloud exige des implications importantes pour assurer la protection des informations personnelles, de business et gouvernementales. Les fournisseurs Cloud peuvent stocker les informations à plusieurs endroits où les externaliser, il sera très difficile alors de déterminer à quel point elles sont sécurisées et qui en a accès **[67]**. L'impact que peut engendrer l'utilisation de ces informations peut être très important, il est donc devenu primordial d'introduire la protection des données personnelles des utilisateurs afin de leur garantir plus de sécurité.

Le Cloud doit fournir des mécanismes forts pour bien authentifier ses utilisateurs et atténuer le plus possible de risques. Un point capital et automatique lors de l'utilisation des services Cloud est la présence d'un bon mécanisme d'authentification. L'authentification étant un processus standardisé et adopté par un grand nombre de pays et d'organisations, ce mécanisme constitue une étape fondamentale avant d'obtenir l'accès aux services procurés. Cependant, les utilisateurs peuvent ne pas vouloir que le CSP apprenne à quels services ils accèdent et combien de fois ils utilisent un service. La question qui se pose alors est : *Comment protéger la vie privée de l'utilisateur final et comment lui assurer une authentification anonyme?*

Ainsi, un système renforcé avec une authentification anonyme efficace, motive les utilisateurs à accéder aux services fournis par le CSP avec plus de confiance et une plus grande capacité de contrôle de leurs informations personnelles. Cependant, le problème de l'anonymat est l'authentification des utilisateurs. Le compromis sera donc de pouvoir vérifier l'authenticité d'un utilisateur sans connaître son identité.

Motivation :

Un intérêt majeur concernant la protection des données personnelles dans le Cloud se reflète dans le Cloud e-santé. Ce dernier permet de fournir une plate-forme intégrée contenant les données médicales de milliers de patients et permet d'unifier le format des enregistrements médicaux ainsi que d'assurer leur disponibilité tout le temps et de n' importe où. L'objectif principal étant de soutenir la recherche médicale en facilitant l'essai clinique d'un nouveau traitement ou en permettant de contrôler la propagation d'infections et d'épidémies à l'échelle nationale d'un pays.

Les données médicales sont à la fois sensibles et privées, elles nécessitent un niveau élevé de sécurité et de protection contre les utilisations non autorisées. La privacy constitue un obstacle automatique lors de l'adoption d'un Cloud e-santé par les institutions médicales. Cependant, un Cloud anonyme respectant les conditions d'accès à ces enregistrements et les personnes autorisées, ainsi que la sécurisation des différents EHR « **E**lectronic **H**ealth **R**ecord », va permettre de bénéficier de la scalabilité et l'élasticité d'un tel environnement.

En outre, une donnée médicale est à la fois confidentielle, sauf pour la relation médecin/patient, en plus d'être personnelle par rapport au patient. Ce dernier ne voudra en aucun cas que ses données médicales soient divulguées (même vis-à-vis du CSP) en dehors du cadre ou elles doivent être manipulées. Autre que le patient concerné, il n'y a que le médecin traitant qui est autorisé à accéder aux enregistrements. Le niveau de privacy peut être amélioré en dissimulant le propriétaire des données et sa provenance sans pour autant anonymiser les données proprement dites (ce qui va assurer leur confidentialité). Le chiffrement est une condition non suffisante pour protéger la vie privée des patients. Dans le domaine médical, pouvoir révéler l'identité d'un patient constitue en effet une violation de sa vie privée, même si ses données médicales sont confidentielles (éventuellement chiffrées). L'accès aux mines de données médicales est considéré comme une action très confidentielle, même vis-à-vis du Provider. Un accès anonyme est considéré comme très approprié dans le Cloud e-santé afin de dissimuler l'utilisateur (patient, médecin traitant).

Notre objectif est de proposer une approche dont le but est de fournir une architecture complète, en vue d'assurer une privacy optimale de l'utilisateur Cloud. La privacy est considérée comme un élément principal, l'authentification anonyme proposée devra donc garantir une consommation anonyme des services Cloud et à la demande. Le CSP adoptant notre approche assurera une préservation de la privacy de ses utilisateurs en termes de protection de leurs données personnelles, notamment l'identité. Ils pourront ainsi accéder et procéder à la consommation des services de manière anonyme et légitime sans que le CSP connaisse leur identité. Il saura néanmoins que des services ont été consommés.

2. Généralités: Définitions

Avant de décrire notre approche, nous commençons par introduire un ensemble de généralités contenant des concepts qui permettront par la suite de faciliter la compréhension au lecteur.

- **Consommation de services Cloud:**

Un service Cloud est un actif échangeable qui s'utilise à la demande, dont la consommation est mesurable et se paie à l'usage. Son échange fait l'objet d'une contractualisation par l'utilisateur soit directement auprès du fournisseur, ou soit auprès d'un intermédiaire (un courtier « Broker ») **[63]**. Le fournisseur de services doit définir tous les engagements qu'il prétend assurer. Ces engagements lui permettent de répondre aux interrogations simples et légitimes de ses futurs utilisateurs, notamment:

- Quelle sera la disponibilité des services: 24h/24h, 7j/7j, les heures ouvrées,
- En cas de problème, en combien de temps les services seront à nouveau disponibles,
- Quelle garantie sur les données: risque de perte, périodicité des sauvegardes, qui les contrôle, etc.

Ces "engagements" que prennent les fournisseurs auprès de leurs utilisateurs métiers s'appellent habituellement contrat de service "**SLA**" «**S**ervice **L**evel **A**greement» contenant tous les engagements du CSP. Evidemment, plus le SLA est contraignant, plus le prix de consommation de services est élevé. Lors de l'accès aux services Cloud, l'authentification est un processus clé qui ajoute une couche de sécurité, notamment contre les utilisations non autorisées, c'est l'étape qui précède chaque scénario d'accès aux services, aux ressources, à un réseau et cela dans n'importe quel domaine. Chaque utilisateur se connectant au Cloud devra prouver son appartenance et sa légitimité vis-à-vis du CSP. Ceci est faisable via le processus d'authentification avant de pouvoir accéder et bénéficier des différents services comme le montre la figure 3.1.

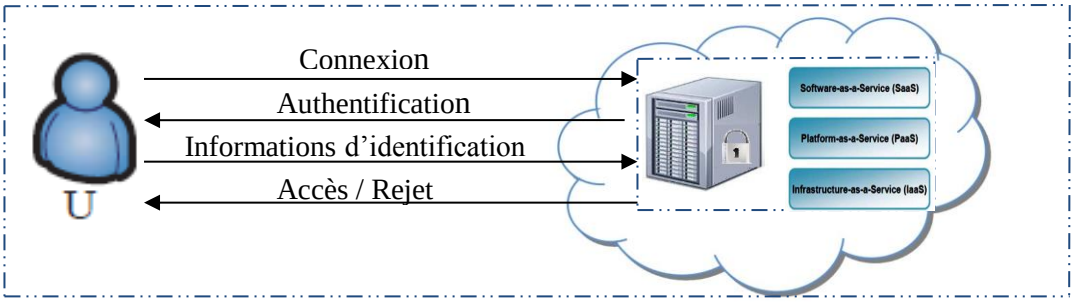


Figure 3.1 Consommation des services Cloud

- **Identité:** Représente l'ensemble de données qui définit de manière unique un utilisateur et le différencie des autres. Tous les utilisateurs d'un système doivent avoir une identité pour obtenir un accès sécurisé aux ressources et services au sein du système.
  Les informations qui peuvent identifier personnellement un utilisateur, sont appelées informations personnellement identifiables PII « **P**ersonally **I**dentifiable **I**nformation ». La protection des PII d'une diffusion non désirée ou non autorisée est souvent une obligation légale et appartient au domaine de la protection de la vie privée. **[17]**

- **Privacy:** Il est essentiel de comprendre que toute information non sécurisée en ligne peut être consultée par toute personne. Cela est dû à l'universalité de l'Internet et de sa capacité à diffuser rapidement des informations importantes. Dans le cadre de notre travail, la privacy est la capacité d'un système à protéger l'identité et la localisation de ses utilisateurs contre la divulgation non autorisée. **[21]**
  Dans notre contexte, la privacy dans le Cloud Computing peut être définie comme : **[24]**
  « La capacité d'une entité à contrôler les informations qu'elle révèle sur elle-même au Cloud (au CSP) et la possibilité de contrôler qui peut accéder à ces informations ».

En général, toutes les définitions de la privacy l'associent au besoin des personnes à garder leurs informations sensibles secrètes, sûres et sous contrôle.

- **Confiance «Trust»:** En général, la confiance se réfère au "niveau de confidence en quelque chose ou à quelqu'un" **[6]**
  La confiance dans le Cloud peut donc être vue comme le niveau de confidence des utilisateurs lors de l'utilisation du Cloud. La confiance tourne autour de l'assurance et de la confidence que les personnes, les données, les entités, les informations ou les processus fonctionnent et se comportent de la manière prévue et n'enfreignent pas les règles. Avoir un contrôle complet sur les données est une voie possible pour gagner la confiance de l'utilisateur et donc le sentiment d'être en sécurité. Le contrôle, la prévention et la sécurité sont les aspects clés qui déterminent le niveau de confiance des utilisateurs vis-à-vis des services et des fournisseurs. A un niveau plus profond, la confiance pourrait être considérée comme une conséquence du progrès vers la réalisation des objectifs de sécurité et de privacy. **[68]**

- **Anonymat:** Selon le standard international ISO/IEC 15408 sur les critères d'évaluation de la sécurité des technologies de l'information, l'anonymat assure que l'utilisateur peut utiliser une ressource ou un service sans divulguer son identité. Les conditions requises pour l'anonymat assurent la protection de l'identité de l'utilisateur liée à un sujet ou à une opération. **[69]**

- **Non-chaînabilité «Unlinkability»:** C'est l'impossibilité pour d'autres utilisateurs d'établir un lien entre les différentes opérations effectuées par le même utilisateur. **[69]**

- **Non-traçabilité «Intraceability»:** C'est l'impossibilité pour d'autres utilisateurs d'établir un lien entre une opération effectuée et l'utilisateur qui l'a effectué. **[69]**

- **Communication anonyme: [70]**

  La majorité des systèmes n'offrent pas la notion d'anonymat. L'attaque possible est la présence d'un sniffer situé sur la route des messages. L'adversaire a seulement besoin de lire les messages interceptés pour connaître l'émetteur et le destinataire d'un message. Pour assurer l'anonymat, les messages sont envoyés à travers le réseau via un chemin aléatoire pour obscurcir leurs origines et rendre l'analyse de trafic plus difficile à réaliser.
  En effet, au lieu d'emprunter un itinéraire direct entre la source et la destination, dans une communication anonyme, les paquets de données suivent une trajectoire aléatoire choisie au préalable. Cette trajectoire définit les points intermédiaires par lesquels doit passer le paquet de données (qui sont en nombre de trois dans le cas du réseau Tor « **T**he **o**nion **r**outing ») en dehors de son routage sur le réseau Internet (le paquet passe par les routeurs du réseau réel mais doit être routé à chaque fois vers un nœud, pour lui effectuer le déchiffrement et la modification de l'entête avant de le réinjecter dans le réseau). Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données. Le circuit anonyme va donc offrir un ensemble de maillons interconnectés permettant d'anonymiser la connexion (voir figure 3.2): N1, N2 et N3 étant les trois nœuds du réseau anonyme. N1 : Nœud d'entrée « Entry Node », N2 : Nœud intermédiaire « Middle Node » et N3 : Nœud de sortie « Exit Node ».

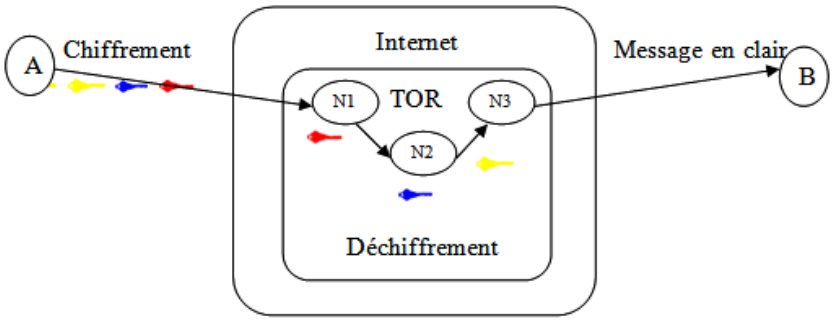


Figure 3.2 Communication anonyme

- **Identification Anonyme:** *cas de la signature en aveugle «Blind Signature»*

  En cryptographie, une signature en aveugle est une signature effectuée sur un document qui a été masqué avant d'être signé, afin que le signataire ne puisse prendre connaissance de son contenu. De telles signatures sont employées lorsque le signataire et l'auteur du document ne constituent pas la même entité. A l'instar d'une signature électronique classique, la signature en aveugle résultante peut être vérifiée avec le document original démasqué **[53]**.
  C'est une primitive cryptographique où le possesseur d'un message peut le faire signer (au sens digital du terme) sans que le signataire ne puisse en lire le contenu. Comme toute signature électronique, la signature obtenue peut être vérifiée en utilisant la clé publique de signature. La signature en aveugle assure automatiquement la propriété de non-chaînabilité: même le signataire du message lui-même ne pourra pas relier la signature et le message correspondant à la version aveugle du message qu'il a signé.
  Le principe de la signature en aveugle est : **[72]**
  1. Le texte (message) à signer est d'abord caché en multipliant le message par un facteur d'aveuglement aléatoire.
  2. Il est ensuite envoyé au signataire qui le signe en utilisant un algorithme de signature standard (exemple RSA).
  3. Le résultat est renvoyé au possesseur du message qui peut ensuite lever le facteur d'aveuglement pour obtenir la signature.
  4. Résultat : la même paire (message, signature) peut être vérifiée comme dans le cas d'un algorithme de signatures standard, sans que le signataire ait eu connaissance du message.

3. Etude du modèle de l'adversaire et informations sensibles

3.1. Classification des menaces et des données sensibles à protéger dans le Cloud

Définir le modèle de l'adversaire nous permettra de cerner les problèmes de sécurité relatifs à un environnement de Cloud Computing, notamment les différentes sources de menaces. Ces menaces peuvent mettre en péril la privacy dans un tel environnement. Avant de le définir, il est important de répondre aux questions suivantes:

- Qui est l'adversaire ?
- Quelles sont ses motivations ?

Un adversaire, dans notre contexte, représente toute entité capable de causer une atteinte à la privacy des utilisateurs en accédant ou en prenant possession de la totalité ou d'une partie de leurs données personnelles. Par exemple, l'adversaire pourrait être lui-même le fournisseur Cloud.
L'atteinte à la privacy qui nous intéresse le plus est que l'identité de l'utilisateur: nom, adresse, etc. puisse être révélée. Une connaissance de l'adversaire représente potentiellement toute information auxiliaire sur les utilisateurs du Cloud qui peut l'aider à inférer afin de divulguer certaines informations personnelles non présentes explicitement et de faire de larges déductions.
L'adversaire peut prendre en entrée un ensemble de données assaini (possiblement des connaissances auxiliaires) et essayer d'inférer de nouvelles informations personnelles. Il peut par conséquent essayer de faire un chainage pour relier conjointement les enregistrements de deux ensembles de données différents contenant une fraction d'utilisateurs en commun.
Parmi les motivations de l'attaquant, nous retrouvons :

- L'usurpation d'identité
- La fuite d'information
- La traçabilité malveillante
- Le déni de service

En outre, Il existe de nombreuses menaces de sécurité qui affectent la confidentialité des données, notamment celles personnelles, dans un environnement Cloud. Ces menaces peuvent être classées en deux catégories à savoir menaces internes ou externes (cas d'un intrus malicieux), pouvant provoquer une perte de données, une perte de contrôle ou l'interruption des services.

Une vue abstraite du modèle de l'adversaire relatif à un environnement Cloud est illustrée dans la figure 3.3. **[62]**

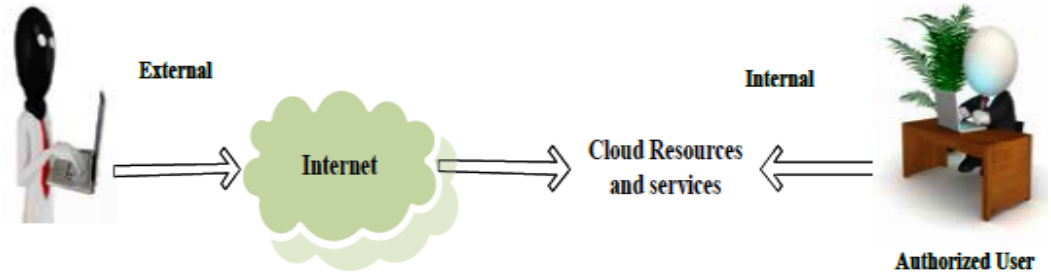


Figure 3.3 Modèle de l'adversaire dans le Cloud

1. Interne: la menace dans ce cas, provient des employés du CSP (actuels ou anciens), qui possèdent une connaissance de l'infrastructure, y compris de la sécurité. Ainsi, dans le cadre de leur mission, ils peuvent avoir un accès direct aux données. **[64]**

Les menaces internes dans le Cloud sont à leur tour divisées en deux catégories: **[65]**

Menaces internes au niveau du CSP: où l'entité interne est un employé malveillant travaillant au niveau du CSP.

Menaces internes au niveau de l'organisation: où l'entité interne est un employé de l'organisation qui a externalisé toute ou une partie de son infrastructure dans le Cloud.

2. Externe: la menace dans ce cas, provient des entités qui existent en dehors du système et tentent d'agir sur la sécurité de l'infrastructure des services. L'attaque peut être passive: écouter le trafic réseau, ou active: insérer du trafic malveillant, lancer une attaque de déni de service, etc. **[64]**
Les menaces externes, comprennent les intrus ou les attaquants du réseau. Leurs objectifs étant d'essayer d'obtenir des informations sur les données des utilisateurs, sur leur comportement et aller jusqu'à vendre les informations collectées. **[66]**

Concernant les deux menaces interne ou externe, la motivation peut avoir des fins malicieuses ou peut être une simple curiosité. Les menaces externes peuvent ne pas être aussi néfastes que celle internes. Cependant, elles restent plus difficiles à dissimuler et peuvent encore être amplifiées via les médias. Le CSP / Organisation doivent donc se préparer à faire face à de telles situations.

Il est à noter qu'outre les menaces internes et externes, il existe des menaces naturelles: des erreurs pouvant se produire naturellement d'un logiciel lui-même ou d'une défaillance matérielle **[64]**.

Dans notre travail, nous avons pu recenser toutes les entités possibles pouvant nuire à la confidentialité des données personnelles de l'utilisateur Cloud présentées comme notre modèle de l'adversaire, ainsi que les informations sensibles pouvant être exploitées par ces entités afin de divulguer des données personnelles de l'utilisateur Cloud.
Nous avons identifié les types de menaces suivantes, qui peuvent être présentes dans un environnement de Cloud Computing:

- Le CSP lui-même: Du point de vue de la privacy, le CSP est en position d'être honnête, ce qui n'est pas toujours vrai. Le CSP peut aussi être curieux voire malhonnête (tente de donner/vendre les données, les jeter ou les perdre volontairement).

- Les employés du CSP: Le CSP peut être considéré comme étant honnête, mais ses employés peuvent ne pas l'être. Comme déjà discuté, la relation entre les utilisateurs Cloud et le CSP est essentiellement une relation de confiance. Ce dernier doit assurer la confidentialité des données stockées. Néanmoins, le problème réside dans le fait que les employés du CSP puissent accéder aux données des utilisateurs, ce qui leur permettra par exemple de les vendre à une société de marketing ou à une entreprise concurrente. Cette dernière situation représente une sérieuse menace. Ces employés internes malveillants sont donc des employés du CSP qui abusent de leur position pour collecter de l'information ou pour d'autres fins néfastes (comme le cas d'un employé mécontent). Ils peuvent ne pas avoir besoin d'exploiter les points d'insécurité techniques et peuvent avoir un accès direct aux données ou un accès grâce à une escalade de privilèges.

- L'utilisateur: Un utilisateur peut être honnête ou malhonnête voire malveillant. Les utilisateurs Cloud peuvent effectuer des scans de ports et d'autres tests sur d'autres utilisateurs dans le réseau interne. La technologie Cloud étant basée sur le partage et la mutualisation des ressources (entre différents utilisateurs), une ressource (physique ou virtuelle) peut être utilisée par plusieurs utilisateurs. Ceci augmente le risque qu'un utilisateur malveillant puisse tenter d'infiltrer les instances ou les espaces de stockage des autres utilisateurs pour voler des informations, insérer des virus pour l'espionnage ou encore détruire intentionnellement les données.

- Un intrus ou attaquant: Peut-être toute personne malveillante (y compris un employé dans le CSP), qui vise à révéler l'identité ou l'activité d'un utilisateur. Les attaquants essayent généralement d'atteindre leurs objectifs en réalisant certains exploits techniques pour avoir l'accès au Cloud. Cela peut inclure le service hijacking, l'usurpation d'identité, les APIs non sécurisées, une vulnérabilité dans le système, de l'ingénierie sociale, etc.

- Un tiers de confiance TTP «**T**rusted **T**hird **P**arty»: Représente une entité facultative. Le CSP peut être en mesure d'utiliser un tiers ayant des capacités telles que de vérifier l'exactitude des fichiers logs des utilisateurs ou de réaliser des audits. Cette entité étant séparée du CSP peut aussi former une menace pour les utilisateurs.

Nous considérons donc, dans notre modèle de l'adversaire, qu'un adversaire (appartenant à une catégorie des cas cités précédemment) peut être malveillant ou simplement curieux, qui tente de révéler et de découvrir l'identité d'un utilisateur, son comportement, ses centres d'intérêt, faire un profilage, trouver sa localisation, etc.

De même, nous considérons comme données ou informations sensibles:

- L'identité d'un utilisateur Cloud : son identité électronique (ID de l'utilisateur (UID), un pseudonyme...) ou son PII «**P**ersonally **I**dentifiable **I**nformation»: Cela inclut toute information qui pourrait être utilisée pour identifier ou localiser un individu, par exemple le nom ou l'adresse, ou toute information qui peut être corrélée avec d'autres informations pour identifier un individu par exemple, un numéro de carte de crédit ou un code postal.

- L'adresse IP de l'utilisateur Cloud.

- L'identifiant du service Cloud à utiliser "Service ID" (SID), mais surtout la relation Identité / Service ID, qui permet de dévoiler quel service est consommé par quel utilisateur.

- Les données de l'utilisateur, ainsi que la relation Identité / Données qui permet de savoir quelles données appartiennent à quel utilisateur (données stockées ou transférées).

3.2. Représentation du modèle de l'adversaire

Etant donné que l'objectif est de proposer une approche dans laquelle la protection des données personnelles de l'utilisateur est assurée (par un mécanisme d'authentification anonyme fournissant une consommation anonyme des services Cloud), une première étude était alors d'identifier les différents types de menaces relatives à l'environnement Cloud par rapport aux données sensibles.
Cela nous a permis de faire une classification illustrée dans la matrice ci-dessous (table 3.1), qui résume le modèle de l'adversaire identifié et relatif à un environnement Cloud par rapport aux données sensibles à anonymiser :

Informations Sensibles / Types de Menaces	Interne				Externe	
	CSP	Employées Malicieux dans le CSP	TTP	Utilisateurs Malicieux	Attaquants Passifs	Attaquants Actifs
Identité Utilisateurs	1	1	x	x	x	x
IP Utilisateurs	1	1	1	1	1	1
Données Utilisateurs	1	1	x	x	x	x
Identité/données	1	1	x	x	x	x
Identité/SID	1	1	x	x	x	x

Table 3.1 Informations sensibles vs menaces

Les lignes de la matrice représentent les informations sensibles, les colonnes représentent les entités pouvant les collecter/exploiter. Concernant les valeurs de la matrice:
1 => L'adversaire a la possibilité d'obtenir/exploiter l'information sensible.
0 => L'adversaire ne peut pas obtenir/exploiter l'information sensible.
x => indéfini peut prendre 1 ou 0.

Les valeurs des différents labels de la matrice de classification sont attribuées selon le modèle général adopté dans un environnement Cloud, sans aucune considération de mécanisme de Sécurité / Privacy.

4. Description de l'approche d'authentification anonyme proposée

Le modèle de référence d'un processus d'authentification standard **[71]** comprend deux phases à savoir : l'enregistrement et l'authentification électronique.
Par analogie à ce modèle, notre approche va également contenir ces deux phases importantes. La différence réside cependant dans le fonctionnement interne de chacune.
La phase d'enregistrement établit comment les jetons d'identité relatifs aux informations d'identification sont attribués aux entités. L'authentification électronique établit à son tour comment vérifier l'identité d'un demandeur via le jeton d'identité préalablement obtenu.
Tout schéma d'authentification suppose au moins deux parties : un Demandeur, qui présente une identité et un Vérificateur, qui s'assure de sa validité. Un schéma d'authentification doit permettre la validation de l'identité d'une entité légitime en présence d'attaques possibles, comme par exemple le rejeu des messages émis par l'entité légitime effectué par un attaquant afin d'usurper l'identité de cette dernière. Pour contrer les attaques, le schéma d'authentification doit fournir des garanties de sécurité qui permettent au Vérificateur de contrôler l'identité présentée par un Demandeur.

Dans notre approche :

- **La phase d'enregistrement** représente le processus par lequel un utilisateur obtient les informations d'identification (comme le cas d'un mot de passe ou d'un certificat électronique) pour une authentification ultérieure.

- **La phase d'authentification électronique** représente la preuve de possession PoP: **P**roof **o**f **P**ossession, au cours de laquelle l'identité électronique de l'utilisateur est vérifiée.

4.1. Architecture générale de l'approche d'authentification anonyme

Pour pouvoir mieux expliquer l'approche proposée: *Authentification Anonyme Adaptative dans un environnement de Cloud Computing*, cette section va illustrer une vue globale de l'architecture.
L'architecture proposée permettra aux utilisateurs de réaliser les opérations suivantes : s'enregistrer, obtenir des tickets d'accès anonymes, s'authentifier et enfin, passer à la consommation des services comme le montre la figure 3.4:

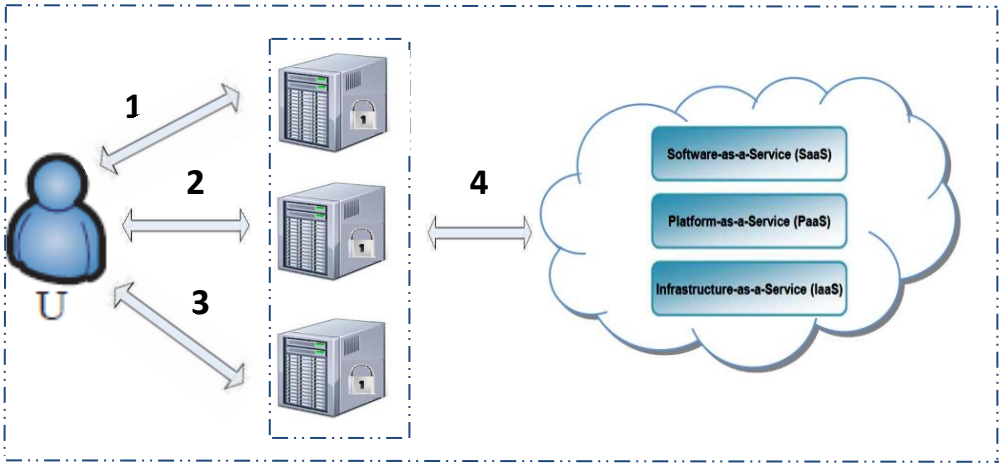


Figure 3.4 Principe du Modèle proposé

Ces quatre opérations sont réalisées via les processus suivants :

1. Enregistrement : Ce processus est initialisé par les utilisateurs qui auront un statut initial de souscripteurs. A l'issue de ce processus, ils prendront le statut d'utilisateurs.

Ce processus permet en premier lieu de procéder à l'enregistrement des utilisateurs. L'enregistrement, dans notre cas se fait de la manière suivante:
- Enregistrement des détails de l'utilisateur : les attributs fournis par l'utilisateur.
- Livraison d'un contrat d'enregistrement (pseudo contrat généralement électronique).
- Livraison d'une preuve d'enregistrement.

Les attributs fournis par l'utilisateur vont inclure : le nom, l'adresse, l'organisation et l'e-mail. Les informations sensibles incluent : les attributs cités, l'adresse IP de l'utilisateur, les données transférées lors de l'accès au Cloud et l'identifiant du service à consommer.

Le point qui caractérise notre processus d'enregistrement consiste à la génération d'une **politique de protection des données personnelles de l'utilisateur**. Cette politique va contenir toutes les clauses expliquées et justifiées notamment quant à :

- L'accès anonyme aux services via des tickets anonymes.
- La négociation avec l'utilisateur à propos de ses attributs fournis en lui demandant le niveau de privacy désiré pour chaque attribut.

L'originalité de notre approche réside en effet, dans la possibilité offerte à chaque utilisateur de pouvoir affiner et personnaliser sa politique de protection de ses données personnelles selon ce qu'il juge nécessaire comme informations à cacher et donc de lui proposer une authentification adaptative et flexible.

2. Obtention des tickets d'accès anonymes: Au cours de ce processus, l'utilisateur enregistré préalablement (possédant une preuve d'enregistrement), se présente dans le but d'obtenir un ticket d'accès anonyme, qui lui sera utile lors du processus d'authentification ultérieure.

3. Authentification : Pour pouvoir accéder aux services, l'utilisateur aura besoin de présenter des informations d'identification obtenues préalablement (qui sont dans notre cas les tickets d'accès). Le processus d'authentification anonyme va donc garantir la légitimité de l'utilisateur en contrôlant le ticket présenté. Le résultat de la vérification permettra à l'utilisateur de passer à la consommation de services, ou le cas échéant de lui refuser l'accès.

4. Consommation des services : Une fois le processus d'authentification achevé, l'utilisateur sera, dans le cas favorable, dirigé vers les services Cloud. Le processus de consommation des services va donc s'occuper des requêtes de l'utilisateur, de sa consommation et par la suite du paiement.

Selon les informations sensibles considérées dans le processus d'enregistrement, l'approche se divise en deux modèles :

- Modèle de base considérant l'anonymat de l'identité de l'utilisateur.
- Modèle étendu prenant en compte l'anonymat de l'identité de l'utilisateur en plus de l'anonymat de sa localisation et de ses différentes connexions : anonymat de l'adresse IP.

Suite à cette considération, l'approche est sélective, elle permettra au CSP d'offrir à ses utilisateurs deux niveaux d'anonymat. L'utilisateur aura donc le choix de sélectionner le niveau d'anonymat souhaité:

- **Premier niveau d'anonymat :** représenté par le modèle de base permettant une consommation anonyme des services Cloud, passant par un ensemble de gestionnaires (Mangers), dont le principe est l'utilisation de tickets d'accès anonymes générés via la technique de signature en aveugle.

- **Deuxième niveau d'anonymat :** représenté par le modèle étendu, composé du modèle de base en plus d'un ensemble de technologies venant se greffer afin d'offrir un meilleur niveau d'anonymat. Ceci permettra de pallier les limites du modèle de base et d'assurer une privacy optimale, en intégrant le principe de communication anonyme.

Considérant ces deux modèles, l'approche se révèle donc adaptative en termes de :
1. Permission à l'utilisateur de choisir le niveau d'anonymat désiré (identité ou identité + localisation).
2. Génération d'une politique adaptative de protection des données personnelles et relative à chaque utilisateur, en lui permettant de choisir le niveau d'anonymat souhaité relatif à chaque attribut constituant son PII.

Avant de procéder à l'explication de chaque modèle, nous allons d'abord présenter les différents acteurs impliqués ainsi que leurs rôles.

4.2. Acteurs et leurs rôles

Par analogie aux différents processus effectués, cette section va présenter les acteurs impliqués ainsi que leurs rôles. Chaque acteur possède une appellation reflétant son rôle :

1. L'utilisateur : Entité principale, l'utilisateur peut être n'importe quel client utilisant les services proposés. Son rôle principal est d'accéder au Cloud afin d'utiliser ses services.

2. Le CSP : Fournisseur de services ayant comme rôle d'offrir un ensemble de services aux différents utilisateurs et d'être sûr que seuls les utilisateurs autorisés pourront y accéder.

3. Gestionnaire d'enregistrement : C'est la première entité impliquée dans le modèle d'authentification anonyme proposé. Il a comme tâche principale l'enregistrement des utilisateurs. Le gestionnaire d'enregistrement procède à l'inscription des utilisateurs et leur fournit un contrat d'engagement et une preuve d'enregistrement. Il a comme rôle principal de garantir l'identité des utilisateurs enregistrés vis-à-vis du gestionnaire d'attribution des tickets d'accès.

4. Gestionnaire d'attribution des tickets d'accès : Deuxième entité importante, le gestionnaire d'attribution des tickets d'accès ayant comme tâche la délivrance des tickets d'accès anonymes aux utilisateurs. Ainsi, il se porte garant de la légitimité des utilisateurs vis-à-vis du gestionnaire de consommation de services.

5. Gestionnaire de consommation de services : Troisième gestionnaire, il s'occupe de la consommation des services et de l'authentification des utilisateurs.

6. L'adversaire : Toute entité malveillante ayant comme motivation la divulgation des données personnelles des utilisateurs Cloud. L'adversaire inclut le CSP (le Provider lui-même ainsi que ses employés), les utilisateurs et les attaquants externes.

Les deux sections suivantes vont présenter chaque modèle d'authentification proposé, à savoir le modèle de base et le modèle étendu, ainsi que les étapes nécessaires à leur fonctionnement.

4.3. Modèle de base

L'objectif de ce modèle est d'obtenir l'autorisation d'accès pour consommer anonymement un service Cloud. Cela se réalisera via des tickets permettant aux utilisateurs Cloud d'effectuer des requêtes anonymes, en passant par un ensemble de Managers (gestionnaires déjà cités) lors de la consommation des services vis-à-vis du CSP.

Le modèle de base est composé de trois principaux gestionnaires, comme illustré dans la figure 3.5:

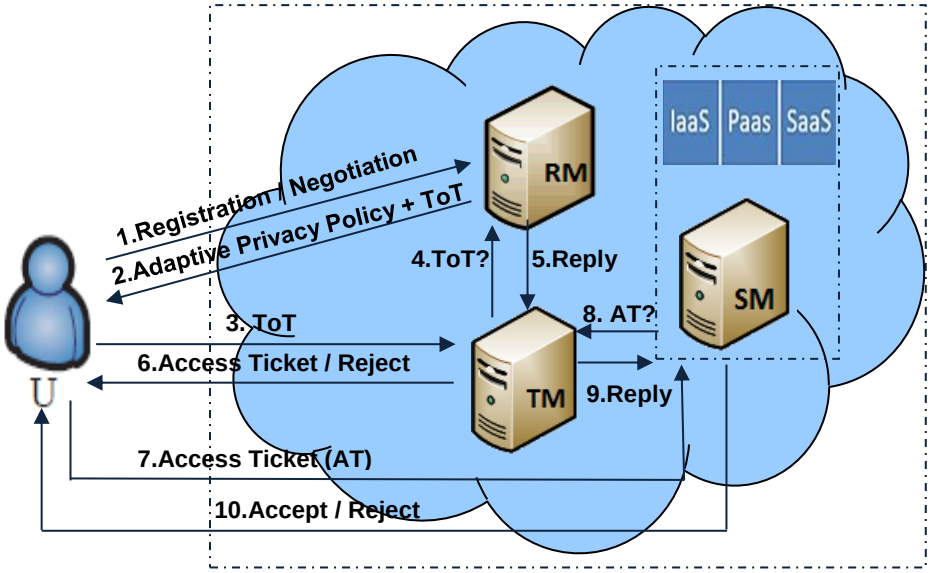


Figure 3.5 Aperçu des différents composants relatifs au modèle de base

4.3.1. Etapes constituant le modèle de base

Nous commençons cette section par la description des différentes étapes constituant le modèle de base de notre approche. Nous décrirons par la suite, dans un scénario d'exécution détaillé, les différents gestionnaires qui la constituent (différents Managers) et l'interaction entre eux.
Pour permettre une consommation anonyme des services dans un environnement de Cloud Computing, nous avons énuméré les étapes suivantes, nécessaires et complémentaires préservant au mieux la privacy des utilisateurs:

- **L'étape1:** Enregistrement des utilisateurs et génération de la politique adaptative de protection des données personnelles relative à chacun.
- **L'étape2:** Obtention du ticket d'accès anonyme «Access Ticket».
- **L'étape3:** Consommation du service Cloud souhaité.

Comme illustré dans le schéma:

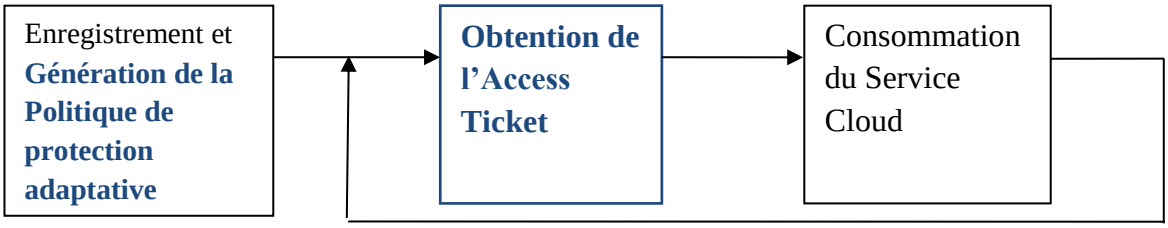


Figure 3.6 Les étapes constituant le modèle de base

Etape1: Enregistrement des utilisateurs et génération d'une politique adaptative de protection des données personnelles relative à chaque utilisateur.

Dans cette première étape, le but est de présenter le système Cloud aux utilisateurs potentiels, le SLA et la politique de protection proposée.

Cette étape a pour vocation de familiariser les utilisateurs et de les motiver à rejoindre ce Cloud pour bénéficier de ses services, notamment le fait d'être anonyme.
Le résultat final sera de recenser et d'enregistrer les utilisateurs intéressés, de formuler les contrats d'engagement, mais surtout dans notre cas, de générer pour chaque utilisateur la politique de protection des données personnelles adaptative et adéquate à ses exigences.

Etape2: Obtention du ticket d'accès « Access Ticket »

Après que l'étape d'enregistrement soit achevée, cette deuxième étape consiste alors à orienter l'utilisateur vers l'obtention d'un ticket anonyme, lui permettant de consommer ultérieurement les services Cloud. Ceci a pour objectif de cacher chaque utilisateur, sans pour autant révéler son identité au CSP.
Ce ticket va donc jouer le rôle des informations d'identification nécessaires au processus d'authentification, qui sera dans ce cas anonyme vu que l'utilisateur n'aura qu'a présenté le ticket d'accès déjà obtenu.

Etape3: Consommation des services Cloud

A ce niveau, l'utilisateur se présentera au système, en ayant comme but de parvenir à passer de manière sûre et correcte le processus d'authentification pour pouvoir accéder aux services offerts (stockage, capacités de calcul CPU, Softwares…). Dans ce cas, il n'aura qu'à présenter son ticket obtenu au préalable dans l'Etape2. Le CSP ne saura pas quel utilisateur vient demander l'accès aux services, mais seulement qu'un utilisateur légitime veut y accéder.

Le détail relatif à chaque étape du processus, ainsi que les différents composants qui assurent ce fonctionnement et l'interaction entre eux, sera détaillé dans les sections suivantes.

4.3.2. Le gestionnaire d'enregistrement

Un utilisateur U doit s'enregistrer vis-à-vis de RM « **R**egistration **M**anager », avant de pouvoir consommer les services offerts par le CSP. RM se porte donc garant de l'identité des utilisateurs vis-à-vis du CSP.
Après finalisation de l'enregistrement, U obtiendra un **ToT** « **T**icket **o**f **T**icket » qui va lui servir à obtenir par la suite un autre ticket chez TM (**T**icket **M**anager). Ce jeton va donc assurer que l'identité correspond effectivement à une entité réelle déjà enregistrée, avec des attributs correctement associés (qui peuvent être parfois très limités, par exemple l'utilisateur ne fournira que l'e-mail). RM est composé de deux modules importants à savoir le Module de négociation et le Module de validation.

- **Module de négociation:** Ce module va se charger de présenter à l'utilisateur les services Cloud offerts, la politique de protection des données personnelles adoptée ainsi qu'un ensemble de suggestions. L'utilisateur lui, aura à présenter un ensemble d'attributs nécessaires à l'enregistrement (son PII).
  La politique de protection proposée va permettre de négocier avec l'utilisateur concernant ses attributs fournis, en lui demandant le niveau de privacy désiré pour chaque attribut. Ceci sera reflété par un flag déterminant le choix de l'utilisateur à propos de chaque attribut concernant son identité:

1- La valeur «1» déterminera que l'anonymat est exigé.
2- La valeur «0» déterminera que l'anonymat n'est pas exigé.

3- Si pas de choix ce cas est pris comme ignoré, le même traitement que le cas précédent sera adopté, la valeur «0» sera enregistrée.

Le résultat sera un vecteur binaire relatif à chaque utilisateur U reflétant son choix. Ce vecteur sera enregistré dans la politique adaptative de protection des données personnelles résultante relative à chaque utilisateur.
Exemple : Si U répond par :

Nom: oui / Adresse: oui / Organisation: oui / e-mail: ignore

Alors, le vecteur sera: V_u= {1, 1, 1, 0}.

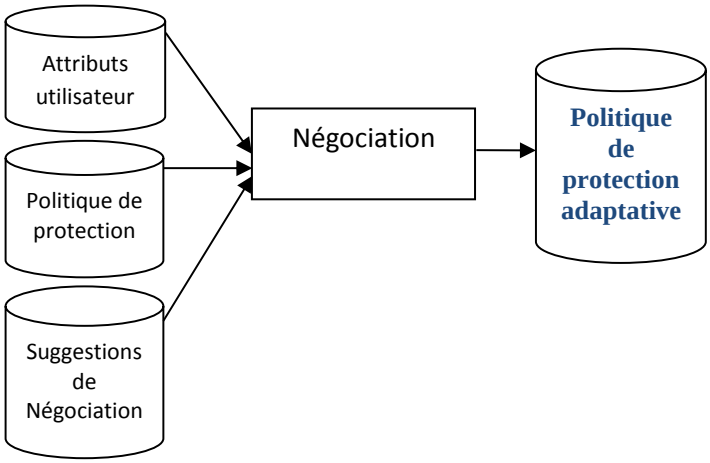


Figure 3.7 Architecture du Module Négociation

- **Module de validation:** Ce module va se charger de valider l'enregistrement des utilisateurs et de générer le contrat d'utilisation tenant compte de la politique de protection des données personnelles adaptative à chacun. En outre, un ToT «**T**icket **o**f **T**icket**»** sera généré comme preuve d'enregistrement, accompagné d'un nonce **n** pour se protéger contre toute interception et retransmission du ToT par un intrus, cherchant à usurper l'identité d'un utilisateur légitime.
  Le ToT est considéré dans notre cas comme un jeton initial, qui caractérise la preuve d'enregistrement. Ce ToT se concrétise comme tout jeton par une chaîne de caractères aléatoire unique et difficile à deviner. Dans notre cas, la chaine est associée à une autre chaine aléatoire, qui représente un nonce nécessaire pour se protéger d'une éventuelle utilisation non autorisée (un rejeu). Ce ToT va permettre à l'utilisateur de s'authentifier après vis-à-vis de RM lui-même, afin de prouver son appartenance à ce Cloud et vis-à-vis de TM afin d'obtenir un Access Ticket.

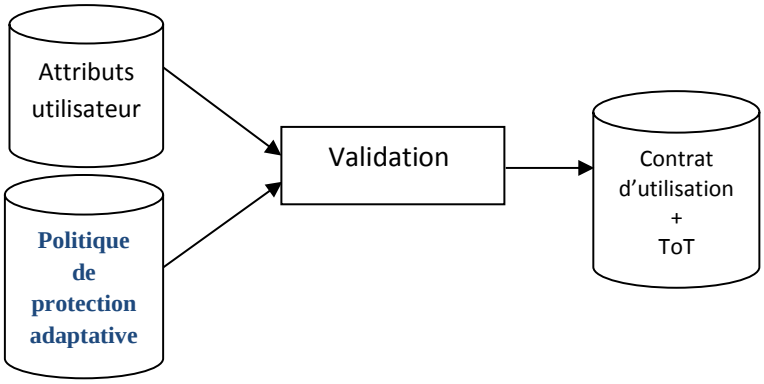


Figure 3.8 Architecture du Module Validation

Il est à noter qu'afin d'empêcher les attaques par rejeu, le modèle inclut une garantie de fraîcheur quant aux ToTs : des données additionnelles qui permettent aux Managers de vérifier que les ToTs reçus sont récents et donc, la certitude que ce n'est pas des versions rejouées d'anciens ToTs. Une solution était la possibilité de les apparier avec une estampille temporelle T. Cependant, les estampilles temporelles sont d'un maniement délicat, la notion d'une horloge suffisamment récente étant relativement vague d'une part. D'autre part, pour que le mécanisme fonctionne, il faut encore que les différentes horloges soient synchronisées et cela par un protocole lui-même sécurisé, pour éviter qu'un intrus n'attaque le système en désynchronisant les horloges, dans le but d'effectuer de nouveau des attaques par rejeu. Une solution plus simple était donc d'adopter l'utilisation de nonces (nombres aléatoires).

4.3.3. Le gestionnaire de tickets

Le gestionnaire de tickets **TM** «**T**icket **M**anager» va s'occuper de la génération des tickets anonymes en usage unique : les tickets générés sont « service dépendant », c'est-à-dire un ticket par service. L'utilisateur présente son ToT à TM qui va vérifier sa validité chez RM avant de lui attribuer un ticket anonyme via la technique de signature en aveugle. Ce ticket anonyme va aider l'utilisateur à prouver la possession et le contrôle d'un ticket équivalent aux informations d'identification.
Le processus de génération des tickets d'accès anonymes se fait donc comme suit :
Comme illustré dans la figure, les acteurs et les processus présents dans un modèle de signature en aveugle sont les suivants :

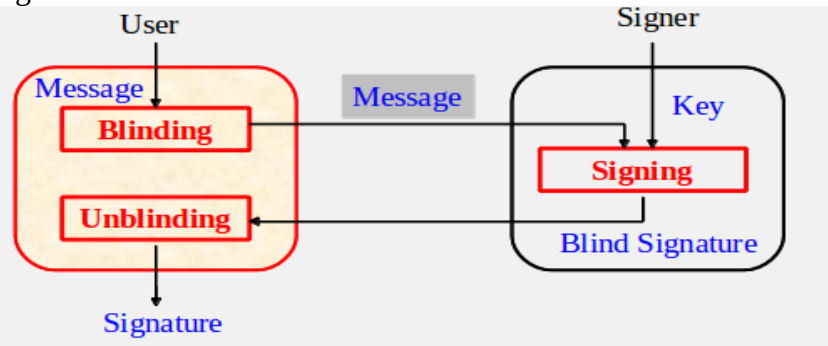


Figure 3.9 Les acteurs et les processus relatifs à la signature en aveugle

1. **Le processus « Blinding » :** L'utilisateur Cloud est le propriétaire du message m à signer. Ce processus consiste à cacher le message **m** avant de le faire signer par le signataire en le multipliant par un facteur d'aveuglement aléatoire **r** choisi par l'utilisateur Cloud.

2. **Le processus de signature « Signing » :** Le Manager TM étant dans notre cas le signataire, il recevra donc de la part de l'utilisateur, une donnée à signer (le message caché). TM procèdera à la signature via sa clé privée de signature et réalisera donc la signature en aveugle, car il signera un message sans voir son vrai contenu, grâce au processus précédent consistant à le masquer.

3. **Le processus « Unblinding » :** Après réception de la signature en aveugle, l'utilisateur procèdera à enlever le facteur d'aveuglement (blinding factor) en appliquant la fonction inverse du processus Blinding. Le résultat sera donc une signature valide relative au message **m** dont le contenu a été signé par le Manager TM. Cette signature représentera dans notre modèle un **ticket d'accès anonyme** préservé par l'utilisateur et utilisé

ultérieurement pour l'accès aux services Cloud : il représente donc l'information d'identification lors de l'authentification vis-à-vis de SM (**S**ervices **M**anager).

La figure 3.10 montre les calculs effectués lors de l'exécution des processus précédents :
Le signataire est TM: ayant comme paire de clés de signature :
Clé publique = **(n, e)** connue par les utilisateurs Cloud et Clé privée = **(n, d)** secrète.
La paire de clés utilisée pour la signature est unique et n'est dédiée que pour la signature, une autre paire sera consacrée au chiffrement.

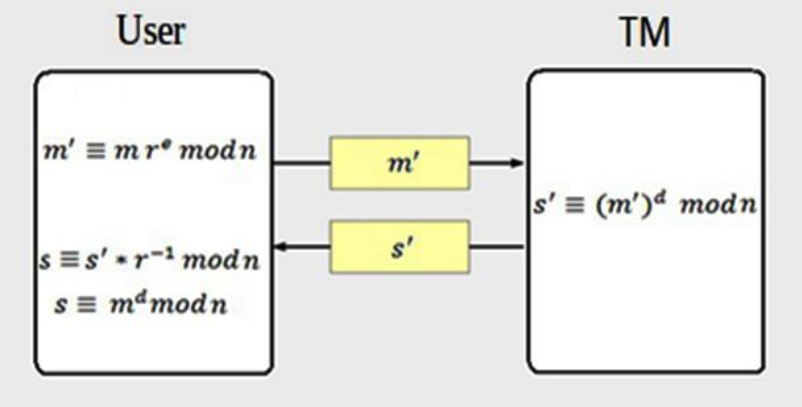


Figure 3.10 Calculs effectués dans les processus 1,2 et 3

4. **La vérification :** Le Vérificateur représente l'entité qui procèdera à la vérification de la signature en aveugle. Le vérificateur est dans notre cas le Manager TM qui va vérifier cette signature suite à une requête venant du Manager SM, lorsque l'utilisateur viendra s'authentifier ultérieurement à son niveau (au niveau du Services Manager).
   Avant d'accéder aux services Cloud, l'utilisateur aura à présenter son ticket d'accès anonyme au Services Manager SM, qui a été généré préalablement à travers les trois processus expliqués précédemment. Le processus de vérification effectué par TM visualisé dans la figure 3.11, aura comme entrée la paire (message, signature) qui sera vérifiée grâce à la clé publique de signature de TM. La sortie de la vérification sera une réponse à SM par Vrai ou Faux pour lui confirmer la validité de ce ticket, ceci permettra à l'utilisateur de commencer la consommation des services, ou lui interdire l'accès dans le cas échéant.

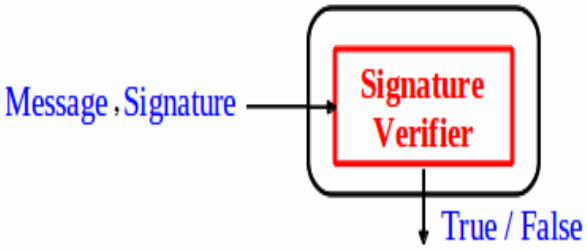


Figure 3.11 Processus de vérification de la signature

Il est à noter que pour des raisons de sécurité quant au message m (à faire signer), une fonction de hachage (ou un padding) doit être appliquée au préalable au message m. Cette technique permet de produire un condensé de message, qui est une représentation réduite et unique (qui s'apparente à une somme de contrôle sophistiquée) du message complet. Les algorithmes de hachage sont des algorithmes de chiffrement unidirectionnels, il est donc impossible de retrouver le message d'origine à partir du condensé. Les raisons principales pour lesquelles le message est haché sont :

1. L'intégrité du message envoyé est préservée: toute altération du message sera aussitôt détectée.
2. La signature sera appliquée au condensé dont la taille est beaucoup plus petite que le message lui-même.
3. Cela assurera plus de sécurité et permettra de se prémunir contre les attaques dont le but est d'observer et d'essayer de deviner le message m.

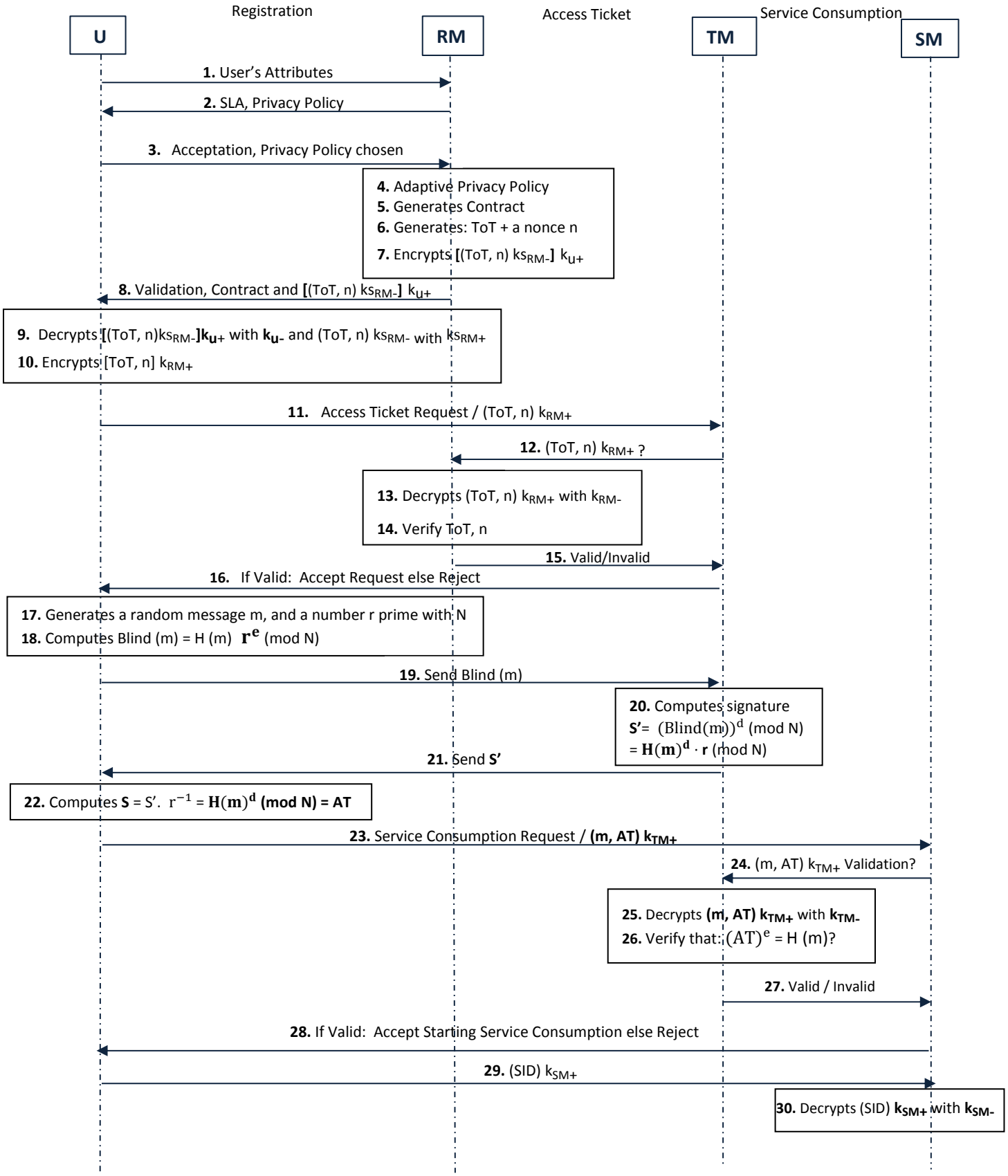
4.3.4. Le gestionnaire de services

Le gestionnaire de services **SM** «**S**ervices **M**anager» s'occupe de la consommation des services. Il reçoit le ticket anonyme de l'utilisateur, le vérifie avec TM avant de laisser l'utilisateur accéder et commencer la procédure de consommation et par la suite de paiement. SM s'appuie donc sur l'affirmation de TM et garantit l'accès aux ressources dans le cas où cette affirmation est positive.

4.3.5. Protocole d'authentification et de communication

Les différents calculs effectués à chaque étape de génération des tickets d'accès anonymes notamment les processus déjà cités, seront présentés dans les différentes transitions du protocole proposé. Ci-dessous quelques notations:

$\mathbf{k_+}$, $\mathbf{k_-}$: Clé Publique, Privée.
U: Utilisateur.
$\mathbf{k_{u+}}$ **/** $\mathbf{k_{u-}}$: Clés Publique / Privée de U.
RM: **R**egistration **M**anager: Gestionnaire d'enregistrement
$\mathbf{k_{RM+}}$ **/** $\mathbf{k_{RM-}}$: Clés Publique / Privée de chiffrement de RM.
$\mathbf{ks_{RM+}}$ **/** $\mathbf{ks_{RM-}}$: Clés Publique / Privée de signature relatives à RM.
TM: **T**icket **M**anager: Gestionnaire de tickets.
$\mathbf{k_{TM+}}$ **/** $\mathbf{k_{TM-}}$: Clés Publique / Privée de chiffrement de TM.
(N,e) , (N,d) : Clés Publique, Privée de signature relatives à TM.
SM: **S**ervices **M**anager : Gestionnaire de services.
$\mathbf{k_{SM+}}$ **/** $\mathbf{k_{SM-}}$: Clés Publique / Privée de chiffrement de SM.
ToT: **T**icket **o**f **T**icket.
n : Un nonce pour assurer la fraicheur du ToT.
H(m): Fonction de hachage appliquée au message m.
SID: Identifiant de service.


Registration
Access Ticket
Service Consumption
U
RM
TM
SM
1. User's Attributes
2. SLA, Privacy Policy
3. Acceptation, Privacy Policy chosen
4. Adaptive Privacy Policy
5. Generates Contract
6. Generates: ToT + a nonce n
7. Encrypts [(ToT, n) ksRM-] ku+
8. Validation, Contract and [(ToT, n) ksRM-] ku+
9. Decrypts [(ToT, n)ksRM-]ku+ with ku- and (ToT, n) ksRM- with ksRM+
10. Encrypts [ToT, n] kRM+
11. Access Ticket Request / (ToT, n) kRM+
12. (ToT, n) kRM+ ?
13. Decrypts (ToT, n) kRM+ with kRM-
14. Verify ToT, n
15. Valid/Invalid
16. If Valid: Accept Request else Reject
17. Generates a random message m, and a number r prime with N
18. Computes Blind (m) = H (m) r^e (mod N)
19. Send Blind (m)
20. Computes signature
S'= (Blind(m))^d (mod N)
= H(m)^d · r (mod N)
21. Send S'
22. Computes S = S'. r^-1 = H(m)^d (mod N) = AT
23. Service Consumption Request / (m, AT) kTM+
24. (m, AT) kTM+ Validation?
25. Decrypts (m, AT) kTM+ with kTM-
26. Verify that: (AT)^e = H (m)?
27. Valid / Invalid
28. If Valid: Accept Starting Service Consumption else Reject
29. (SID) kSM+
30. Decrypts (SID) kSM+ with kSM-

4.3.6. Modèle de base : Limites

En déroulant un scénario d'exécution, les tickets d'accès générés via la signature en aveugle assurent la non traçabilité de l'utilisateur, car il n'existe aucun lien entre ce ticket et l'identité de l'utilisateur. Cependant, la visibilité de l'adresse IP reste un point critique et permet à l'adversaire de faire d'éventuelles analyses de trafic et d'observations, pour essayer d'inférer et de tracer un utilisateur ciblé. Comme le montre la figure 3.12, les intrus externes, d'autres utilisateurs ou le CSP (le Provider lui-même ainsi que ses employés) peuvent essayer de tracer et de localiser un utilisateur via son adresse IP. Il est donc nécessaire et bénéfique de cacher cette information sensible.

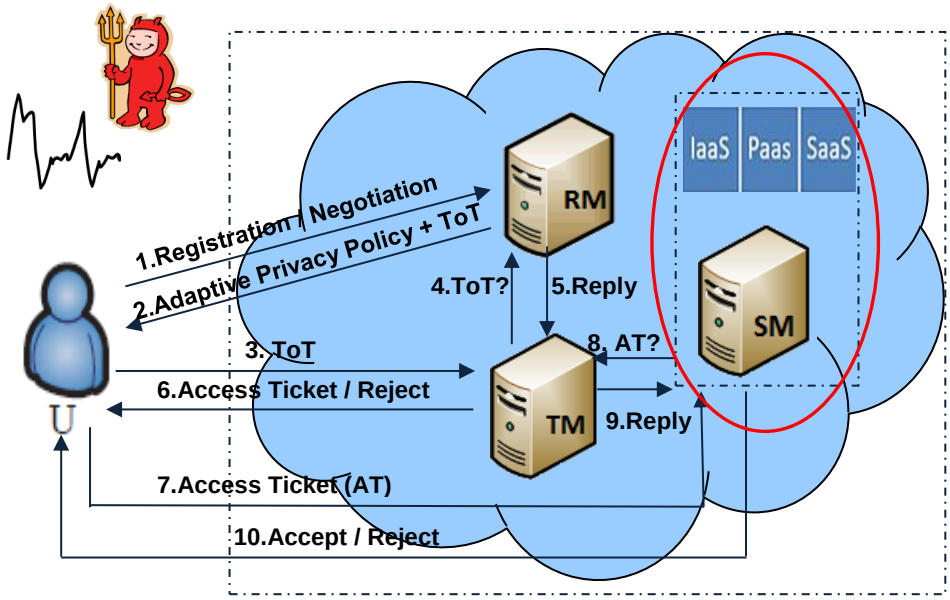


Figure 3.12 Modèle de base : traçabilité possible via l'adresse IP

La table 3.2 illustre la matrice relative au modèle de l'adversaire du modèle de base. Nous constatons que les différentes entités peuvent voir l'adresse IP de l'utilisateur.

Informations Sensibles / Types de Menaces	Interne				Externe	
	CSP	Employées Malicieux dans le CSP	TTP	Utilisateurs Malicieux	Attaquants Passifs	Attaquants Actifs
Identité Utilisateurs	0	0	0	0	0	0
IP Utilisateurs	1	1	1	1	1	1
Données Utilisateurs	0	0	0	0	0	0
Identité/données	0	0	0	0	0	0
Identité/SID	0	0	0	0	0	0

Table 3.2 Modèle de l'adversaire relatif au modèle de base

Le but du modèle étendu sera alors de parvenir à cacher cette information sensible, assurant ainsi :

- La non visibilité de l'adresse IP de l'utilisateur afin d'empêcher tout tiers non autorisé (y compris le CSP) de connaître directement ou de pouvoir dériver des informations à propos de l'utilisateur, en se basant sur son adresse IP.
- Un anonymat des différentes communications de l'utilisateur.

4.4. Modèle étendu

L'information fournie par l'utilisateur désirant l'anonymat lors de l'authentification, ne doit contenir aucune information qui pourra révéler son identité : attributs fournis lors de l'enregistrement et aussi son adresse IP. Il est à souligner que cette information doit servir à authentifier l'utilisateur, tout en étant non révélatrice de son identité.
Dans ce modèle, un ensemble de techniques vont être ajoutées au modèle de base, pour résoudre les contraintes venant se joindre à l'objectif de base, qui est de cacher l'adresse IP de l'utilisateur Cloud. En effet, dans la majorité des cas, l'adresse IP peut révéler l'identité et la localisation (position géographique) de l'utilisateur. De plus et par implication, le fait de cacher l'adresse IP, cela permet également de cacher le comportement de l'utilisateur à partir de ses différentes connexions en assurant la non possibilité de les corréler dans le temps.
Dans cette optique, au modèle de base vient s'ajouter la notion de communication anonyme se basant sur le principe du réseau Tor (déjà introduite dans les définitions section 2). Ceci va permettre de ne pas dévoiler l'adresse IP de l'utilisateur vis-à-vis de **TM**, lors de l'obtention de l'Access Ticket et vis-à-vis de **SM**, lors du passage à la consommation des services Cloud choisis. Cette manière de procéder évitera donc une éventuelle tentative d'exploitation de l'adresse IP, pour essayer de tracer l'utilisateur ou d'essayer de corréler ses connexions au fil du temps pour lier les sessions et les services consommés par ce même utilisateur offrant ainsi une privacy optimale.

4.4.1. Etapes constituant le modèle étendu

Dans cette section, nous allons présenter les différentes étapes relatives au modèle étendu de notre approche :

- **L'étape1:** Enregistrement des utilisateurs et génération de la politique de protection des données personnelles, ainsi que la gestion des accès anonymes.
- **L'étape2:** Construction du circuit anonyme permettant l'obtention des tickets et la consommation des services.
- **L'étape3:** Obtention des tickets d'accès «Access Ticket».
- **L'étape4:** Consommation du Service Cloud souhaité.

Comme illustré dans le schéma:

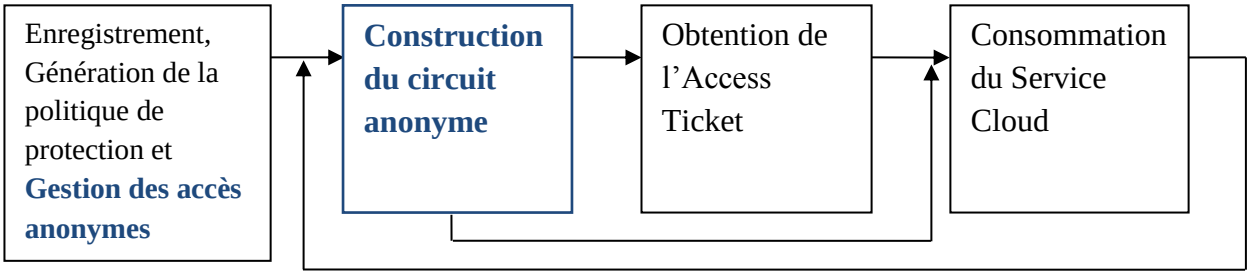


Figure 3.13 Les étapes constituant le modèle étendu

Etape1: Enregistrement des utilisateurs, génération de la politique de protection des données personnelles et gestion des accès anonymes.

Cette étape est similaire à la première étape du modèle de base. Le but étant toujours d'arriver à enregistrer les utilisateurs et leur générer la politique de protection des données personnelles adaptative et adéquate aux exigences de chacun. La seconde tâche réalisée dans cette étape est la gestion des accès anonymes des utilisateurs. Cette nouvelle manière de procéder se caractérise par l'ajout de la possibilité de procurer une communication anonyme aux utilisateurs Cloud. Cette dernière nécessite la gestion d'un ensemble de nœuds offerts par le CSP, ainsi que la participation des utilisateurs en tant que nœuds volontaires du réseau anonyme. Cela permettra d'acheminer et d'encapsuler les données envoyées entre l'utilisateur et les différents Managers.

Etape2: Construction du circuit anonyme

C'est dans cette étape que se fera la construction du circuit anonyme permettant de réaliser des communications anonymes. Tout le trafic des données transmises, lors de l'accès aux services entre l'utilisateur et le CSP sera protégé par la communication anonyme, via un ensemble de nœuds offerts par le CSP lui-même, pour relayer les communications et aussi avec la participation des utilisateurs en tant que nœuds volontaires. Cette nouvelle combinaison va permettre en effet d'éliminer la notion de confiance au CSP et le fait de router les paquets qu'à travers ses nœuds.

En outre, les nœuds du CSP ne seront choisis que comme intermédiaires. Ce sont les nœuds des utilisateurs (nœuds volontaires) qui auront la position d'entrée et de sortie « Entry et Exit node». Cette parade va permettre d'éliminer toute tentative de corrélation entre le nœud d'entrée et celui de sortie que pourra réaliser le CSP pour essayer de relayer les deux afin de compromettre la vie privée de l'utilisateur Cloud. En effet, un attaquant doit contrôler un sous-ensemble m > 1 des nœuds dans l'ensemble des nœuds actifs. Il pourrait obtenir de tels nœuds en les fournissant directement dans le réseau, ou en compromettant des nœuds existants. Son but est de coordonner ces machines compromises afin d'orchestrer mieux son attaque de corrélation.

Un cas spécifique existe cependant, consistant en la possibilité que les deux nœuds d'entrée et de sortie puissent communiquer, car appartiennent à la même entité virtuelle, comme le montre la figure 3.14:
- Un utilisateur Cloud possédant plusieurs comptes, donc plusieurs nœuds volontaires, ou
- Deux entités physiques qui peuvent collaborer pour compromettre la confidentialité du système (cas de l'attaquant collaboratif).

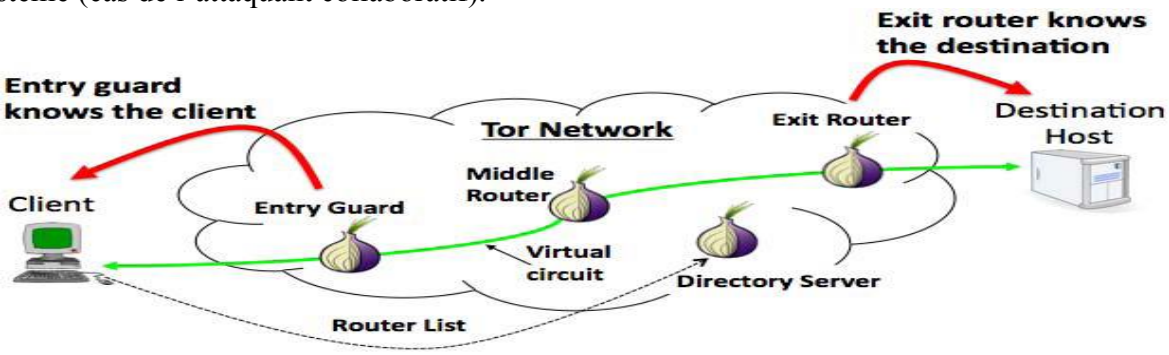


Figure 3.14 Corrélation possible entre les deux flux en entrée et à la sortie du circuit

Cette situation illustrée dans la figure 3.14 (collaboration possible entre les nœuds d'entrée et de sortie), même étant présente et avec les deux cas de figure précédents, peut être évitée ou réduite, du moment où dans la politique de choix des nœuds constituant le circuit anonyme, les nœuds sont choisis le plus possible géographiquement distants.

Etape3: Obtention de l'Access Ticket

Après l'achèvement des étapes d'enregistrement et de **construction du circuit anonyme**, cette étape consiste à orienter l'utilisateur vers l'obtention d'un ticket anonyme, en passant par le circuit anonyme déjà établi. Le ticket va permettre à l'utilisateur de consommer ultérieurement dans l'étape 4, les services Cloud.

Etape4: Consommation des services Cloud

A ce niveau, l'utilisateur aura à s'authentifier, afin de pouvoir accéder et passer par la suite à la consommation des services Cloud offerts. Dans ce cas, il aura à présenter son ticket anonyme obtenu au préalable dans l'étape 3, en l'encapsulant et en l'envoyant à travers le circuit anonyme déjà établi dans l'étape 2. Le CSP ne saura pas quel utilisateur vient demander l'accès aux services ni même voir son adresse IP, mais seulement qu'un utilisateur légitime veut y accéder. Le CSP aura l'illusion que le dernier nœud (le nœud de sortie du circuit) envoyant le ticket est bel et bien l'utilisateur. Hors, l'utilisateur réel (initiateur de la requête) remonte à trois sauts en arrière dans le circuit anonyme.

Le détail relatif à chaque étape du processus, ainsi que les différents composants qui assurent ce fonctionnement et l'interaction entre eux, sera présenté dans la section suivante.

4.4.2. Les gestionnaires (Différents Managers)

La figure 3.15, illustre un aperçu des différents Managers relatifs au modèle étendu et les différentes interactions entre eux afin d'enregistrer l'utilisateur et de procéder à la génération de l'Access ticket:

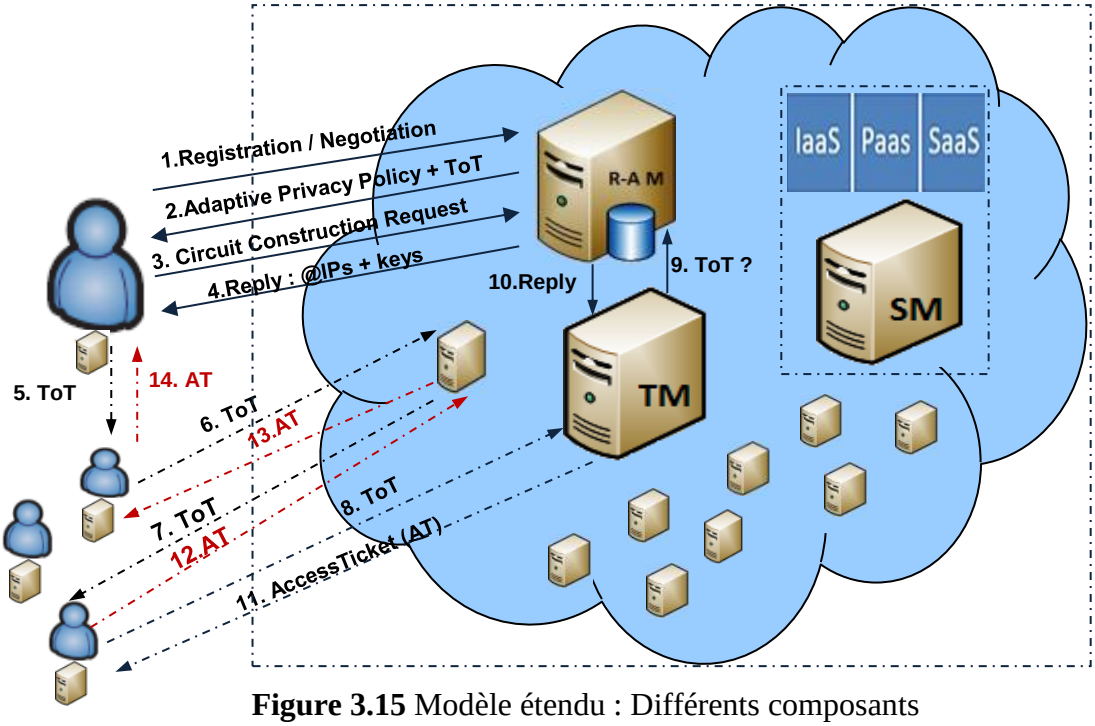


Figure 3.15 Modèle étendu : Différents composants

La figure 3.16 illustre toujours les différents Managers constituant le modèle étendu et les différentes requêtes/réponses échangées entre eux, afin de permettre à l'utilisateur de s'authentifier via son Access ticket et de commencer la consommation des services, ceci en passant par le circuit anonyme déjà établi.

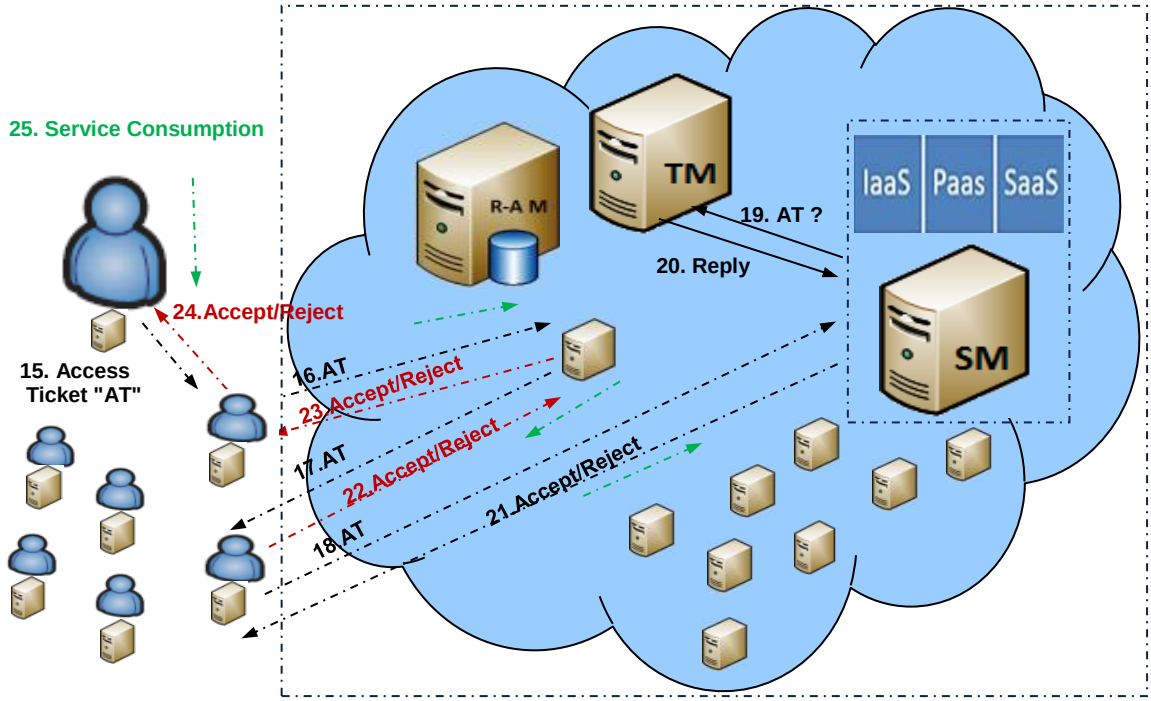


Figure 3.16 Modèle étendu : Vérification de l'Access ticket et Consommation des services

a- Le gestionnaire d'enregistrement et d'accès

Comme dans le modèle de base, un utilisateur U doit s'enregistrer chez le premier gestionnaire, qui est dans ce modèle surnommé : R-A M «**R**egistration and **A**ccess **M**anager» avant de pouvoir passer à la consommation des services offerts par le CSP. Après finalisation de l'enregistrement identique au modèle de base, U obtiendra le **ToT** « **T**icket **o**f **T**icket » qui va lui servir à obtenir par la suite un autre ticket chez TM (**T**icket **M**anager).
Les deux principaux modules de R-A M sont toujours le Module de négociation et le Module de validation, en plus d'un **Module Annuaire**.
Le traitement effectué par le module de négociation est identique au modèle de base, excepté la négociation du choix de l'utilisateur à propos de son accord ou non de relayer les communications anonymes. Si l'utilisateur choisit de devenir nœud volontaire pour acheminer les communications dans le circuit anonyme, il sera alors enregistré dans l'annuaire.

Le module annuaire va s'occuper dans ce cas, d'obtenir une paire de clés à chaque utilisateur volontaire, pour lui permettre après de participer à relayer les communications en tant que nœud volontaire. Il est également responsable de la mise à jour de la base de donnés en enregistrant l'utilisateur et la paire de clés attribuée. Cette base qui reflète le graphe de connectivité des nœuds, va lui permettre après de fournir les informations nécessaires aux utilisateurs, lors de la construction des circuits anonymes.
La construction des circuits anonymes va permettre de sécuriser le trafic et d'assurer l'anonymat des utilisateurs (anonymisation de l'adresse IP source et des différentes

connexions), du fait que les communications rebondissent à travers un réseau de nœuds distribués. Le mode de routage utilisé est en charge de l'anonymisation des connexions.
En effet, l'utilisateur Cloud construira un chemin de nœuds choisis aléatoirement pour atteindre la destination. L'utilisateur établit alors un circuit, les paquets seront routés à travers plusieurs nœuds, ce qui rendra la source de la connexion difficilement identifiable (l'utilisateur Cloud). Chacun des nœuds, dont transitent les communications via le réseau, connaît uniquement le nœud précédent et le nœud suivant. Ce dernier n'est alors pas en mesure de connaître le chemin complet emprunté par une requête envoyée par l'utilisateur.
Quant au chiffrement, il constitue la méthode qui assure l'anonymat et la confidentialité des connexions. Avant que le paquet ne soit envoyé, l'utilisateur récupère les clés publiques des nœuds du circuit aléatoire à partir de l'annuaire de R-A M, avant de construire un circuit de façon incrémentale **[56]**. Cela signifie que le circuit est construit tronçon par tronçon, en commençant par sa source. Des clés symétriques sont générées entre chaque nœud constituant le circuit anonyme (nœuds choisis aléatoirement à partir de la liste récupérée) et l'utilisateur, en utilisant les clés publiques relatives aux nœuds afin d'assurer la confidentialité des clés symétriques générées. Seule la source (qui est l'utilisateur Cloud) connait l'intégralité de ces clés symétriques, chaque nœud pour lequel la clé symétrique a été générée la connait également. L'utilisateur chiffre les données de la manière suivante:

-Le paquet est chiffré avec la clé symétrique partagée avec le dernier nœud i
-Le paquet obtenu est chiffré avec la clé symétrique partagée avec le nœud i-1 etc.

Le chiffrement mis en place ne doit pas permettre à un élément du circuit de déchiffrer le message transmis. Pour cela, lorsque le premier nœud reçoit le paquet de données, il peut le déchiffrer partiellement, mais le contenu du paquet reste toujours inaccessible puisque d'autres couches de chiffrement encapsulent les données initiales.

Pour conclure, afin de définir un trajet privé à travers le réseau, l'utilisateur Cloud doit construire au fur et à mesure un circuit de connexions chiffrées. Le circuit est construit étape par étape, chaque nœud le long du chemin ne connaît que celui qui lui a transmis les données et celui auquel il va les retransmettre. Aucun nœud ne connaît à lui seul le chemin complet pris par les données. Aucun d'eux ne peut donc intercepter la connexion au passage. Une fois le circuit établi, l'échange de données pourra commencer. Chaque nœud ne voit pas plus d'une étape dans le circuit, ni un éventuel intermédiaire, ni un nœud compromis ne peuvent analyser le trafic pour établir une relation entre la source et la destination d'une connexion. La réponse prendra le même circuit déjà établi au préalable jusqu'à l'utilisateur.

b- Le gestionnaire de tickets

Ce gestionnaire aura comme tâche la génération des tickets anonymes. L'utilisateur présente son ToT à TM « **T**icket **M**anager » qui va vérifier sa validité chez R-A M avant de lui attribuer un ticket anonyme, selon le même principe décrit dans le modèle de base. La seule différence dans ce cas, est que l'utilisateur va devoir passer par un circuit anonyme pour communiquer avec TM et ainsi obtenir le ticket anonyme en passant par un circuit anonyme déjà établi.

c- Le gestionnaire de services

Le gestionnaire de services SM «**S**ervices **M**anager» s'occupera de la consommation des services, il reçoit le ticket anonyme de l'utilisateur, le vérifie avec TM avant de laisser

l'utilisateur accéder et commencer la procédure de consommation et par la suite de paiement. La seule différence dans ce modèle est aussi le passage par un circuit anonyme pour communiquer avec SM. L'utilisateur va devoir passer par le circuit anonyme pour envoyer sa requête d'authentification et par la suite celle de la consommation de services. Toutes les communications entre U et SM seront anonymes et difficiles à corréler.

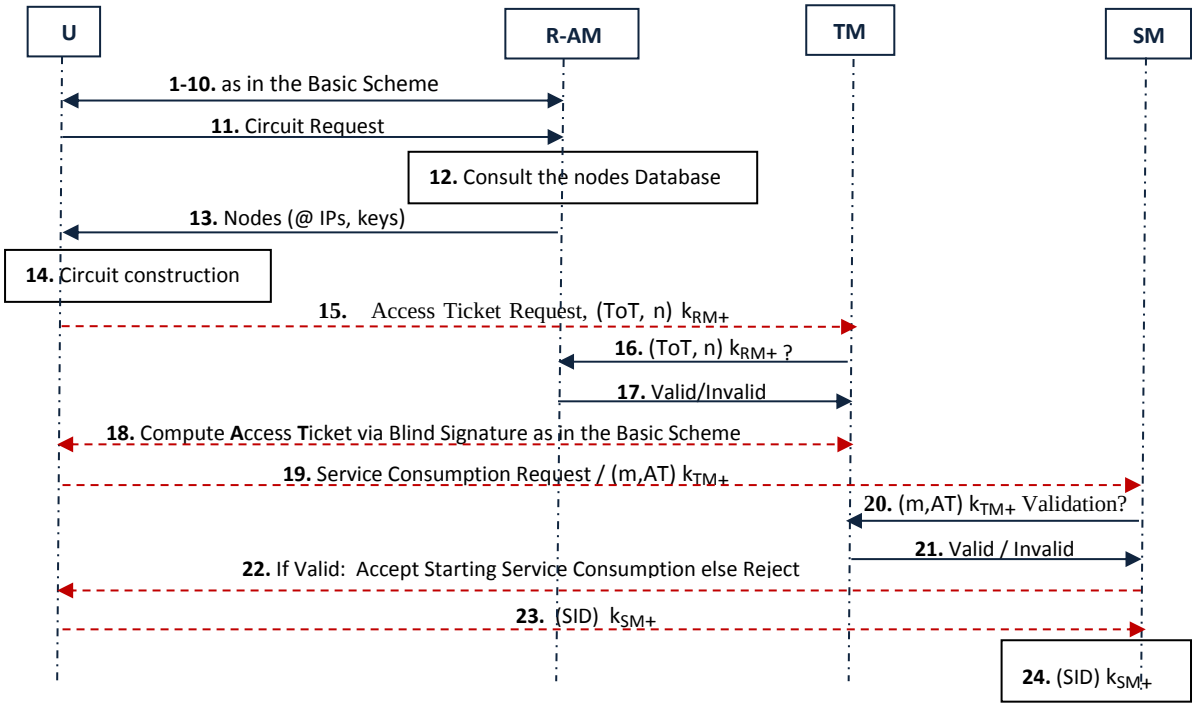
4.4.3. Protocole d'authentification et de communication

Notations (mise à jour) :

: Communication directe (non anonyme)

: Communication anonyme

R- A M: Registration and **A**ccess **M**anager : Gestionnaire d'accès et d'enregistrement



Il est à noter que le ToT même étant signé avec la clé privée de RM (respectivement de R-A M), il peut être intercepté dans le réseau. Si c'est le cas d'un attaquant externe et que la supposition de pouvoir accéder et collecter des informations est présente, le ToT reste protégé car signé avec la clé privée de RM (respectivement de R-A M). Ceci étant assuré car seuls les utilisateurs légitimes du Cloud possèdent la clé publique de signature de RM (respectivement de R-A M). Ainsi, la présence d'un utilisateur malveillant peut nuire à la sécurité des ToTs car il peut récupérer le contenu de n'importe quel ToT, du moment qu'il possède la clé publique de signature de RM (respectivement de R-A M). Pour cela, l'attribution d'une paire de clés à chaque utilisateur va permettre de bien protéger le ToT vis-à-vis d'attaquants externes ou d'utilisateurs malveillants, en le chiffrant après signature avec la clé publique relative à chaque utilisateur et assuré que lui seul serait en mesure de le déchiffrer.

De plus, il est intéressant de doter le ToT d'une durée de validité qui permettra de le renouveler seulement à l'expiration de cette durée. Dans ce cas, une date d'expiration est nécessaire. A l'envoi du ToT, la durée de validité est incluse et est validée à la réception.

4.4.4. Algorithme d'authentification anonyme proposé

Initialization:

CA: Certificate Authority
U: User who owns a public key $\mathbf{K_{U+}}$/ private key $\mathbf{K_{U-}}$ of encryption obtained from CA
RM: **R**egistration **M**anager on listening which owns a public key $\mathbf{K_{RM+}}$ / private key $\mathbf{K_{RM-}}$ obtained from CA
a public key $\mathbf{KS_{RM+}}$ / private key $\mathbf{KS_{RM-}}$ obtained from CA
TM: **T**icket **M**anager on listening which owns a public key $\mathbf{K_{TM+}}$/ private key $\mathbf{K_{TM-}}$ obtained from CA
SM: **S**ervices **M**anager on listening which owns a public key $\mathbf{K_{SM+}}$/ private key $\mathbf{K_{SM-}}$ obtained from CA
Attributes U = {Name, Organization, e-mail, Address}
ToT: Ticket of Ticket
n: a nonce to ensure a fresh ToT
Hash (m): Hash function applied to the message m
(N, e): RSA public key of signature of TM relative to blind signature obtained from CA
(N, d): RSA private key of signature of TM relative to blind signature obtained from CA

Repeat
U sends its attributes to RM
RM sends the SLA + the Privacy Policy
U chooses the Privacy Policy desired + level of anonymity required
RM:
Creates the Adaptive Privacy Policy relative to U
Generates Contract {U} as a proof of join
Generates (ToT, n) as a proof of registration
RM signs (ToT, n) with his private key KS_{RM-}
RM encrypts [(ToT, n) KS_{RM-}] with the public key K_{U+} of U
RM sends Contract {U} + [(ToT, n) KS_{RM-}] K_{U+}
U:
U decrypts the message [(ToT, n) KS_{RM-}] K_{U+} with his private key K_{U-}
U decrypts the message of the previous step with the public key of signature of RM KS_{RM+} included in the certificate
U encrypts (ToT, n) with the public key of encryption of RM K_{RM+}
U sends a Circuit Request to RM + (ToT, n) K_{RM+}
RM:
RM decrypts the message (ToT, n) K_{RM+} with his private key K_{RM-}
if U has invalid **ToT** or invalid nonce **n then**
RM rejects the request from U
else
RM sends a list of Nodes (IP addresses of nodes) and provides to U public keys K_{Nodes} (the most available)
U:
U chooses a number of available Nodes (in general 3 Nodes)
U validates keys K_{Nodes} with the CA

repeat
if any key fails validation by the CA **then**
U revokes the invalid key and chooses another node
end if
Until all keys are valid

end if

U performs anonymous circuit construction over the Nodes using K_{Nodes} to generate session symmetric keys
U sends an Access Ticket Request in layered encryption format over the anonymous circuit of the previous step to TM + (ToT, n) K_{RM+}
TM:
TM Checks the validity of the ToT with RM which returns Valid / Invalid to TM
If Valid ToT **then** RM sends Valid to TM
else RM sends Invalid to TM
end if
If U has an Invalid (ToT, n) **then** TM rejects the Request of U
else TM sends his Validation over the anonymous circuit to U
end if

U:
U generates a random message **m**
U generates a number **r** prime with **N**
U Computes: Blind (m) = Hash (m). r^e (Mod N)
U Sends Blind (m) to TM
TM:
TM Computes signature S' for Blind (m) via his RSA private key of signature: S' = Blind (m)^d (Mod N)
TM Sends S' to U
U:
U Computes: S = S'. Inverse (r) ⇔ Access ticket relative to U
U sends a service consumption request to access resources in layered encryption format over the anonymous circuit to SM
SM:
SM forwards an authentication request
U:
U Encrypts the pair: (m, S) with the public key of encryption of TM K_{TM+} and sends it as credentials of authentication process to SM
SM:
Checks the validity of (m, S) K_{TM+} with TM which returns Valid / Invalid to SM
If the pair (m, S) is valid **then** TM sends Valid to SM
else TM sends Invalid to SM
end if
If U has an Invalid Access Ticket **then** SM rejects the Request to access services of U
Authentication then fails and SM discards the service consumption request
else SM returns his acceptation and sends Valid to U
end if
U:
U encrypts (SID) with K_{SM+} and sends the service ID required over the anonymous circuit to SM
U starts anonymous consumption of the Cloud service

Until there is Users

4.4.5. Modèle étendu : modèle de l'adversaire

Dans le modèle de l'adversaire, nous avons déjà classifié les informations sensibles ainsi que les entités pouvant les percevoir/exploiter. Par conséquent, nous pouvons illustrer le modèle étendu par la matrice précédente telle que toutes les cases prennent zéro comme valeur précisément la ligne de l'adresse IP des utilisateurs. La matrice ci-dessous illustre le cas du modèle étendu (voire table 3.3):

Informations Sensibles / Types de Menaces	**Interne**				**Externe**	
	CSP	Employées Malicieux dans le CSP	TTP	Utilisateurs Malicieux	Attaquants Passifs	Attaquants Actifs
Identité Utilisateurs	0	0	0	0	0	0
IP Utilisateurs	**0**	**0**	**0**	**0**	**0**	**0**
Données Utilisateurs	0	0	0	0	0	0
Identité/données	0	0	0	0	0	0
Identité/SID	0	0	0	0	0	0

Table 3.3 Modèle de l'adversaire relatif au modèle étendu

5. Synthèse et contribution

La contribution principale dans notre approche était de proposer un système d'authentification anonyme adaptative aux exigences, en matière de protection des données personnelles de chaque utilisateur dans l'environnement Cloud.
L'authentification proposée permet au CSP d'offrir deux niveaux d'anonymat, s'adaptant ainsi aux exigences de privacy des utilisateurs potentiels.
Le premier niveau consistait à permettre aux utilisateurs d'être anonymes grâce à une consommation des services via des tickets anonymes.
Le deuxième offre à son tour, l'ajout de l'anonymisation de la communication elle-même, ce qui offre un niveau plus élevé d'anonymat pour les utilisateurs désirant une privacy optimale.
La spécificité de chaque niveau est de pouvoir s'adapter également aux différents choix des utilisateurs, qui peuvent paramétrer et affiner leur politique de protection de leurs données personnelles.

Le point crucial et important était de faire participer les utilisateurs eux-mêmes comme des nœuds volontaires, pour acheminer les communications, ce qui réduira ou écartera le cas où seuls les nœuds du CSP acheminent les communications. Ces derniers peuvent par conséquent, s'entendre et essayer de corréler le trafic pour rompre l'anonymat du système. Ayant à la fois un accès physique aux machines (les nœuds mis en œuvre en machines physiques ou virtuelles) et un contrôle global sur elles, le CSP peut potentiellement inspecter la mémoire et l'espace de stockage de n'importe quel nœud. Notre manière de procéder a permis donc d'être indépendant de la notion de confiance qui exige un certain niveau de loyauté pour l'assurance de l'anonymat des utilisateurs.

L'avantage majeur de notre approche est que même si les différents Managers communiquent, la divulgation de l'identité de l'utilisateur ou sa traçabilité reste difficile à réaliser.

Notre approche assure donc:

- **L'Anonymat ou la préservation de la Privacy:** Chaque utilisateur demeure anonyme lors de sa consommation des différents services Cloud. L'identité et l'adresse IP de l'utilisateur sont cachées. Cela permet de rendre difficile toute corrélation entre un utilisateur et ses données en transit/stockées dans le Cloud, ainsi que la correspondance entre un utilisateur et les services qu'il consomme.

- **La Non chaînabilité**: Les sessions de l'utilisateur vers les services Cloud sont difficiles à corréler. Personne (inclut le CSP lui-même) n'est en mesure de relier deux ou plusieurs sessions entre un certain utilisateur U et le CSP. Un cas spécifique se présente, est quand il existe une collaboration potentielle entre les nœuds du circuit (notamment The Entry Node « Nœud d'entrée » et l'Exit Node « Nœud de sortie »). La parade étant expliquée dans l'approche 'étape Construction des circuits anonymes'.

- **L'Intraçabilité:** Le CSP ainsi que les autres utilisateurs ne sont pas en mesure de retracer l'authentification d'un utilisateur et sa communication concrète. De même que la non chaînabilité, il pourrait exister une collaboration entre les nœuds du circuit (les extrémités). La parade pour surpasser une telle situation étant la même citée précédemment.

- **La Confidentialité:** La session de chaque utilisateur vers le CSP est confidentielle. Personne n'est en mesure d'obtenir les données transmises entre U et le CSP, car les communications sont encapsulées et envoyées via le circuit anonyme préalablement construit.

- **L'Intégrité:** Les données envoyées dans la session de l'utilisateur ne peuvent pas être modifiées grâce à leur passage par le circuit anonyme (encapsulation et chiffrement).

- **L'Authentification est mutuelle :** L'authentification proposée étant mutuelle car chaque gestionnaire possède un certificat qui confirme la validité de sa clé publique et est signé par un organisme de confiance CA « *Autorité de Certification* ». Les utilisateurs peuvent s'assurer que la clé publique qu'ils utilisent est bien la clé publique du gestionnaire avec lequel ils veulent communiquer et non celle d'un intrus. Ils peuvent ainsi être sûrs que l'entité avec laquelle ils communiquent est bien l'un des gestionnaires.

Il est à noter que :

- La séparation des fonctions d'enregistrement et d'authentification en les confiant à des entités distinctes (différents gestionnaires) est bénéfique quant à la perspective d'amélioration de la privacy. Cette séparation permet de limiter les actions de traitement des données à caractère personnelle et à restreindre leur disponibilité uniquement pour des tâches précises. En raison de l'efficacité de la signature en aveugle, le Registration Manager RM et le Ticket Manager TM peuvent être assimilés dans la même entité nommée « Registration and Ticket Manager RTM », car il n'existe aucun lien entre le ticket initial généré à savoir le ToT et le ticket d'accès anonyme. Cela va permettre d'optimiser les modèles proposés en termes d'accès, notamment lors de la phase de déploiement.

- Le niveau d'anonymat offert par notre modèle augmente autant que le nombre d'utilisateurs participant en tant que nœud du circuit anonyme croît. La diversité des utilisateurs est une composante importante : plus la base d'utilisateurs est nombreuse et variée, meilleure est la protection de l'anonymat.

6. Conclusion

La protection des données personnelles « privacy » est une problématique importante et non négligeable dans un environnement Cloud, tant en termes de conformité légale et du niveau de confiance de l'utilisateur vis-à-vis du Cloud. La protection des données personnelles doit donc être considérée à chaque phase de la conception, notamment dans un environnement de Cloud Computing.
Cependant, un focus automatique lors de l'utilisation des services Cloud est la présence d'un bon mécanisme d'authentification. La puissance de ce système d'authentification est relative au besoin de protection des données personnelles réclamé par les utilisateurs (niveau de privacy désiré).

De ce fait, les garanties qui doivent être fournies à l'utilisateur Cloud afin qu'il soit convaincu que ses informations soumises soient bien protégées sont : la maximisation du contrôle individuel, la création de services anonymes et la limitation des informations d'identité PII. Du point de vue du CSP, il doit y avoir un maintien de l'anonymat des informations personnelles, un chiffrement des données si elles contiennent des informations personnelles, la dissociation entre le traitement et le stockage des données et la gestion explicite des exigences de la privacy.

Notre objectif était donc, de proposer une authentification anonyme adaptative aux exigences de privacy des utilisateurs Cloud **(politique adaptative de protection des données personnelles)**. Cette proposition considère deux modèles pouvant être adopté par les Cloud Services Provider:

- Un modèle de base assurant une consommation anonyme des services via des tickets anonymes générés lors de chaque requête de consommation de services.

- Un modèle étendu qui est une extension du modèle de base, permettant une authentification anonyme optimale car les informations fournies par l'utilisateur ne contiendront aucune information qui pourrait révéler son identité même son adresse IP. La nouvelle particularité de ce modèle, était d'impliquer les utilisateurs eux-mêmes en tant que nœuds volontaires pour acheminer les paquets.

L'introduction de cette nouvelle combinaison élimine la notion de confiance au CSP. Cela permet donc aux utilisateurs de consommer en toute sécurité les services Cloud, tout en étant indépendants de la notion de confiance qui nécessite un certain niveau de loyauté pour l'assurance de l'anonymat des utilisateurs, comme c'est le cas dans la majorité des systèmes.

Dans le prochain chapitre, nous allons décrire les étapes de validation et d'implémentation du modèle de base constituant l'approche proposée.

Chapitre 4: Validation et Implémentation du Protocole

1. Introduction

Après le fondement théorique de l'approche proposée, qui consistait à assurer une authentification anonyme via un protocole d'authentification permettant aux utilisateurs, d'accéder aux services Cloud tout en préservant leur privacy. Ce chapitre a donc pour but de présenter la validation du protocole proposé ainsi que l'implémentation d'un prototype.
La protection des données personnelles (privacy) étant un élément de base dans le protocole proposé, une discussion à propos des propriétés d'anonymat et de l'assurance de la non divulgation des informations personnelles des utilisateurs notamment leur identité, a été présentée dans la proposition de l'approche. La validation étant une étape primordiale lors de la proposition d'un protocole de sécurité (dans notre cas d'authentification anonyme), cela pour assurer le bon fonctionnement du protocole notamment, en ce qui concerne le cheminement des étapes concrétisées via les différentes transitions allant de l'enregistrement jusqu'à l'accès aux services Cloud.
Cette validation va être réalisée via un outil de vérification et de validation de protocoles de sécurité choisi pour effectuer l'analyse du protocole. L'analyse en question va concerner la sécurité des échanges et des secrets échangés, cela face aux différents modèles d'adversaires pouvant être présent lors de l'exécution du protocole en question (adversaire passif ou actif, interne ou externe).

Le bon déroulement d'une communication entre plusieurs participants repose sur la formalisation commune que constitue le protocole utilisé. Ce dernier, décrit l'ordre selon lequel les messages peuvent être envoyés par les différents participants, ainsi que la structure des messages échangés. Un protocole qui utilise des primitives cryptographiques : comme des fonctions de chiffrement ou de hachage, pour sécuriser la communication est lui-même dit cryptographique. **[73]**

Ce chapitre va donc illustrer d'une manière détaillée les deux phases complémentaires de validation puis d'implémentation de notre protocole nommé « AnonCloud ». En premier, nous décrirons la validation du cheminement ainsi que la sécurité des échanges de secrets entre l'utilisateur et les différents Managers. Puis, nous présenterons le prototype implémenté à travers le langage java et les sockets et exposerons les différentes interfaces et interactions entre les différentes entités.

2. Vérification et Validation du protocole AnonCloud

2.1. Du modèle formel à l'automatisation

L'automatisation des méthodes de vérification permet de prendre en compte un attaquant ayant des possibilités plus étendues. Une faille peut exploiter un nombre important d'étapes de communication et est donc difficile à trouver manuellement : un outil automatique sera donc nécessaire.

L'utilisation d'outils de vérification automatique de protocoles permet donc de prouver certaines propriétés de sécurité exprimées de manière formelle. Il est le plus souvent nécessaire d'assurer certaines propriétés de sécurité sur les protocoles conçus, par exemple, assurer qu'un message sensible ne peut pas être lu par quelqu'un d'autre que la personne à qui il est destiné. De nombreux outils de vérification ont été conçus dans ce but, l'enjeu est de rendre automatique la preuve de telles propriétés et d'exhiber des traces d'attaques lorsqu'une propriété est mise en défaut (prouver qu'elle est vulnérable).

En l'occurrence, le protocole NSPK proposé par Needham et Schroeder en 1978 **[97]** dont le but était d'utiliser la cryptographie à clés publiques pour établir une clé de session K commune entre deux rôles A et B, a été démontré sûr après vérification en 1990 par Burrow, Abadi et Needham en utilisant la logique BAN **[98]**. Hors, En 1996, Lowe trouve une attaque au moyen de son vérifieur FDR et le protocole était donc vulnérable à une attaque MITM (man in the middle), d'où la naissance de l'automatisation. **[74]**

2.2. Outil utilisé lors de la validation du protocole AnonCloud

Conformément à la figure 4.1, le but de l'utilisation d'un outil de vérification de protocoles est de pouvoir répondre à la question : *Y-a-t-il des vulnérabilités dans ce protocole ?* **[74]**

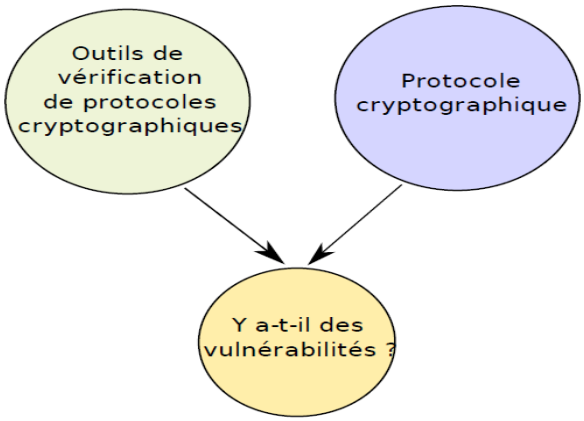


Figure 4.1 Objectif de la vérification automatique d'un protocole

Afin de vérifier et d'analyser le protocole proposé, nous avons utilisé un outil automatisé de vérification de sécurité des protocoles à savoir l'outil Scyther **[75]**.

Scyther: est un outil écrit en langage Python, créé par Cas Cremers à but principalement pédagogique. C'est un des outils de vérification de protocoles cryptographiques les plus rapides et les plus conviviaux à utiliser qui permet de trouver les failles et de prouver la sécurité des protocoles **[75]**.
Scyther permet de définir un protocole en fonction des rôles de ses participants. Les points forts de Scyther étant sa lisibilité d'entrée (le code) et sa lisibilité de sortie (graphe). En outre, Scyther est multi plateformes disponible pour Windows, Linux et Mac OS. La figure 4.2 montre l'interface principale de l'outil.

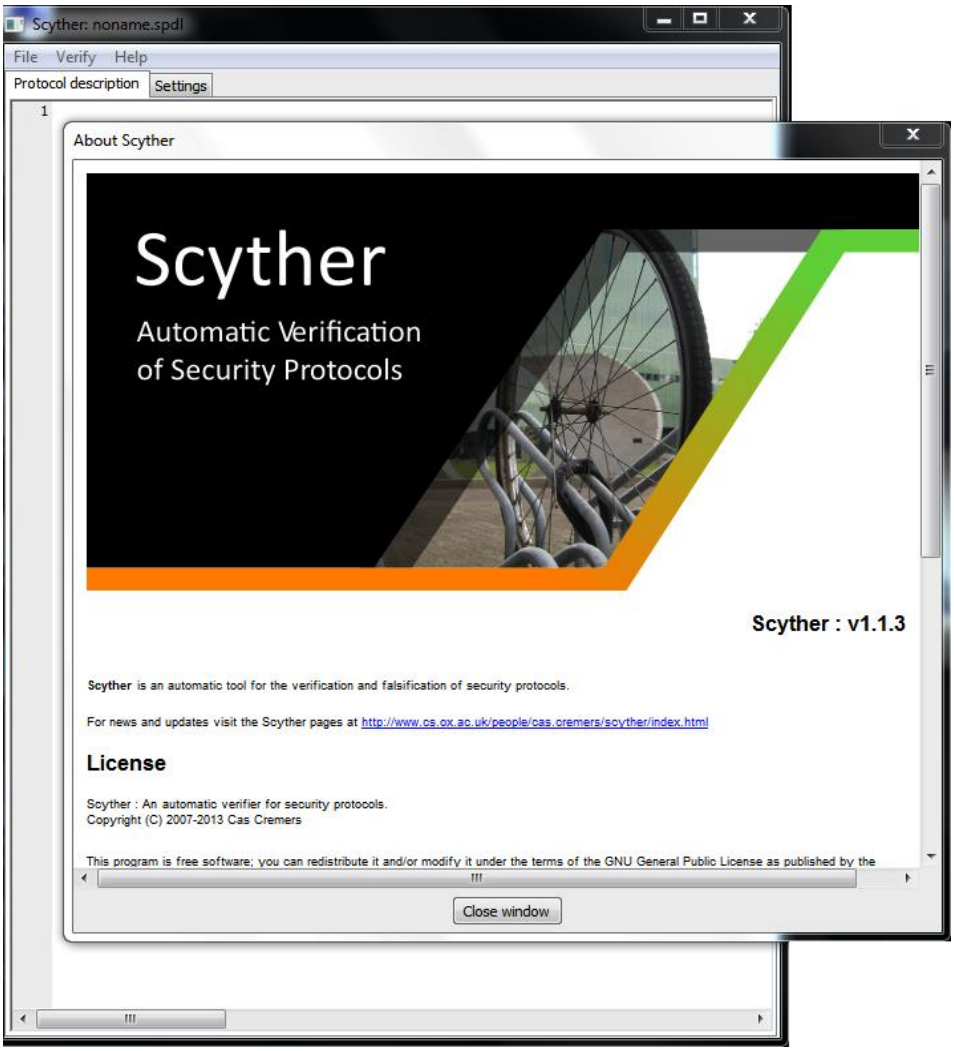


Figure 4.2 Interface de l'outil Scyther

Scyther constitue donc un Framework pour la vérification automatique des protocoles de sécurité. Afin de construire un modèle dans Scyther, nous devons définir les rôles du protocole. Le rôle dans un modèle Scyther décrit la fonctionnalité d'un participant dans le protocole. Notre modèle aura donc à considérer trois rôles, l'utilisateur et les deux Managers RTM « **R**egistration and **T**icket **M**anager » et SM « **S**ervices **M**anager ». Lors de la vérification, chaque agent assume un rôle et agit en fonction de la définition du rôle assumé.

Scyther permet de tester automatiquement les modèles de protocole contre une famille de modèles d'adversaires. Les adversaires peuvent révéler les différents états de sécurité lors de l'exécution du protocole. Mener une telle analyse avancée d'un protocole, aide à mieux comprendre ses propriétés de sécurité. En particulier, les tests effectués contre des adversaires aident à identifier les limites de la sécurité du protocole analysé. **[76]**

Scyther réalise la vérification automatique de protocoles de sécurité via son algorithme de vérification. Les revendications (claims) représentent les connaissances d'un émetteur et d'un récepteur et également l'objectif d'un éventuel adversaire (généralement un intrus). La cryptographie symétrique et asymétrique et les fonctions de hachage sont aussi supportées par Scyther. **[77]**

Nous avons effectué nos expériences en utilisant la dernière version stable de l'outil de vérification automatique de protocoles Scyther, sortie en Avril 2014 **[78]** à savoir la version 1.1.3.

Scyther, à un niveau élevé, fonctionne comme suit:

- Lorsqu'une description de protocole est introduite en entrée, il en déduit le comportement des agents dans le contexte de présence d'un adversaire. Il explore ensuite l'espace d'états dans ce système et vérifie un nombre d'exécutions en utilisant une recherche sur la base de modèles. **[75]**
- Lorsque Scyther explore le système, il peut établir qu'une certaine propriété est conservée par le système ou que cette dernière est fausse. Son résultat sera alors un modèle d'attaque contre la propriété en question. **[79]**

Il s'agit donc de fournir un modèle ou une description formelle en entrée spécifiant la description du protocole en utilisant un langage spécifique à savoir le langage SPDL **«S**ecurity **P**rotocol **D**escription **L**anguage**»**, ainsi que la description des différentes propriétés de sécurité à vérifier.
Comme illustré dans la figure 4.3, l'outil permettra de trouver les failles en appliquant un algorithme de vérification.

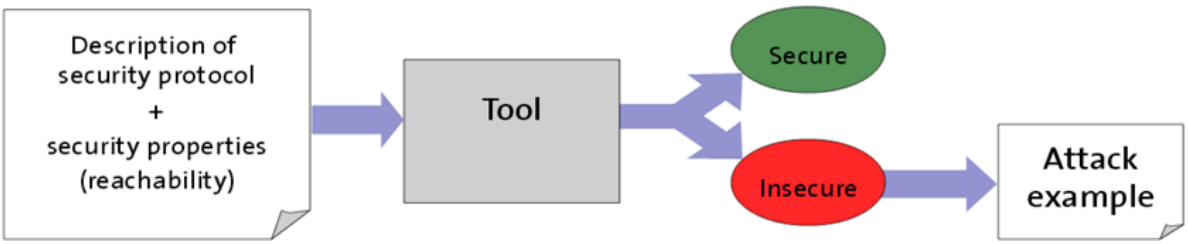


Figure 4.3 Façon de procéder de l'outil Scyther

La sortie de l'outil Scyther consiste à dire si le protocole est sécurisé à travers la description fournie ainsi que la vérification des propriétés de sécurité qui dans le meilleur cas, elles n'auront engendré aucune faille. Dans le cas échéant, où le protocole n'est pas sécurisé, un exemple d'attaque trouvée sera fourni sous forme de graphe. Les failles ou vulnérabilités recensées sont en termes d'attaques connues à savoir:

- Attaques liées à la logique du protocole : différentes transitions et échanges effectués, surtout quant au cheminement proposé.

- Attaques liées à la faiblesse de la cryptographie (primitives cryptographiques) utilisée pour assurer la sécurité du protocole.

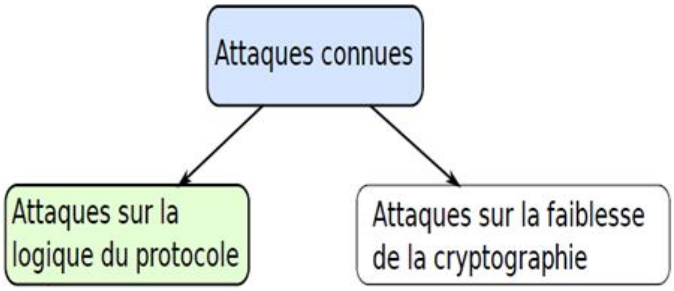


Figure 4.4 Types d'attaques recensés lors de la vérification d'un protocole

Pour visualiser la sortie graphique de Scyther, un outil graphique à savoir **Graphviz** est nécessaire **[80]**. Il permet de représenter graphiquement des graphes, conçu par une équipe de laboratoires de recherche American «Telephone & Telegraph». Cette application convient à la représentation de graphes très denses comprenant un très grand nombre de nœuds grâce à des algorithmes puissants. L'outil est très rapide à l'exécution et le rendu est optimisé afin que les liens ne recouvrent pas les nœuds et ne se croisent pas.

2.3. Modèle de l'adversaire

La vérification d'un protocole cryptographique constitue un problème indécidable et la vérification d'absence d'attaques est un problème complexe, car :

- Le nombre de sessions est non borné.
- Le nombre de participants est non borné.
- La taille des termes utilisés (variables, constantes, etc.) est non bornée.

Plusieurs approches de résolution se présentent : **[74]**

- Borner le nombre de sessions: le problème devient NP-complet.
- Utiliser des approximations: le problème reste indécidable, ce qui revient donc à essayer de:
  - Prouver la propriété,
  - Trouver une attaque,
  - La propriété ne peut pas être prouvée.

Conformément à la figure 4.5, ces deux approches de résolution sont utilisées par l'outil Scyther:

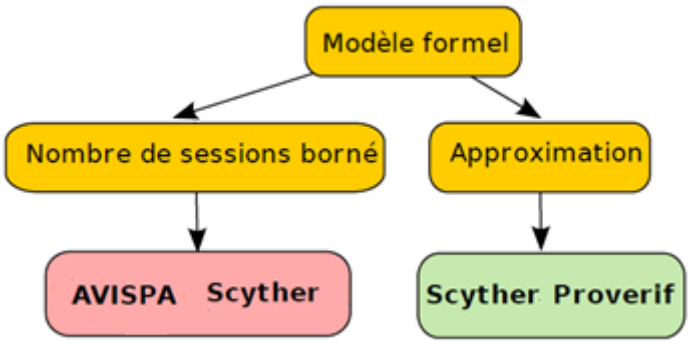


Figure 4.5 Approches de résolution utilisées par Scyther

Concernant les types d'attaquant possibles, l'attaquant peut être passif ou actif: **[81]**

- **Attaquant passif :** Il ne peut interagir avec le protocole et peut juste intercepter et analyser les messages qui ont circulé.

- **Attaquant actif :** Il contrôle le réseau : peut intercepter, détruire et falsifier les messages, ou même être un agent du protocole (participant malhonnête).

En 1983, Dolev et Yao ont proposé les bases d'un modèle de l'adversaire réseau, qui est actuellement le plus largement utilisé. Ce modèle sert de fondement à l'étude des protocoles cryptographiques **[82]**.

Le modèle de Dolev-Yao consiste à simplifier le modèle de communication entre principaux, en prenant en compte la quasi-omnipotence des intrus. Nul n'est besoin de préciser le modèle de communication (files, réseaux avec ou sans panne, avec ou sans perte, etc.) entre principaux : l'intrus pouvant espionner et dérouter toutes les lignes de communication, toute communication d'un message M entre deux principaux peut être simulée par un envoi de M à l'intrus, suivi d'un envoi de M par l'intrus au destinataire souhaité. Etant donné que l'intrus peut simuler n'importe quel envoi et réception de message, le modèle de communication est simplifié, en supposant que tout message envoyé est envoyé à l'intrus et tout message reçu peut provenir de l'intrus.

En second lieu, le modèle de Dolev-Yao suppose que les messages envoyés et reçus ne sont ni des nombres ni des suites de bits, mais des éléments d'une algèbre de termes, éventuellement modulo une théorie équationnelle. Les messages sont engendrés par une grammaire de la forme :

$$M ::= D \mid K \mid pair\ (M, M) \mid p_1\ (M) \mid p_2\ (M) \mid encrypt\ (M, K) \mid decrypt\ (M, K)$$

Où : D parcourt un ensemble de données de base (entiers, réels, etc.),
K parcourt un ensemble de clés,
pair (M_1, M_2) est le couple formé de M_1 et de M_2,
p_1 (M) récupère la première composante du couple M,
p_2 (M) récupère la deuxième composante du couple M,
encrypt (M, K) chiffre le message M avec la clé K,
decrypt (M, K) déchiffre le message chiffré M à l'aide de la clé K.

Nous avons alors la théorie équationnelle :

$$p_1\ (pair\ (M_1, M_2)) = M_1$$
$$p_2\ (pair\ (M_1, M_2)) = M_2$$
$$decrypt\ (encrypt\ (M, K), K) = M$$

En particulier, toute tentative de déchiffrer $\{M\}_K$ (codé par encrypt (M, K)) en utilisant une clé K' différente de K, fournit un terme de la forme : decrypt (encrypt (M, K), K') qui est prouvablement différent de M dans la théorie équationnelle ci-dessus.

Troisièmement, le modèle de Dolev-Yao représente l'intrus comme un système déductif, qui représente tous les messages qu'un intrus peut fabriquer par un ensemble de règles, qui définissent un prédicat E $\vdash$ M (à partir de l'ensemble de messages E, l'intrus peut fabriquer le message M): **[99]**

1. E, M $\vdash$ M : de tout ensemble E de messages augmenté d'un message M, l'intrus peut inférer M (rejeu simple).
2. Si E $\vdash$ M_1 et E $\vdash$ M_2, alors E $\vdash$ pair (M_1, M_2) : l'intrus peut fabriquer tous les couples de messages formés de messages qu'il peut fabriquer.
3. Si E $\vdash$ M alors E $\vdash$ p_1 (M) et E $\vdash$ p_2 (M) : l'intrus peut extraire les composantes des couples.
4. Si E $\vdash$ M et E $\vdash$ K alors E $\vdash$ encrypt (M, K) : l'intrus peut effectuer tous les chiffrements qu'il souhaite.
5. Si E $\vdash$ M et E $\vdash$ K alors E $\vdash$ decrypt (M, K) : l'intrus peut tenter de déchiffrer tout message avec toute clé qu'il sait fabriquer.
6. Si E $\vdash$ M et M=N, alors E $\vdash$ N.

Dans le modèle de Dolev-Yao, l'intrus possède donc un contrôle complet sur le réseau de communication. L'intrus peut intercepter n'importe quel message et également insérer n'importe quel message, tant qu'il est en mesure de construire son contenu à partir des connaissances qu'il possède. Les variantes couramment utilisées du modèle Dolev-Yao, incluent implicitement des agents qui collaborent.
Dans le modèle relatif à Scyther, la notion d'agents qui collaborent est explicite, ce qui permet un calcul systématique de la connaissance initiale de l'intrus.
Les modèles d'intrus, qui sont plus faibles que le modèle de Dolev-Yao, sont également un élément d'intérêt lors par exemple de l'étude des piles de protocoles ou de supports de communication particulière comme les communications sans fil.

Enfin, pour résumer, dans le modèle de l'adversaire considéré dans Scyther, il y a eu :

- Premièrement, l'intégration de la possibilité que le réseau soit partiellement ou totalement sous le contrôle d'un intrus.
- Deuxièmement, il peut y avoir des agents qui collaborent entre eux ou la présence d'un agent compromis par un intrus.

2.4. Propriétés de sécurité

Les propriétés qui existent dans les protocoles cryptographiques sont nombreuses, deux grandes classes de propriétés se distinguent : les propriétés dites «de secret», qui s'intéressent à l'ensemble des agents ayant connaissance d'un message, ainsi que les propriétés «d'authentification» dont la vocation est d'assurer la cohérence de l'exécution du protocole avec les attentes de chacun des agents qui l'exécute vis-à-vis des autres agents et des messages reçus **[73]**.

2.4.1. Cas des propriétés de secret

L'une des propriétés les plus connues est la propriété de secret. Elle se décline souvent en plusieurs versions. Intuitivement, le secret d'une donnée *S* est assuré dans un protocole quand il n'existe aucun moyen pour l'intrus de connaitre *S* (en clair, non chiffré). Par exemple, le protocole minimaliste où *Alice* envoie à *Bob* un message secret *M* chiffré par la clé publique de *Bob* assure naturellement le secret de *M*, puisque l'intrus ne peut pas décrypter le message transmis. La plupart du temps, cette notion de secret est amplement suffisante. Cependant, elle repose sur le fait que l'intrus ne peut pas énumérer toutes les valeurs de *M*, de même qu'il ne peut pas énumérer toutes les valeurs d'une clé. **[100]**

Selon **[74]**, Un protocole préserve le secret de K si un adversaire ne peut jamais obtenir K en le construisant à partir des sorties du protocole.

$$\exists \{\alpha_i\}_i, p \rightarrow \dots \rightarrow 0 : \alpha_1 \dots \alpha_n \vdash K$$

$\{\alpha_i\}_i$ sont les sorties du protocole lors des transitions

2.4.2. Cas des propriétés de l'authentification

Les propriétés de l'authentification sont classées selon la hiérarchie de Gavin Lowe de la plus faible propriété à la plus forte **[84]**, faisant suite aux travaux de Woo et Lam sur les claims de correspondance **[85]**. Ces propriétés sont :

1. La Vitalité
2. L'Accord faible
3. L'Accord (sur une liste de termes S)

- **Vitalité « Aliveness »**
  Si un participant A exécute le protocole en pensant qu'il l'effectuait avec un participant B, alors B a précédemment exécuté le protocole. Notons que B n'a pas nécessairement la certitude d'avoir exécuté le protocole avec A.

- **Accord faible « Weakagreement »**
  En plus de la vitalité, B admet qu'il est en train de communiquer avec A.

- **Accord sur une liste de terme S «agreement»**
  En plus de l'accord faible, A et B sont d'accord sur les valeurs incluses dans une liste S.

2.5. Script d'entrée

Afin de mieux éclaircir la compréhension du lecteur quant au script d'entrée relatif au protocole proposé, cette section va d'abord expliquer les notations du langage d'entrée employé par l'outil Scyther. Une représentation des propriétés de sécurité considérées sera ensuite présentée.

2.5.1. Notations

Le langage d'entrée de Scyther à savoir le langage SPDL, s'inspire de la syntaxe des langages C / Java. Le but principal de la présence de ce langage est de pouvoir décrire les protocoles, qui sont définis par un ensemble de rôles. Les rôles, à leur tour, sont définis par une séquence d'événements, dont la plupart sont des événements qui dénotent l'envoi ou la réception de termes. **[83]**

- Un protocole est donc un ensemble fini de rôles.
- Un rôle est une suite finie d'actions d'un participant légitime.
- Action = envoi ou réception d'un message.
- Un message est modélisé par des symboles : termes.
- Termes : variables, constantes, nonces, etc.
- Les revendications (claims) qui apparaissent dans les rôles sont la définition des propriétés de sécurité à assurer notamment les secrets.

Notons que:

- La représentation de l'envoi et de la réception des messages est effectuée avec les mots clés send_i et recv_i qui prennent en paramètres les deux rôles intervenant dans l'échange décrit.
- Le label i indique que les deux évènements sont reliés, c'est-à-dire qu'à chaque envoi d'un message dans le protocole, correspond une réception du même message.
- Parmi les types de variables disponibles, les nonces, les agents et les clés, ainsi que des types définis par l'utilisateur.
- Les variables qui sont générées par les agents sont déclarées avec le mot clé fresh, les autres sont définies avec le mot clé var.

- La syntaxe générale pour la vérification d'une propriété est : claim (rôle, propriété, options). Par exemple claim (R, Secret, N) permet d'indiquer le secret de N dans le rôle R où N par exemple est un nonce.

  Quant aux clés, dans le cas de notre protocole AnonCloud:
- Chaque utilisateur possède une paire de clé (pk, sk) pour le chiffrement.
- Le Manager RTM possède deux paires de clé asymétriques (pke, ske) pour le chiffrement et respectivement (pk, sk) pour la signature.
- Le Manager SM ne possède qu'une paire (pk, sk) dédiée principalement à la signature.
- En outre, deux clés symétriques (SK pour Session Key) ont été rajoutées respectivement entre l'utilisateur et le Manager RTM et également entre l'utilisateur et le Manager SM, dans le protocole à vérifier (protocole proposé dans la contribution).
  Ces clés ont permis de protéger la session entre l'utilisateur et RTM lors de la génération du ticket d'accès anonyme ainsi que la protection des communications lors de l'authentification (via les tickets anonymes générés préalablement) afin de se protéger contre les attaques MITM décelées par l'outil lors de la vérification du protocole AnonCloud et expliquées dans la section 2.6.

Pour résumer, l'outil Scyther étant utilisé à des fins de vérification de protocoles, le détail du script Scyther est une liste d'instructions écrites en langage SPDL, qui sont constituées d'un ensemble de déclarations globales et la description elle-même du protocole (différents rôles).

2.5.2. Propriétés de sécurité considérées

Dans Scyther, les propriétés à vérifier apparaissent dans les revendications déclarées (claims) qui sont en nombre de quatre, nommées dans Scyther par **[84]**:

- *Alive* pour la vitalité.
- *Weakagree* pour l'accord faible.
- *Niagree pour* « Non injective agree » : l'accord qui assure la correspondance sur le contenu de tous les messages échangés, mais qui permet qu'un message puisse être reçu avant qu'il ne soit envoyé.
- *Nisynch* pour « Non injective Synchronisation » : la synchronisation exige que les envois et réceptions des messages doivent être exécutés dans l'ordre attendu, un message doit être envoyé avant qu'il ne puisse être reçu.
- Dans la spécification relative au secret, nous écrivons : **claim_I1 (I, Secret, k1)**.
  claim_I2 (I, Secret, k2).
  etc.

2.5.3. Le script AnonCloud

Le script ci-dessous décrit les variables, les rôles et les claims pour tous les composants (dans notre cas les Managers) du protocole AnonCloud relatif au modèle de base proposé dans la contribution. Nous pouvons examiner le flux du protocole et la communication entre tous les Managers à partir du script Scyther.

Le code est simple à comprendre car il est constitué d'une liste d'évènements d'envois et de réceptions, suivi d'une liste de propriétés à vérifier. De la même manière pour tous les composants, les rôles et les claims ont été définis un par un dans le script à exécuter.

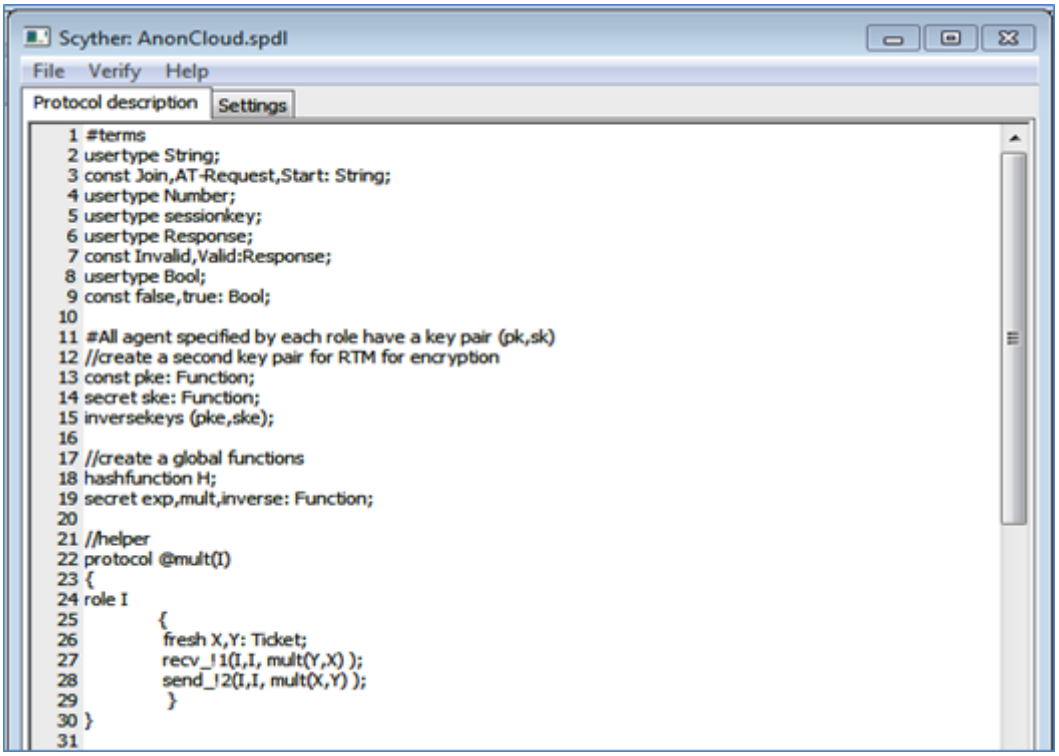


Figure 4.6 Script Scyther : déclarations globales

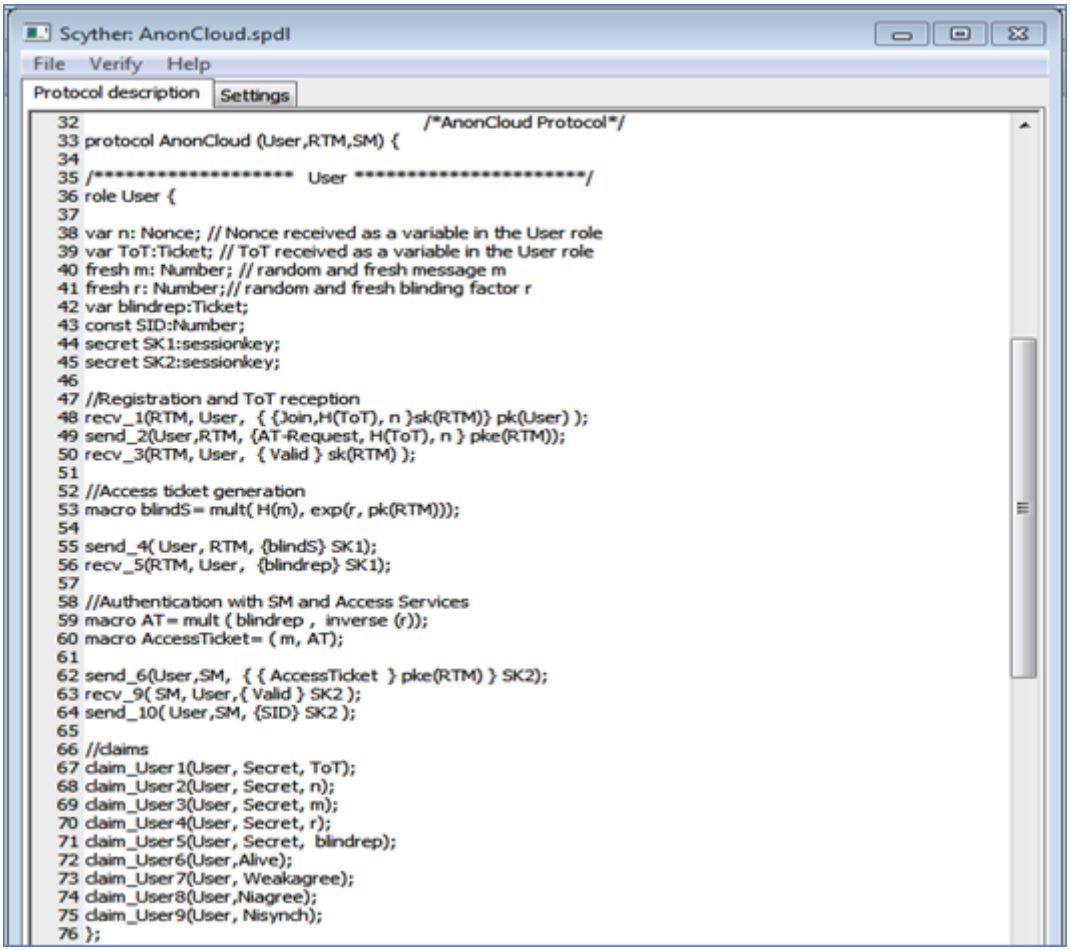


Figure 4.7 Script Scyther : rôle Utilisateur

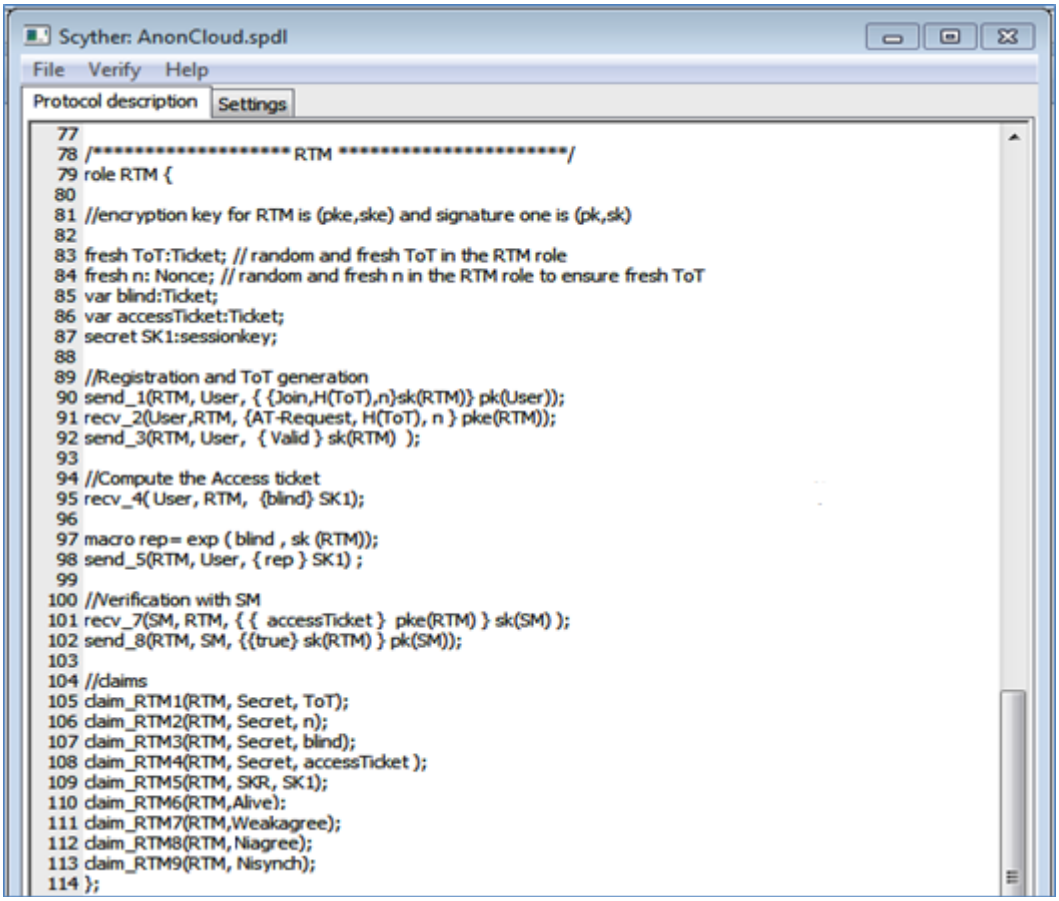


Figure 4.8 Script Scyther : rôle RTM

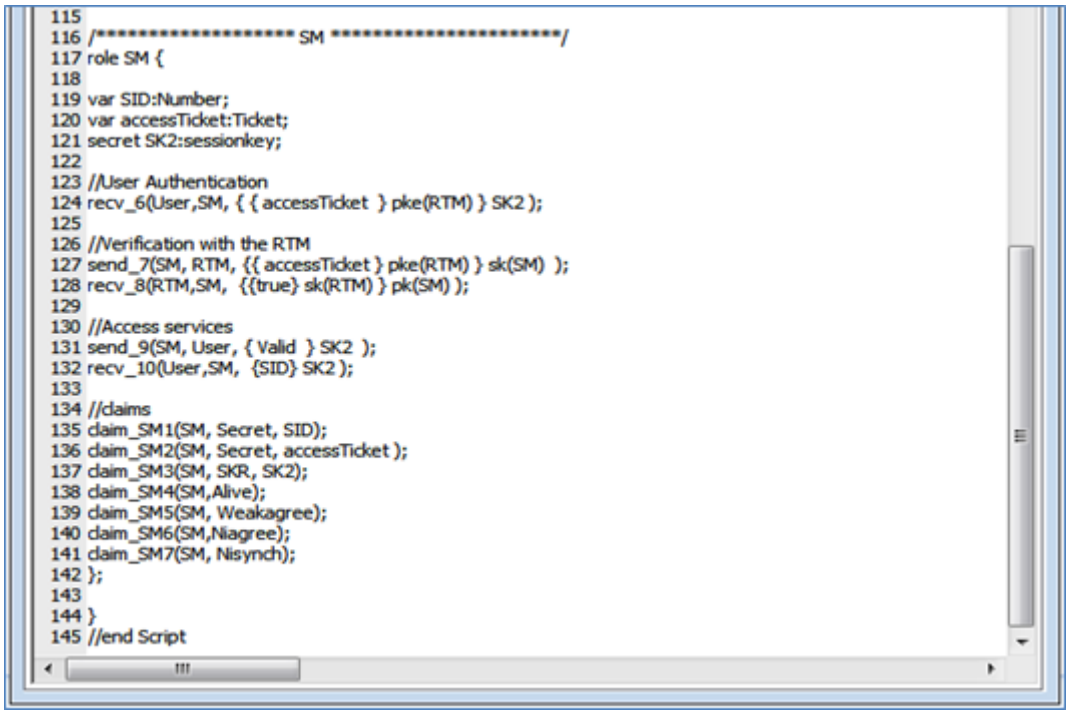


Figure 4.9 Script Scyther : rôle SM

Nous avons prouvé formellement la sécurité de notre protocole en utilisant l'outil automatique Scyther. C'est le protocole relatif au modèle de base proposé dans la contribution qui a été vérifié, cependant :

- Le protocole tel que présenté dans la proposition de l'approche, s'est avéré résistant aux attaques par rejeu notamment dans la phase d'enregistrement via la présence de nonces,
- tandis qu'il s'est révélé vulnérable aux attaques Man In The Middle en présence d'un intermédiaire malicieux qui peut notamment, compromettre la session entre l'utilisateur et le Services Manager lors de l'authentification, comme illustré dans la figure 4.10:

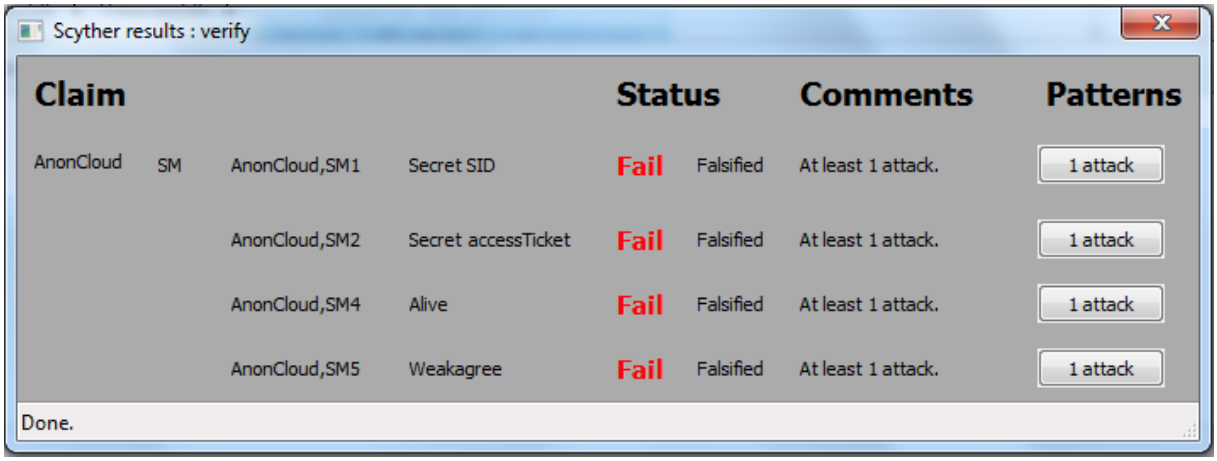


Figure 4.10 Présence d'attaques dans le rôle SM

Pour cela, **l'ajout de deux clés de session, à savoir SK1 et SK2** (dans le cas réel générées via le protocole Diffie-Hellman), a fait face à cette vulnérabilité. Ceci est illustré dans le script précédent, reflétant le modèle de base dans lequel les deux clés de session ont été rajoutées : entre l'utilisateur et le Manager RTM dans le cas de la clé SK1 et entre l'utilisateur et le Manager SM dans le cas de la clé SK2.
La clé de session SK2 (partagée entre l'utilisateur et le Services Manager), constitue particulièrement une parade contre les attaques décelées dans le rôle du Services Manager. La clé SK2 utilisée lors de la phase d'authentification de l'utilisateur vis-à-vis de SM, apparait dans le rôle de l'utilisateur et également dans le rôle du Services Manager.

Les exemples d'attaques relatives à la session entre l'utilisateur et le Services Manager dans le cas du protocole relatif au modèle de base avec absence de la clé de session SK2, sont illustrés dans la section suivante.

2.6. Attaques contre le protocole AnonCloud sans clés de sessions

La preuve de l'existence d'une faille dans un protocole est présentée généralement sous forme d'une trace valide de ce protocole montrant qu'un des objectifs visés en termes de propriété de sécurité n'est pas atteint. Cette trace constitue en effet le contre-exemple. Un point distinctif de Scyther est sa sortie graphique (voir figures ci-dessous). Alors que d'autres outils ne présentent qu'une trace textuelle de l'attaque, Scyther produit un graphe pour schématiser les attaques.

Les nœuds dans ce graphe représentent les événements de communication et les flèches l'ordre de ces évènements. Ce graphe est orienté verticalement, ce qui facilite la compréhension de la chronologie des événements lorsque plusieurs sessions se chevauchent.

Les figures ci-dessous montrent les attaques décelées par l'outil contre le protocole AnonCloud notamment dans la phase d'authentification : envoie de l'Access ticket et consommation des services. Ces attaques (généralement présentes contre les messages envoyés dans tout système) visent à écouter, modifier, substituer, supprimer les messages, remettre en jeu d'anciens messages, forger de nouveaux messages en utilisant les connaissances initiales/apprentissage etc. Ceci étant le cas de la session entre l'utilisateur et le Services Manager exposée à ces attaques de type MITM.

La figure 4.11, montre l'attaque possible sur le secret de l'Access Ticket lors de l'authentification vis-à-vis du Services Manager SM (Alice). Un intrus actif (Charlie) va s'interposer entre l'utilisateur (Dave) et le Services Manager (Alice) afin d'intercepter/modifier les échanges entre ces deux entités. Il va donc pouvoir corrompre la session entre ces deux parties communicantes et par la même occasion générer ou plutôt fabriquer un autre message connaissant la clé publique de RTM (nommé Bob). Même si lors de la vérification, RTM (Bob) va répondre par invalide Access Ticket à SM (Alice), mais du moment où l'intrus (Charlie) a pu entrer comme intermédiaire entre l'utilisateur et le Services Manager et générer un message de la même structure que le message attendu, la session de communication entre les deux est donc jugée vulnérable.

L'intrus a réussi donc à perturber le bon déroulement des échanges de messages. Le même cas se présente lors de la consommation des services, voir figure 4.12, qui montre à son tour l'attaque possible sur le secret du Service ID identique à celle relative au secret de l'Access Ticket. Dans les deux cas, l'attaquant est un attaquant actif qui peut fabriquer/modifier les messages.

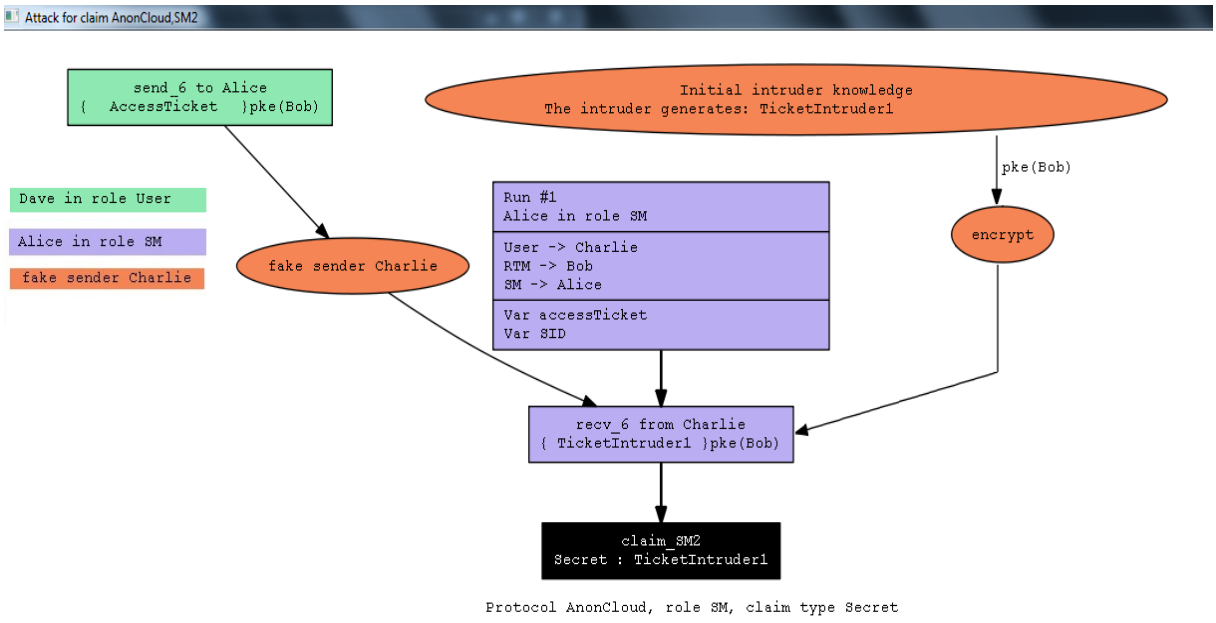


Figure 4.11 Attaque man in the middle active contre l'Access ticket

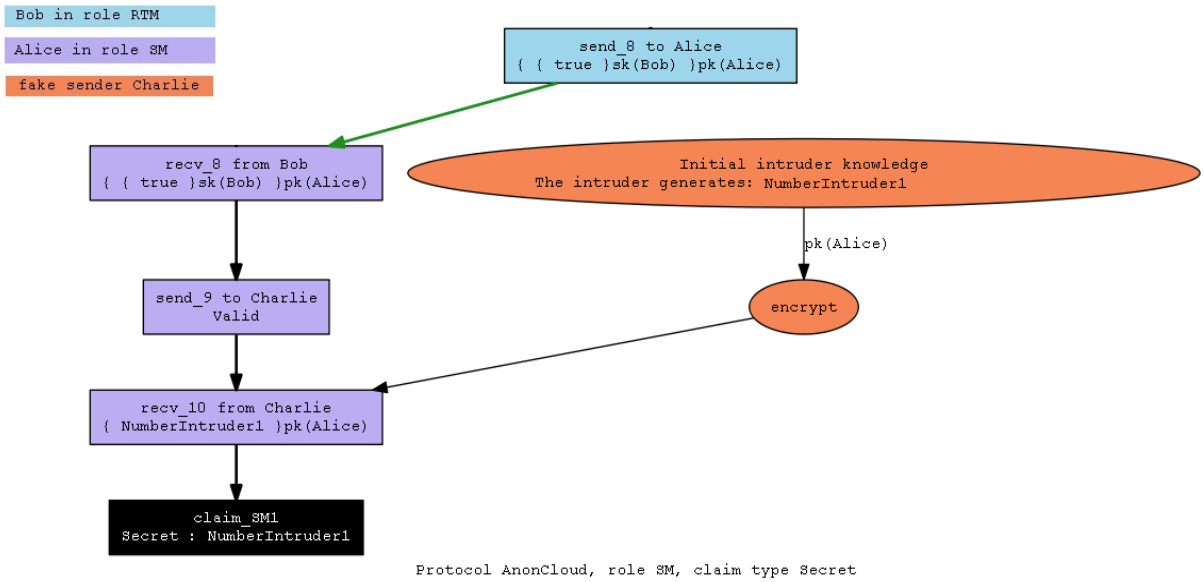


Figure 4.12 Attaque man in the middle active contre le service id

Les figures (4.13, 4.14) montrent à leurs tours, les scénarios d'attaque possibles compromettant la confidentialité des échanges entre l'utilisateur (Dave) et le Service manager (Alice), ce qui implique la non validation des propriétés de sécurité relatives à la vitalité et l'accord faible (alive et weakagree).

L'intrus (Charlie) va donc se mettre entre l'utilisateur (Dave) et le Services Manager (Alice) afin d'intercepter les messages échangés entre ces deux parties, puis les rediriger comme si de rien n'était. Les deux parties communicantes ne vont pas s'apercevoir de cette fraude et chacune aura comme certitude ou plutôt illusion, que les messages échangés arrivent parfaitement à l'autre sans que leur intégrité ou confidentialité ne soit affectée. Ceci est dû à la transparence que réalise l'intrus (Charlie) en étant passif : pas de modification sur les messages reçus, mais plutôt une interception de la part du Services Manager (Alice) puis une redirection vers l'utilisateur (Dave) et inversement : l'utilisateur voulant répondre au Services Manager, l'intrus (Charlie) s'est mis en position de destinataire, il recevra donc le message de l'utilisateur puis le redirigera vers son destinataire légitime qui est le Services Manager (Alice).

Pour conclure, nous remarquons que les deux parties communicantes n'ont pas la certitude chacune qu'elle est entrain de communiquer réellement avec l'autre d'où la non vérification de la vitalité et de l'accord faible. Dans ce cas, l'attaquant est un attaquant passif qui écoute les échanges sans les modifier.

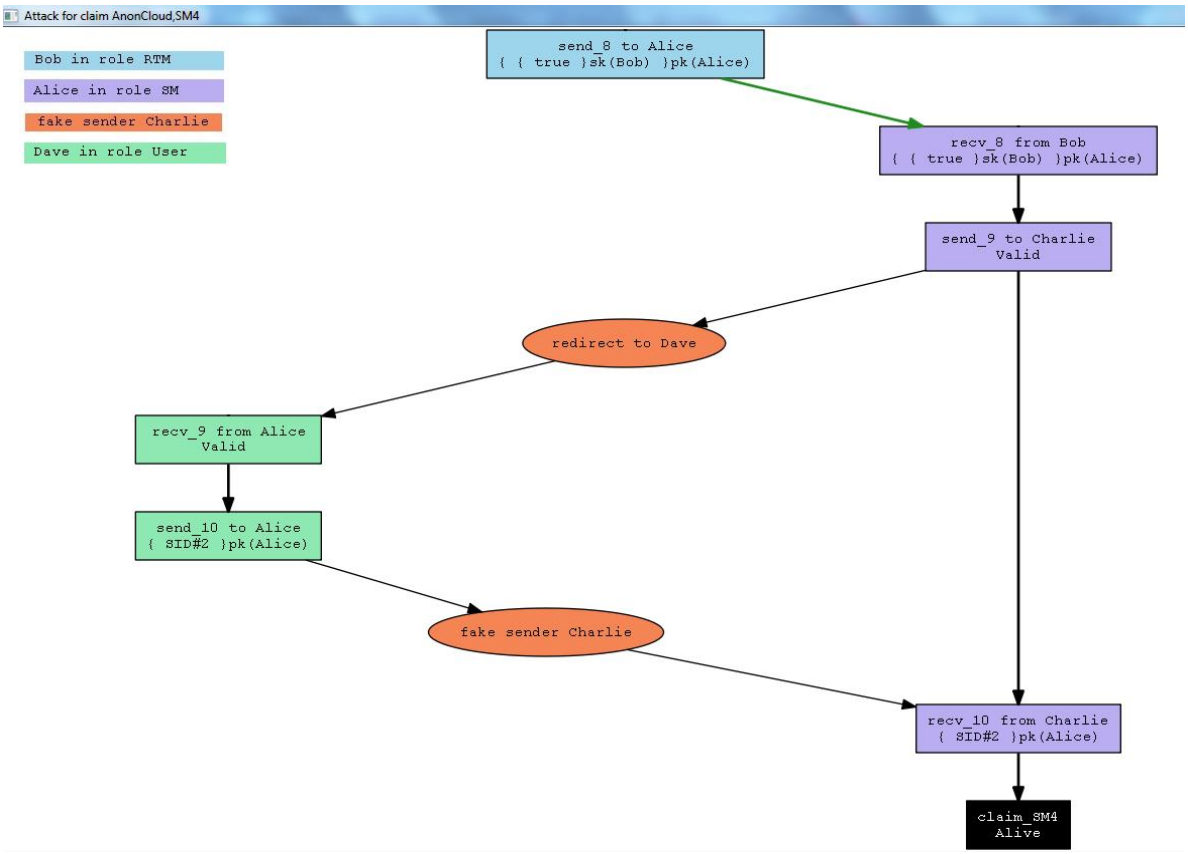


Figure 4.13 La vitalité « alive » non vérifiée

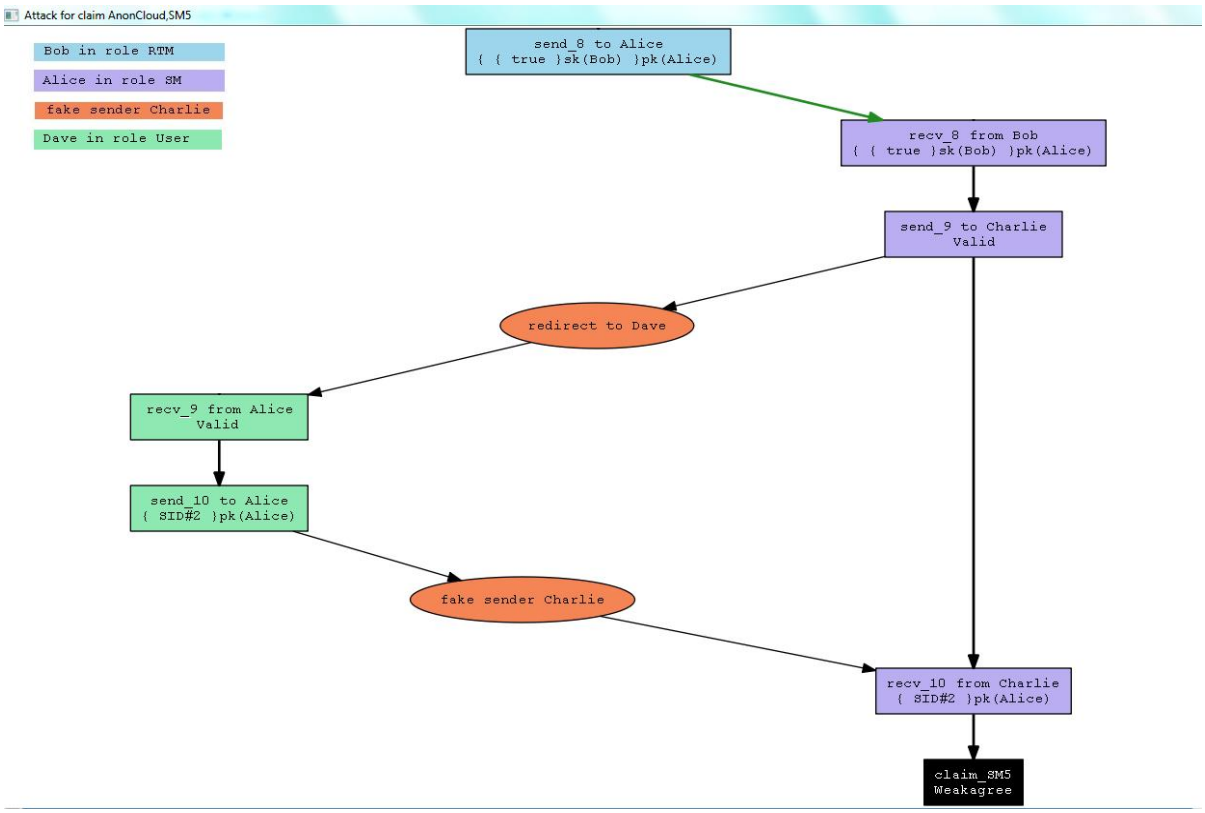


Figure 4.14 L'accord faible « weakagree » non vérifié

2.7. Résultat

Grâce à l'outil Scyther, nous avons pu vérifier les claims de notre protocole avec notamment la persistance de la vitalité et de l'accord faible, ainsi que tous les secrets supposés dans notre système. La figure suivante montre la sortie du script Scyther relatif au script déjà présenté, avec le statut de chaque claim défini dans le script. Chaque claim est vérifié pour chaque composant du système ainsi que l'absence d'attaques possibles car toutes les communications ont été sécurisées en utilisant différentes techniques cryptographiques.
Nous avons analysé le protocole à l'égard des objectifs de sécurité: secret du ToT, de l'Access ticket, du ServiceID et le secret des deux clés de session SK1 et SK2 rajoutées respectivement entre l'utilisateur et RTM et entre l'utilisateur et SM, ainsi que la vérification des deux propriétés : Vitalité et Accord faible.

Scyther results : verify

Claim				Status	Comments
AnonCloud	User	AnonCloud,User1	Secret ToT	Ok	No attacks within bounds.
		AnonCloud,User2	Secret n	Ok	No attacks within bounds.
		AnonCloud,User3	Secret m	Ok	No attacks within bounds.
		AnonCloud,User4	Secret r	Ok	No attacks within bounds.
		AnonCloud,User5	Secret blindrep	Ok	No attacks within bounds.
		AnonCloud,User6	Alive	Ok	No attacks within bounds.
		AnonCloud,User7	Weakagree	Ok	No attacks within bounds.
	RTM	AnonCloud,RTM1	Secret ToT	Ok	No attacks within bounds.
		AnonCloud,RTM2	Secret n	Ok	No attacks within bounds.
		AnonCloud,RTM3	Secret blind	Ok	No attacks within bounds.
		AnonCloud,RTM4	Secret accessTicket	Ok	No attacks within bounds.
		AnonCloud,RTM5	SKR SK1	Ok	No attacks within bounds.
		AnonCloud,RTM6	Alive	Ok	No attacks within bounds.
		AnonCloud,RTM7	Weakagree	Ok	No attacks within bounds.
	SM	AnonCloud,SM1	Secret SID	Ok	No attacks within bounds.
		AnonCloud,SM2	Secret accessTicket	Ok	No attacks within bounds.
		AnonCloud,SM3	SKR SK2	Ok	No attacks within bounds.
		AnonCloud,SM4	Alive	Ok	No attacks within bounds.
		AnonCloud,SM5	Weakagree	Ok	No attacks within bounds.

Done.

Figure 4.15 Fenêtre de sortie Scyther : le résultat du script

De plus, l'outil Scyther permet de vérifier automatiquement chaque propriété de sécurité parmi les quatre considérées, ce qui va rajouter deux propriétés à savoir l'Accord et la Synchronisation qui ont été également validées. Les figures suivantes montrent la validation des quatre propriétés dans chacun des rôles du protocole AnonCloud:

AnonCloud	User	AnonCloud,User6	Alive	Ok	No attacks within bounds.
		AnonCloud,User7	Weakagree	Ok	No attacks within bounds.
		AnonCloud,User8	Niagree	Ok	No attacks within bounds.
		AnonCloud,User9	Nisynch	Ok	No attacks within bounds.

Figure 4.16 Propriétés de sécurité dans le rôle utilisateur

AnonCloud	RTM	AnonCloud,RTM6	Alive	Ok	No attacks within bounds.
		AnonCloud,RTM7	Weakagree	Ok	No attacks within bounds.
		AnonCloud,RTM8	Niagree	Ok	No attacks within bounds.
		AnonCloud,RTM9	Nisynch	Ok	No attacks within bounds.

Figure 4.17 Propriétés de sécurité dans le rôle RTM

AnonCloud	SM	AnonCloud,SM4	Alive	Ok	No attacks within bounds.
		AnonCloud,SM5	Weakagree	Ok	No attacks within bounds.
		AnonCloud,SM6	Niagree	Ok	No attacks within bounds.
		AnonCloud,SM7	Nisynch	Ok	No attacks within bounds.

Done.

Figure 4.18 Propriétés de sécurité dans le rôle SM

Pour conclure, le résultat de Scyther a prouvé les claims du protocole. Le premier claim étant le secret du ToT qui représente la preuve de l'enregistrement, qui demeure sécurisé et non révélé et donc également protégé contre les attaques. Les claims concernant le secret du ticket d'accès anonyme et du service ID à consommer ont également été vérifiés.
Les propriétés de sécurité ont également été vérifiées notamment la vitalité du système : qui assure que, dans tout système garantissant la confidentialité, il existe toujours une réponse de la part du récepteur à la suite d'un message ou d'un événement généré par un expéditeur.
Les résultats de Scyther montrent également que les messages échangés et communiqués ne sont pas modifiés parce qu'ils sont signés et ne sont pas rejoués en raison de l'utilisation de nonce. L'intégrité et la confidentialité du système restent alors préservées et aucune attaque d'intrusion n'a pu être lancée sur le système notamment avec l'ajout de deux clés de session entre l'utilisateur et le Manager RTM ainsi que l'utilisateur et le Manager SM.

3. Implémentation du protocole AnonCloud

Pour pouvoir illustrer le déploiement de notre protocole dans un environnement Cloud, nous avons implémenté un prototype. Un prototype combinant le langage Java et les sockets a été développé. Le protocole peut être intégré comme première phase lors de l'accès aux services Cloud.

3.1. Outils utilisés

- **Java :** Afin d'implémenter notre application, nous avons opté pour le langage Java comme outil de développement. Ce choix est dû, d'une part, au fait que ce langage est indépendant de toute plate-forme et qu'il est orienté objet. La technologie Java est à la base de la plupart des applications informatiques et elle est exploitée dans le monde entier pour développer et fournir des applications multiples. La technologie Java permet de développer, de déployer et d'utiliser efficacement des applications et des services intéressants. **[86]**

- **NetBeans IDE version 8.0.2 :** NetBeans est un environnement de développement intégré (IDE) pour Java, placé en open source par SUN en juin 2000 sous licence CDDL et GPLv2 (Common Development and Distribution Licence). En plus de Java, NetBeans permet également de supporter différents autres langages comme : Python, C, C++, XML, et HTML. Il comprend toutes les caractéristiques d'un IDE moderne : éditeur de couleur, projet multi-langage, éditeur graphique d'interfaces et pages web, etc. **[87]**

- **Les sockets:** Un modèle permettant la communication inter processus afin de permettre à divers processus de communiquer, aussi bien sur une même machine qu'à travers un réseau utilisant le protocole TCP/IP ou UDP. Un socket est un point de terminaison d'un lien de communication bidirectionnelle entre deux programmes en cours d'exécution sur le réseau. Un socket est lié à un numéro de port de sorte que la couche TCP puisse identifier l'application dont les données sont destinées à être envoyées. Un point de terminaison est une combinaison d'une adresse IP et un numéro de port. Chaque connexion TCP peut être identifiée de manière unique par ses deux points de terminaison. **[88]**

- **Serveur web EasyPHP:** Environnement comprenant deux serveurs (un serveur web Apache et un serveur de bases de données MySQL), ainsi que des outils de développement comme le gestionnaire de base de données PhpMyAdmin **[89]**.

- **Vmware workstation:** Logiciel qui permet la création d'une ou de plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliées au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de la machine hôte. **[90]**

3.2. Les interfaces

Au démarrage de l'exécution des trois codes séparés à savoir les deux serveurs RTM et SM et l'application côté client (différentes interfaces), chaque code s'exécutera dans une machine virtuelle crée préalablement.
Les deux serveurs s'initialisent et prennent l'état running pour rester à l'écoute de connexions venant des utilisateurs dans un but d'authentification pour accéder à la consommation de services Cloud et cela dans le cas du serveur SM port 18000.

Dans le cas du serveur RTM, il existe deux types de requêtes : venant des utilisateurs pour des requêtes d'enregistrement et ultérieurement d'obtention de tickets d'accès et cela via le port d'écoute 25000, ou venant du serveur SM (qui devient client de RTM) pour des requêtes de vérification des tickets d'accès afin de rediriger les utilisateurs vers la consommation de services et cela via le port d'écoute 24000.

3.2.1. Interfaces Utilisateurs

La figure 4.19 illustre l'interface principale de l'outil AnonCloud du côté de l'utilisateur. Les trois tâches principales étant ordonnées comme suit : l'enregistrement de l'utilisateur, la négociation à propos du niveau de privacy des attributs fournis ainsi que le niveau d'anonymat désiré lors de l'accès aux services : anonymat partiel ou complet.

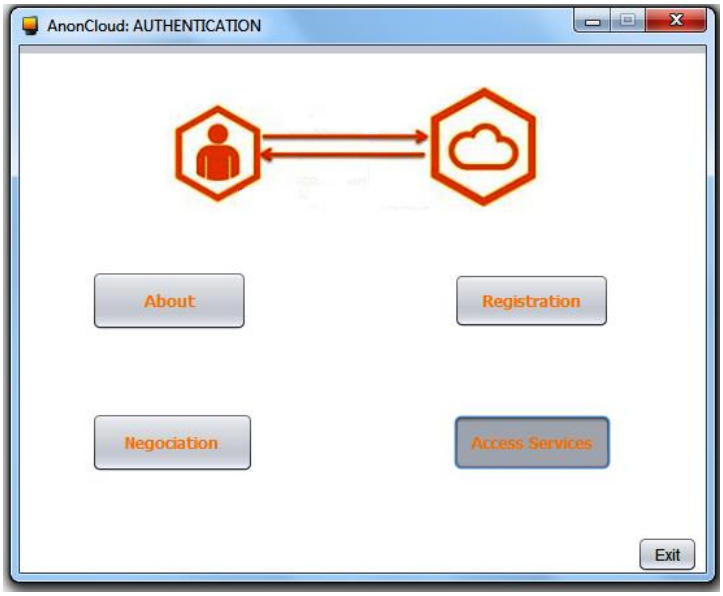


Figure 4.19 Interface principale

Les deux figures ci-dessous montrent les étapes préliminaires d'enregistrement et de négociation que l'utilisateur devra passer en premier avant de pouvoir accéder aux services.

Figure 4.20 Interface d'enregistrement

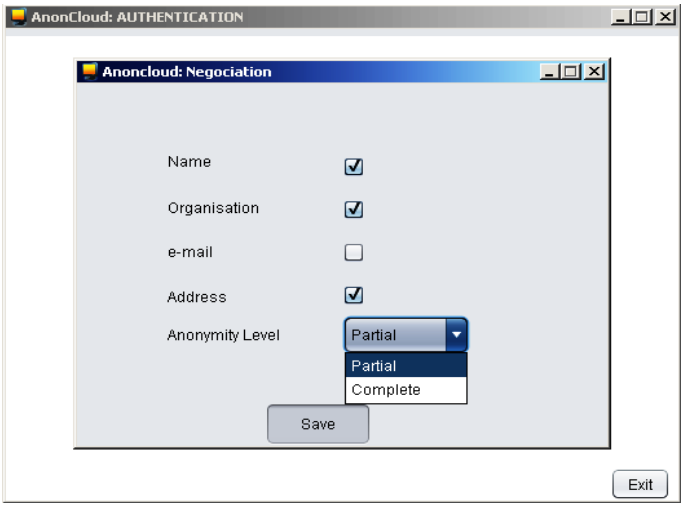


Figure 4.21 Interface de négociation

Une fois les deux premières étapes achevées, à savoir l'enregistrement et la négociation qui permettent à l'utilisateur de s'enregistrer en fournissant les attributs souhaités, un ToT sera généré et envoyé à l'utilisateur et en parallèle enregistré dans la base de données du côté du serveur RTM.
L'utilisateur pourra maintenant passer à l'accès aux services en cliquant sur le bouton *Access Services* dans l'interface principale. Ceci va lui permettre de passer en premier lieu à valider son appartenance au Cloud via l'insertion de son ToT obtenu préalablement. La vérification du ToT se fait en cliquant sur le bouton *Anonymous Access* figure 4.23. Si la vérification réussit, la génération d'un Access Ticket entre l'utilisateur et RTM sera réalisée.

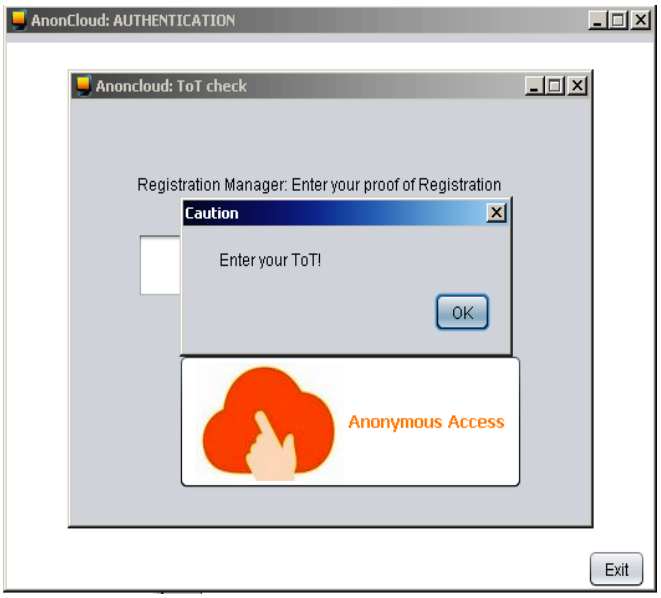


Figure 4.22 Interface de contrôle du ToT

Figure 4.23 Vérification du ToT

L'étape de vérification du ToT est indispensable pour éventuellement obtenir un Access Ticket limité seulement aux utilisateurs enregistrés. L'Access Ticket généré est temporaire, en utilisation unique et non extensible : l'Access ticket est service dépendant, à chaque accès un Access Ticket est généré.

Avant de pouvoir accéder aux services, l'utilisateur doit passer par l'interface de vérification de l'Access Ticket figure 4.24, avant d'envoyer sa requête d'accès aux services. Si cette étape se déroule avec succès reflétant un Access Ticket valide introduit par l'utilisateur, ce dernier sera donc rediriger vers les services Cloud pour commencer sa consommation en toute sécurité tout en préservant sa vie privée et son anonymat vis-à-vis du CSP.

Figure 4.24 Interface de contrôle de l'Access ticket

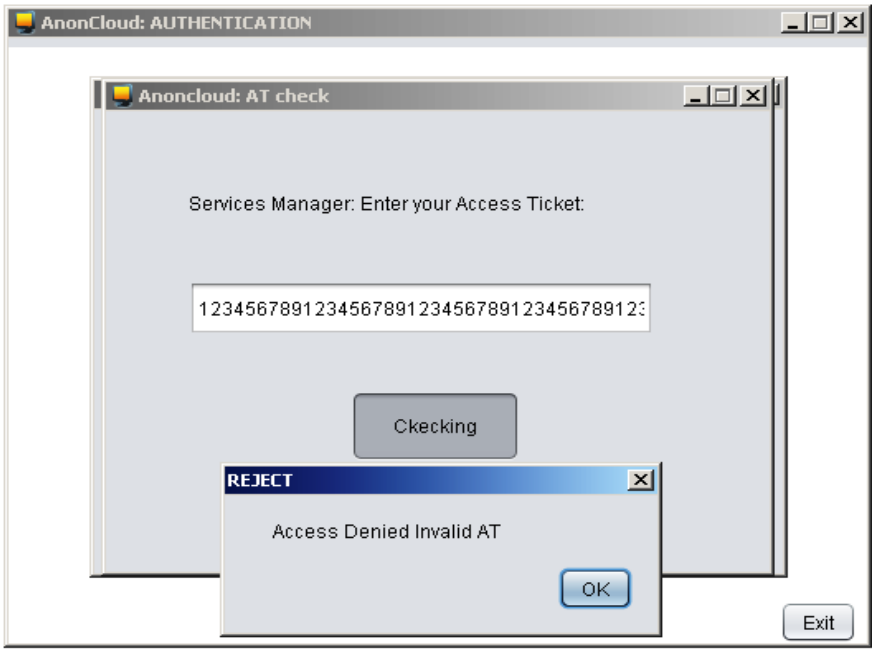


Figure 4.25 Interface de vérification de l'Access ticket avec message d'erreur

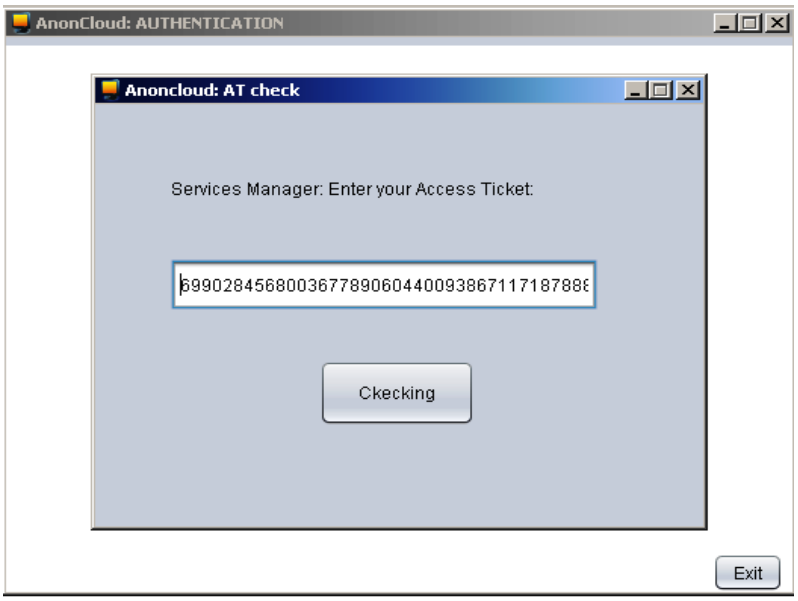


Figure 4.26 Interface reflétant un Access ticket valide

La figure 4.27 illustre la sortie du processus du côté de l'utilisateur avec tous les calculs effectués notamment, lors de la génération de l'Access Ticket via la signature en aveugle avec le serveur RTM et lors de la vérification de l'Access Ticket avec le serveur SM.

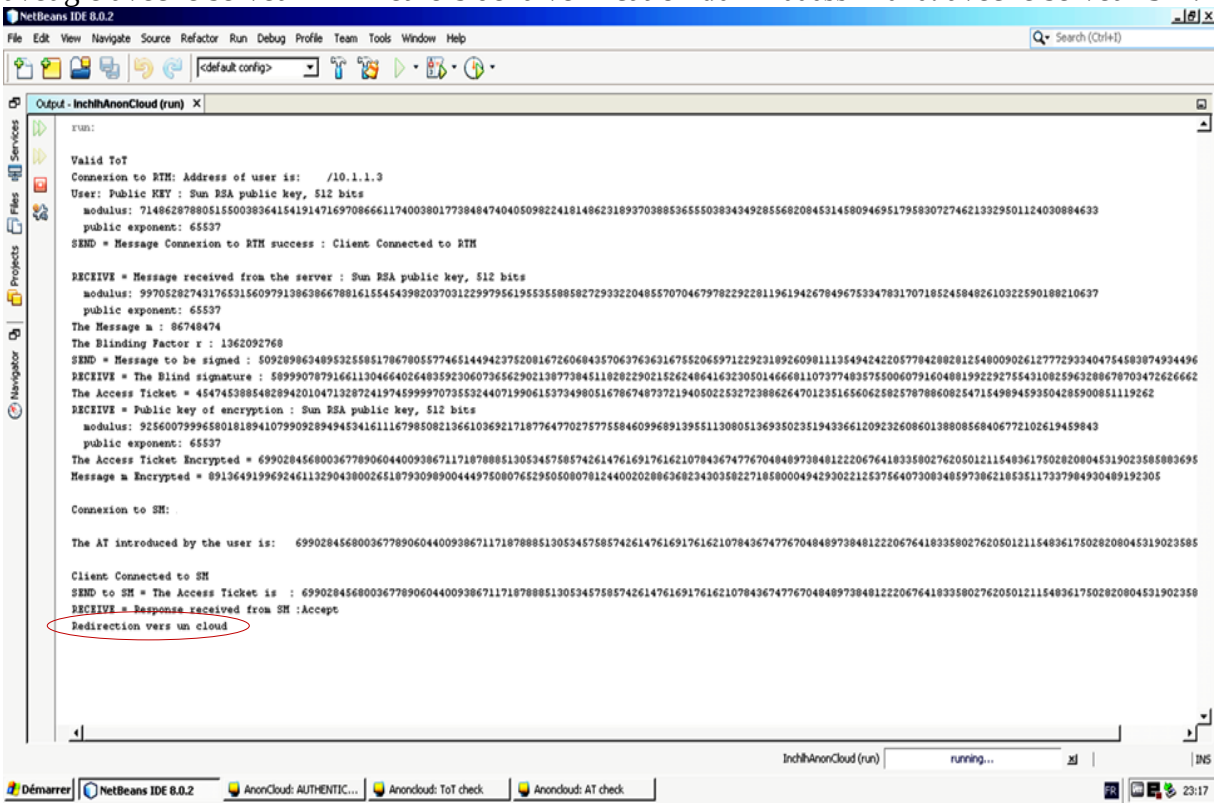


Figure 4.27 Sortie du côté de l'utilisateur après tous les calculs

3.2.2. Opérations effectuées par le serveur RTM

La figure 4.28, montre la sortie du serveur RTM illustrant les réponses à la requête de génération de l'Access Ticket ainsi que la réponse au serveur SM lors de sa vérification.

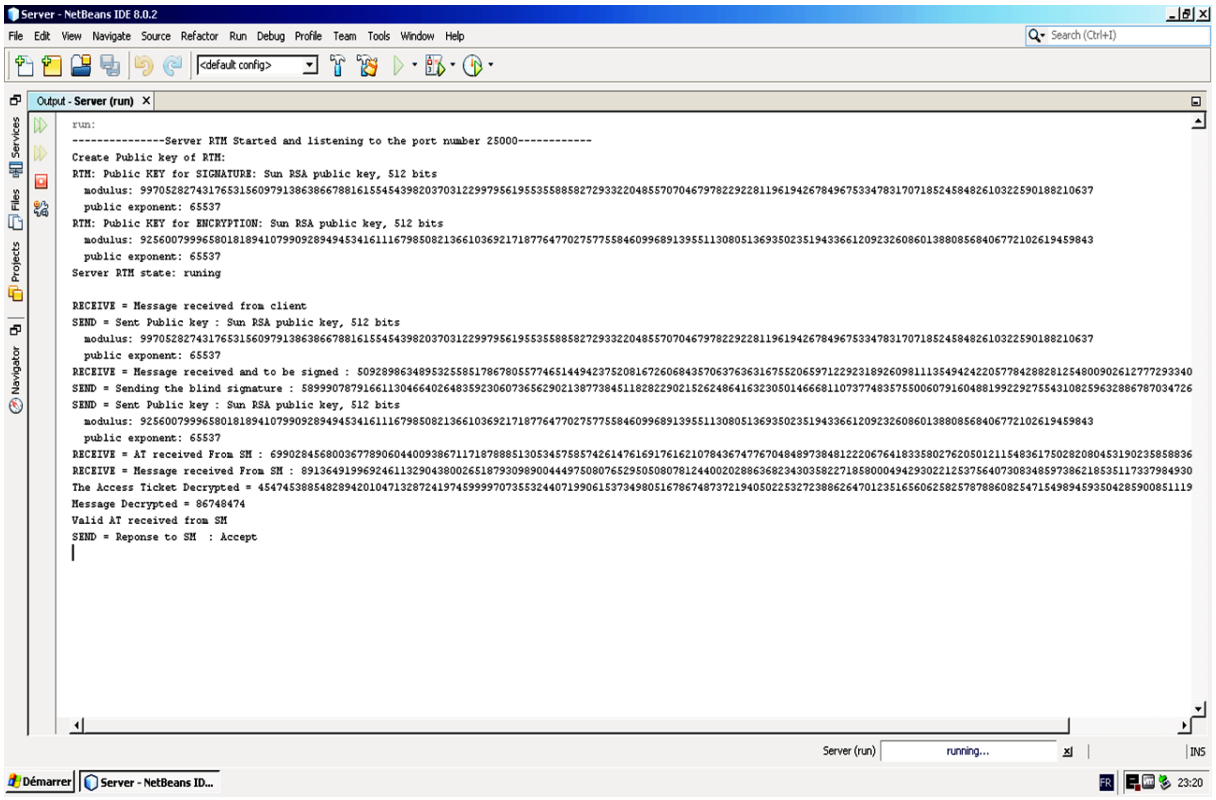


Figure 4.28 Sortie du serveur RTM

3.2.3. Opérations effectuées par le serveur SM

La figure 4.29, montre la sortie du serveur SM illustrant les réponses à la requête d'un utilisateur venant s'authentifier afin de pouvoir accéder aux services.

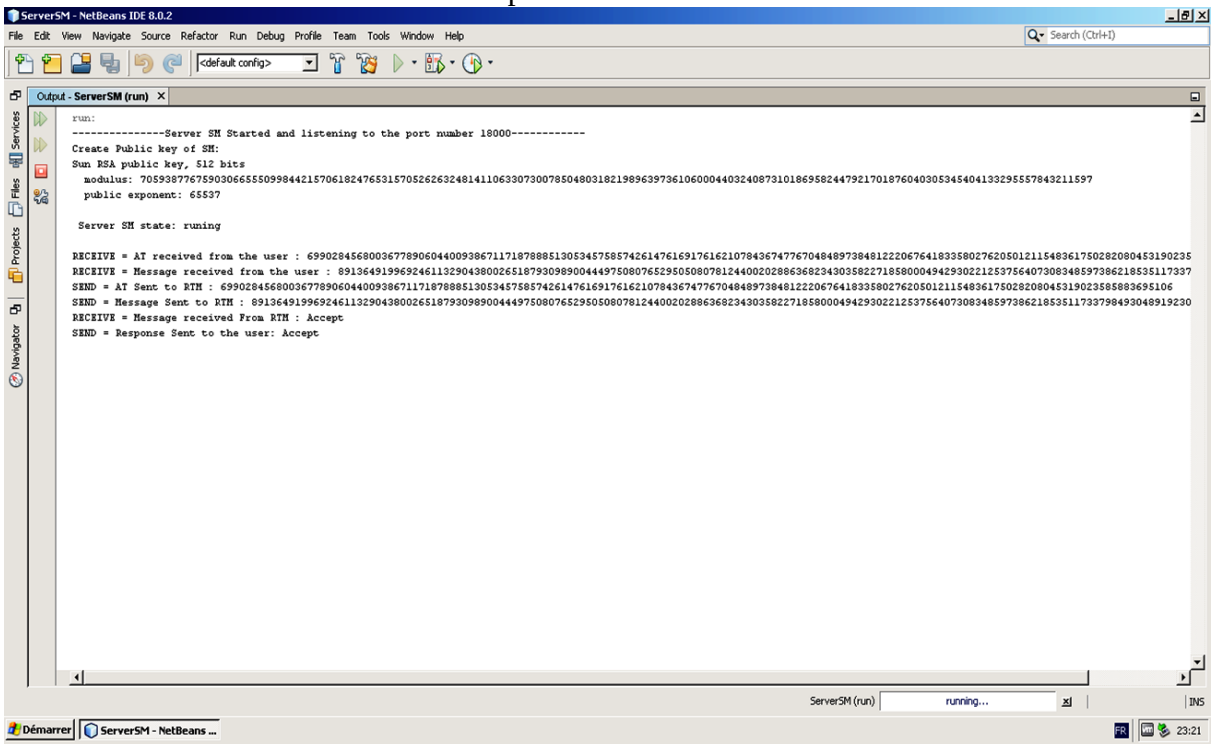


Figure 4.29 Sortie du serveur SM

3.3. La base de données

Une base de données MySQL nommée « anoncloud » a été créé afin d'enregistrer les informations d'enregistrement des utilisateurs (les différents attributs fournis) et les flags relatifs au niveau d'anonymat requis pour chaque attribut, ainsi que l'enregistrement des ToT attribués après enregistrement.
La base contient alors trois tables à savoir : « Registration », « Negociation » et « TicketofTicket » comme montré dans les trois figures suivantes.

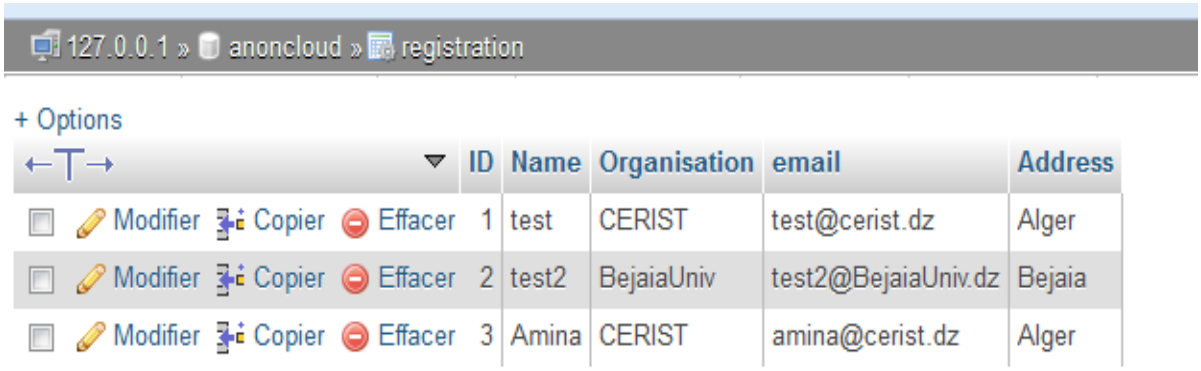


Figure 4.30 Table Registration

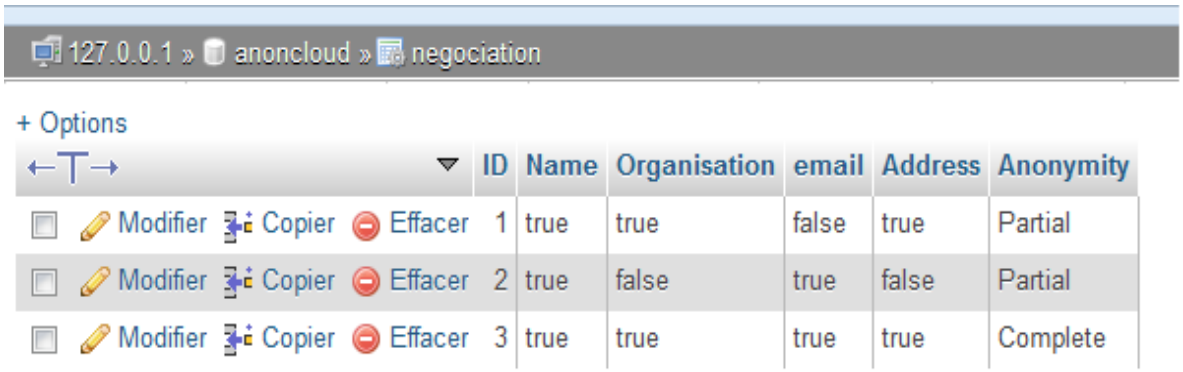


Figure 4.31 Table Negociation

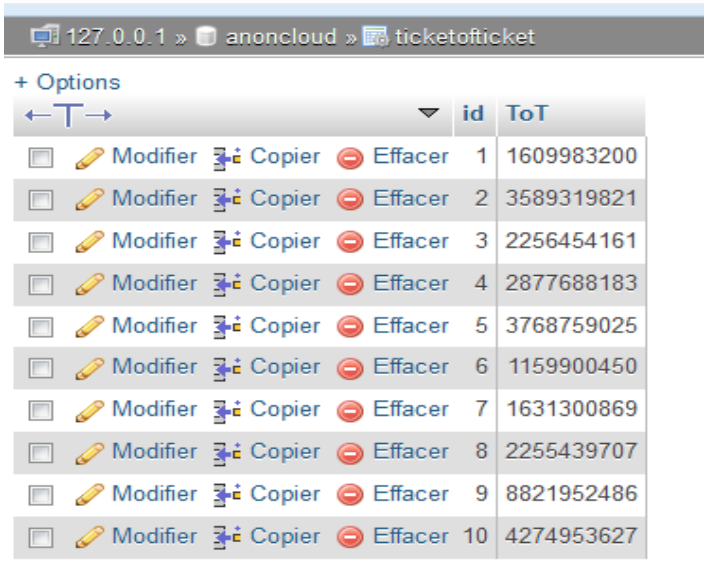


Figure 4.32 Table des ToT

4. Conclusion

Après la conception et l'élaboration du protocole, nous avons procédé à sa vérification en utilisant l'outil de vérification de sécurité Scyther. La vitalité, l'accord faible ainsi que deux autres propriétés, en plus des différents secrets supposés dans le système ont été vérifiés et aucune attaque n'a été découverte particulièrement, après l'ajout de deux clés de session protégeant les communications entre l'utilisateur et les deux Managers.

La sécurité des protocoles repose sur la sécurité des primitives cryptographiques et sur l'absence de failles dans la construction et l'agencement de ces primitives. Les preuves de sécurité ont pour objectif de montrer l'impossibilité de casser le protocole. Ces preuves de sécurité sont techniquement intéressantes et importantes d'un point de vue pratique. Elles permettent de montrer que les schémas utilisés en pratique ne présentent pas de failles. Etant donné qu'une faille peut contenir un nombre important d'étapes de communication et est difficile à trouver manuellement, le besoin d'utiliser un outil automatique était donc nécessaire. L'automatisation de la vérification des protocoles nous a donc permis de valider et de corriger le nôtre pour faire face aux différentes vulnérabilités vis-à-vis d'un intrus ou d'un agent compromis. L'ajout des deux clés de session partagées respectivement entre l'utilisateur et le Manager RTM ainsi que l'utilisateur et le Manager SM, a permis d'obtenir un protocole d'authentification vérifié et validé avec absence d'attaques possibles.

Une fois achevée, cette étape nous a permis de passer à l'étape d'implémentation d'un prototype java qui pourra être intégré comme première phase lors de l'accès aux services Cloud, afin d'assurer la privacy des utilisateurs Cloud vis-à-vis du CSP.

Conclusion Générale

Le concept d'anonymat surgit à de nombreuses occasions sur Internet, notamment pour la messagerie électronique, la navigation et plusieurs applications qui nécessitent de garantir la propriété d'anonymat particulièrement le commerce électronique. Cependant, avec l'émergence du Cloud Computing, de nouveaux challenges se présentent, en matière de sécurité et de confiance lors de l'utilisation des différents services. La technologie Cloud, avant d'être entièrement sûre, elle devra intégrer des améliorations qui permettront de protéger au mieux les utilisateurs et ainsi, leur garantir la confidentialité de leurs données personnelles.

A tire d'exemple, le Cloud e-santé, où les données médicales sont à la fois confidentielles, sauf pour la relation médecin/patient, en plus d'être très personnelles par rapport au patient. Ce dernier ne voudra en aucun cas que ses données médicales soient divulguées (même vis-à-vis du CSP). Dans le domaine médical, pouvoir révéler l'identité d'un patient constitue en effet une violation de sa vie privée, même si ses données médicales sont confidentielles. Un accès anonyme est considéré comme très approprié dans le Cloud e-santé afin de dissimuler l'utilisateur (le patient).

Notre problématique consistait donc en premier lieu, à étudier les problèmes de protection des données personnelles dans un environnement Cloud notamment lors de la phase d'authentification et ensuite, de s'intéresser plus précisément à l'authentification anonyme dans ce type d'environnement. Dans une première étape, une comparaison a été portée sur les modèles relatifs aux approches mises en œuvre pour la protection des données personnelles. Par la suite, une nouvelle approche d'authentification anonyme dans le Cloud a été proposée, se basant sur l'anonymisation des informations sensibles pouvant révéler l'identité de l'utilisateur Cloud. De plus, une classification a été faite cernant les données sensibles à protéger dans le Cloud vis-à-vis des entités pouvant les percevoir/exploiter.

Notre principale contribution était donc de proposer une authentification anonyme adaptative aux exigences de privacy des utilisateurs Cloud, qui se caractérise par une politique adaptative de protection des données personnelles. Cette proposition considère deux modèles, à savoir:

- Un modèle de base assurant une consommation anonyme des services Cloud via des tickets anonymes générés lors de chaque requête de consommation de services.
  Les caractéristiques du modèle de base sont:
  - Politique adaptative de protection des données personnelles définie pour chaque utilisateur, lui permettant de choisir le niveau d'anonymat requis.
  - Consommation anonyme des services Cloud: la seule information que connaitra le CSP est qu'un utilisateur légitime a demandé un service.
  - Informations d'identification anonymes: tickets d'accès via la signature en aveugle, permettent aux utilisateurs d'effectuer des requêtes anonymes sans divulguer d'autres informations d'identité.

- Dans le modèle de base, la métadonnée adresse IP n'a pas été protégée ce qui permet une éventuelle traçabilité des utilisateurs, en se basant sur cette information sensible. Un modèle étendu a donc été proposé comme extension du modèle de base, afin de contrecarrer ses limites. Ce modèle étendu permet ainsi une authentification anonyme complète. Les caractéristiques de ce modèle sont:

- Ajout d'une couche de communication anonyme afin de cacher l'adresse IP des utilisateurs vis-à-vis du CSP, en plus de la consommation anonyme des services.
- Même si les différents Managers communiquent, la divulgation de l'identité ou la traçabilité de l'utilisateur reste difficile à réaliser.
- La nouvelle particularité était d'impliquer les utilisateurs eux-mêmes en tant que nœuds volontaires pour acheminer les communications.
- Cette nouvelle combinaison élimine la notion de confiance au CSP en acheminant les communications via ses nœuds seulement.
- Permettre aux utilisateurs de consommer en toute sécurité les services Cloud tout en étant indépendants de la notion de « confiance » qui nécessite un certain niveau de loyauté pour l'assurance de l'anonymat des utilisateurs.
- Nous constatons en conséquence que, plus le nombre d'utilisateurs augmente, mieux sera le niveau d'anonymat offert par ce modèle.

L'originalité était alors de réduire ou éliminer le cas où seuls les nœuds du CSP maintiennent les communications et pourra par conséquent, établir une corrélation entre le trafic lui permettant de casser l'anonymat du système. Le besoin à atteindre était d'autoriser les utilisateurs à consommer en toute sécurité les services Cloud tout en étant indépendants de la notion de confiance via la proposition d'un protocole relatif à chaque modèle d'accès proposé.

En outre, nous avons prouvé formellement la sécurité de notre protocole relatif au modèle de base en utilisant l'outil automatique Scyther. De plus, pour pouvoir illustrer le déploiement de notre protocole, nous avons implémenté un prototype. Le protocole peut être intégrer comme première phase lors de l'accès aux services Cloud.

Des perspectives futures sont envisagées pour la suite de ce travail, nous proposons de:

1. Croiser le résultat de l'outil Scyther avec d'autres vérificateurs de protocoles pour donner un avis plus précis.

2. Voir réellement comment les améliorations affectent les performances, vu que l'anonymat est assuré et les vulnérabilités peuvent être résolues par les mécanismes proposés à savoir l'utilisation de la signature en aveugle et le routage en oignon. Cependant, cela se traduit, dans le pire des cas, par une augmentation dans le temps d'exécution. Cela peut être considéré comme relativement faible lorsque la sécurité notamment la privacy est plus importante puisque entre performances et sécurité un compromis doit toujours être considéré.

3. Introduire le paiement à l'usage via l'introduction d'une entité « Banque » qui aura comme tâche de manipuler une monnaie électronique « Principe du e-cash » et cela toujours via la technique de la signature en aveugle : offrir aux utilisateurs l'équivalent électronique du billet de banque, qui ne porte pas le nom de son utilisateur et garantit son anonymat.

4. S'intéresser à la confidentialité des données elles même : toutes les données manipulées dans l'architecture Utilisateurs/CSP, stockées ou transférées. Ces données pouvant éventuellement contenir des informations sensibles et permettent ainsi d'inspecter et également de dévoiler l'identité réelle des utilisateurs, il est alors essentiel d'éliminer toute information qui permet l'identification des utilisateurs à partir des données proprement dites. L'objectif visé étant de trouver un compromis entre la sécurité des données (intégrité et confidentialité) et l'anonymat de l'utilisateur Cloud (notamment d'un patient dans le cas d'un Cloud e-santé).

Bibliographie

[1] MELL, Peter et GRANCE, Tim. The NIST definition of cloud computing. *National Institute of Standards and Technology NIST special publication*, 2011, vol. 800, no 145.

[2] KIM, Manjea, JEONG, Hoon, et CHOI, Euiin. Context-aware Platform for User Authentication in Cloud Database Computing. In : *International Conference on Future Information Technology and Management Science & Engineering Lecture Notes in Information Technology*. 2012. vol.14, p. 170-176.

[3] Direction Régionale des Entreprises de la Concurrence de la Consommation du Travail et de l'Emploi. *Le Cloud Computing: une nouvelle filière fortement structurante* [en ligne]. Ile-de-France : DIRECCTE, 2012. [Consulté le 01 mars 2016]. Disponible sur : <http://old.idf.direccte.gouv.fr/IMG/pdf/ cloud_computing_final.pdf>.

[4] T-Systems International GmbH. *Livre Blanc : Le Cloud Computing, Une stratégie de sourcing alternative pour votre système d'information* [en ligne]. Allemagne : T-Systems, 2009. [Consulté le 01 mars 2016]. Disponible sur : <http://www.t-systems.fr/home/page-d-accueil/492094_1/blobBinary/WhitePaper_Cloud+ Computing-ps.pdf>.

[5] VMWARE. *Livre Blanc : Transition vers votre Cloud, Pour que votre organisation réactive devienne innovante* [en ligne]. USA : Vmware, Inc, 2012. [Consulté le 01 mars 2016]. Disponible sur : <http://www.vmware.com/files/fr/pdf/vmware-journey-to-your-cloud-wp-fr.pdf>.

[6] JANSEN, Wayne, GRANCE, Timothy, *et al.* Guidelines on security and privacy in public cloud computing. *National Institute of Standards and Technology NIST special publication*, 2011, vol. 800, no 144.

[7] DONALD, A. Cecil, JENIS, A., et AROCKIAM, L. An Authentication Mechanism to Enhance Security in the Cloud Environment. *International Journal of Current Engineering and Technology*, 2014, vol. 4, no 5.

[8] RIVARD, François. *Cloud Computing: le système d'information sans limite*. Lavoisier, 2012.

[9] GUPTA, Niharika et RANI, Rama. Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. *International Journal of Web & Semantic Technology (IJWesT)*, 2015, vol. 6, no 2, p. 9.

[10] TOP THREATS WORKING GROUP, *et al.* The notorious nine: cloud computing top threats in 2013. *Cloud Security Alliance*, 2013.

[11] MODI, Chirag, PATEL, Dhiren, BORISANIYA, Bhavesh, *et al.* A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing*, 2013, vol. 63, no 2, p. 561-592.

[12] SINGH, Shikha, *et al.* Cloud computing attacks: a discussion with solutions. *Open Journal of Mobile Computing and Cloud Computing*, 2014, vol. 1, no 1.

[13] YU, Shui. *Distributed Denial of Service Attack and Defense*. Springer New York, 2014.

[14] CLAYCOMB, William R. et NICOLL, Alex. Insider threats to cloud computing: Directions for new research challenges. In : *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*. IEEE, 2012. p. 387-394.

[15] SYNTEC Numérique. Livre Blanc : Sécurité du Cloud Computing, Analyse des risques, réponses et bonnes pratiques [en ligne]. Paris : Syntec, 2010. [Consulté le 01 mars 2016]. Disponible sur: <http://www.config.fr/press/Livre_Blanc_Cloud_Computing_Securit%C3% A9.Vdef.pdf>.

[16] HALBHEER, Roger, CAVIT, Doug. *Miscrosoft: Sécurité et Cloud Computing* [en ligne]. Microsoft Corporation, 2010. [Consulté le 01 mars 2016]. Disponible sur : <http://download.microsoft.com>.

[17] THAKORE, Uttam et LAUDE, Summa Cum. Scalable and Privacy-preserving Access Mechanism for Dynamic Clouds. 2012.

[18] TRUDEL, Pierre. *La protection de la vie privée* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : < http://pierretrudel.chairelrwilson.ca/cours/drt3805/Prot.%20vie%20Privee .pdf>

[19] SWIRE, Peter P. et BERMANN, Sol (ed.). *Information Privacy: Official Reference for the Certified Information Privacy Professional (CIPP)*. International Association of Privacy Professionals, 2007.

[20] GAMBS, Sébastien. *Respect de la vie privée dans la société de l'information* [en ligne]. Renne : 2011. [Consulté le 01 mars 2016]. Disponible sur : <http://videos.rennes.inria.fr/conf-Descartes/Sebastien-Gambs /protection_vie_privee.pdf>.

[21] ELSER, Amy. *Reliable distributed systems: technologies, web services, and applications*. Springer Science & Business Media, 2005.

[22] PEARSON, Siani. Taking account of privacy when designing cloud computing services. In : *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*. IEEE Computer Society, 2009. p. 44-52.

[23] ISO. *International Standard ISO*/IEC *15408-2 : 2008. Information technology, Security techniques, Evaluation criteria for IT security, Part 2: Security functional components* [en ligne]. Switzerland : International Organization for Standardization, 2008. [Consulté le 01 mars 2016]. Disponible sur : <https://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf>.

[24] ANGIN, Pelin, BHARGAVA, Bharat, RANCHAL, Rohit, *et al.* An entity-centric approach for privacy and identity management in cloud computing. In : *Reliable Distributed Systems (SRDS), 2010 29th IEEE Symposium on*. IEEE, 2010. p. 177-183.

[25] RAHAMAN, Syed Mujib et FARHATULLAH, Mohammad. PccP: A model for Preserving cloud computing Privacy. In : *Data Science & Engineering (ICDSE), 2012 International Conference on*. IEEE, 2012. p. 166-170.

[26] PEARSON, Siani et YEE, George (ed.). *Privacy and security for cloud computing*. Springer Science & Business Media, 2012.

[27] CHRISTIANSON, Bruce, MALCOLM, James, STAJANO, Frank, *et al.* (ed.). *Security Protocols XX: 20th International Workshop, Cambridge, UK, April 12-13, 2012, Revised Selected Papers*. Springer, 2012.

[28] KHAN, Hafiz Zahid Ullah et ZAHID, H. Comparative study of authentication techniques. *International Journal of Video & Image Processing and Network Security IJVIPNS*, 2010, vol. 10, no 04, p. 09-13.

[29] VILLACRES, Caline. *L'Authentification de A à Z* [en ligne]. USA : Ernst & Young LLP, 2003. [Consulté le 01 mars 2016]. Disponible sur : <http://repo.hackerzvoice.net/depot_ madchat/sysadm/unix.seku/Authentification_de_A_a_Z.pdf>.

[30] CHIA, Wan Yin. *The classification of e-authentication protocols for targeted applicability*. 2009. Thèse de doctorat. Monterey, California. Naval Postgraduate School.

[31] BURR, William E., DODSON, Donna F., POLK, William T., *et al*. *Electronic authentication guideline*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2013, vol. 800, no 63-2.

[32] CHAURASIA, Brijesh Kumar, SHAHI, Awanish, et VERMA, Shekhar. Authentication in cloud computing environment using two factor authentication. In : *Proceedings of the Third International Conference on Soft Computing for Problem Solving*. Springer India, 2014. p. 779-785.

[33] MICROSOFT. *La vie privée sur Internet: soyez sur vos gardes* [en ligne]. Canada : Microsoft Canada, 2001. [Consulté le 01 mars 2016]. Disponible sur : < https://www.ipc.on.ca/images/Resources/up-primer_f.pdf >.

[34] LIN, Hsiao-Ying, TZENG, Wen-Guey, *et al.* Anonymous Password Based Authenticated Key Exchange with Sub-Linear Communication. *Journal of information science and engineering*, 2009, vol. 25, no 3, p. 907-920.

[35] ISO. *International Standard ISO*/IEC *7498-2 : 1989. Information processing Systems, Open Systems Interconnection, Basic Reference Model, Part 2 : Security Architecture* [en ligne]. Switzerland : International Organization for Standardization, *1989*. [Consulté le 01 mars 2016]. Disponible sur : <https://webstore.iec.ch/preview/info_iso7498-2%7Bed1.0%7Den.pdf>.

[36] AHN, Hyosik, CHANG, Hyokyung, JANG, Changbok, *et al.* User authentication platform using provisioning in cloud computing environment. In : *Advanced Communication and Networking*. Springer Berlin Heidelberg, 2011. p. 132-138.

[37] BABAEIZADEH, Mahnoush, BAKHTIARI, Majid, et MOHAMMED, Alwuhayd Muteb. Authentication methods in cloud computing: A survey. *Research Journal of Applied Sciences, Engineering and Technology*, 2015, vol. 9, no 8, p. 655-664.

[38] KARNAN, M., AKILA, M., et KRISHNARAJ, N. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 2011, vol. 11, no 2, p. 1565-1573.

[39] ACAR, Tolga, BELENKIY, Mira, et KÜPÇÜ, Alptekin. Single password authentication. *Computer Networks*, 2013, vol. 57, no 13, p. 2597-2614.

[40] ABHISHEK, Kumar, ROSHAN, Sahana, KUMAR, Prabhat, *et al.* A Comprehensive Study on Multifactor Authentication Schemes. In : *Advances in Computing and Information Technology*. Springer Berlin Heidelberg, 2013. p. 561-568.

[41] YASSIN, Ali A., JIN, Hai, IBRAHIM, Amin, *et al.* Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. In : *Cloud and Green Computing (CGC), 2012 Second International Conference on*. IEEE, 2012. p. 282-289.

[42] TODOROV, Dobromir. Chapter 1: User Identification and Authentication Concepts. *From the book: Mechanics of User Identification and Authentication: Fundamentals of Identity Management. Auerbach Publications. Taylor & Francis Group*, 2007, vol. 200, p. 1-64.

[43] ZISSIS, Dimitrios et LEKKAS, Dimitrios. Addressing cloud computing security issues. *Future Generation computer systems*, 2012, vol. 28, no 3, p. 583-592.

[44] HAIDAR, Ali Nasrat et ABDALLAH, Ali E. Formal modelling of pki based authentication. *Electronic Notes in Theoretical Computer Science*, 2009, vol. 235, p. 55-70.

[45] FAHMY, Sherif F., SELIM, Gamal I., *et al.* MCSAuth: A New Authentication Mechanism for Cloud Systems. *International Journal of Computer Applications*, 2014, vol. 88, no 15.

[46] SHARMA, Shabnam et MITTAL, Usha. Comparative analysis of various authentication techniques in Cloud Computing. *International Journal of Innovative Research in Science, Engineering and Technology*, 2013, vol. 2, no 4, p. 994-998.

[47] JOHANSEN, Tor Anders. Identity management in future personalized service environments. 2010.

[48] RASS, Stefan et SLAMANIG, Daniel. *Cryptography for Security and Privacy in Cloud Computing*. Artech House, 2013.

[49] BELLOVIN, Steven M. et MERRITT, Michael. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In : *Research in Security and Privacy, 1992. Proceedings, 1992 IEEE Computer Society Symposium on*. IEEE, 1992. p. 72-84.

[50] BELLARE, Mihir, POINTCHEVAL, David, et ROGAWAY, Phillip. Authenticated key exchange secure against dictionary attacks. In : *Advances in Cryptology—EUROCRYPT 2000*. Springer Berlin Heidelberg, 2000. vol. 1807, p. 139-155.

[51] VIET, Duong Quang, YAMAMURA, Akihiro, et TANAKA, Hidema. Anonymous password-based authenticated key exchange. In : *Progress in Cryptology-INDOCRYPT 2005*. Springer Berlin Heidelberg, 2005. vol. 3797, p. 244-257.

[52] CHAUM, David et VAN HEYST, Eugène. Group signatures. In : *Advances in Cryptology—EUROCRYPT'91*. Springer Berlin Heidelberg, 1991. p. 257-265.

[53] CHAUM, David. Blind signatures for untraceable payments. In : *Advances in cryptology*. Springer US, 1983. p. 199-203.

[54] OLIVIER, Martin S. Distributed proxies for browsing privacy: a simulation of flocks. In: *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*. South African Institute for Computer Scientists and Information Technologists, 2005. p. 104-112.

[55] GOLDSCHLAG, David, REED, Michael, et SYVERSON, Paul. Onion routing. *Communications of the ACM*, 1999, vol. 42, no 2, p. 39-41.

[56] SYVERSON, Paul, DINGLEDINE, R., et MATHEWSON, N. Tor: the second-generation onion router. In : *Usenix Security*. 2004.

[57] BERTHOLD, Oliver, FEDERRATH, Hannes, et KÖPSELL, Stefan. Web MIXes: A system for anonymous and unobservable Internet access. In : *Designing Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2001. p. 115-129.

[58] IMPERVA. *Man in the Cloud MITC Attacks, hacker intelligence initiative report* [en ligne]. Imperva, Inc, 2015. [Consulté le 01 mars 2016]. Disponible sur : < https://www.imperva.com/docs/HII_Man_In_ The_Cloud_Attacks.pdf >.

[59] HAWKEY, Kirstie. Examining the shifting nature of privacy, identities, and impression management with Web 2.0. In : *Computational Science and Engineering, 2009. CSE'09. International Conference on*. IEEE, 2009. Vol.4, p. 990-995.

[60] KHAN, Safwan Mahmud et HAMLEN, Kevin W. AnonymousCloud: A data ownership privacy provider framework in cloud computing. In : *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012. p. 170-176.

[61] PACHECO, Vinicius et PUTTINI, Ricardo. SaaS Anonymous Cloud Service Consumption Structure. In : *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*. IEEE, 2012. p. 491-499.

[62] MUNIR, Kashif et PALANIAPPAN, Sellapan. Security threats/attacks present in cloud environment. *IJCSNS*, 2012, vol. 12, no 12, p. 107-114.

[63] LAISNE, Jean-Pierre. *Qui êtes-vous, monsieur le Cloud Broker ?* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <http://www.eurocloud.fr/qui-etes-vous-monsieur-le-cloud-broker/>

[64] NEELIMA, S. LAKSHMI, Y., et BADMAVATHI, M. A Survey on Security Issues and Threat Models in the Cloud. Int.J.Computer Technology and Applications, 2012, vol. 3, no 5, p. 1704-1709.

[65] KANDIAS, Miltiadis, VIRVILIS, Nikos, et GRITZALIS, Dimitris. The insider threat in cloud computing. In : *Critical Information Infrastructure Security*. Springer Berlin Heidelberg, 2011. p. 93-103.

[66] RAGIB, H. *Security and Privacy in Cloud Computing* [en ligne]. Johns Hopkins University, 2010. [Consulté le 01 mars 2016]. Disponible sur : <http://www.cs.jhu.edu/~ragib/sp10/cs412/lectures/ 600.412.lecture05.pdf >.

[67] GELLMAN, Robert. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In : *Proceedings of the World privacy forum,*. 2012.

[68] ROBINSON, Neil, VALERI, Lorenzo, CAVE, Jonathan, *et al.* The cloud: understanding the security, privacy and trust challenges. *Privacy and Trust Challenges (November 30, 2010)*, 2010.

[69] ISO. *International Standard ISO*/IEC *15408-1 : 2009. Information technology, Security techniques, Evaluation criteria for IT security, Part 1: Introduction and general model* [en ligne]. Switzerland : International Organization for Standardization, 2009. [Consulté le 01 mars 2016]. Disponible sur : <https://webstore.iec.ch/preview/info_isoiec15408-1%7Bed3.0%7Den.pdf>.

[70] TOR PROJECT. *Tor : Overview* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <https://www.torproject.org/ about/overview.html.en>.

[71] European eGovernment Services. *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms* [en ligne]. 2007. [Consulté le 01 mars 2016]. Disponible sur : < http://ec.europa.eu/idabc/servlets/Docbf72.pdf?id=29622 >.

[72] GAMBS, Sébastien. *Accréditations anonymes* [en ligne]. Irisa, 2015. [Consulté le 01 mars 2016]. Disponible sur : <https://www.irisa.fr/prive/sgambs/cours6_pvp.pdf >.

[73] TRIEU, Alix, CHATALIC, Amélie Royer Antoine, TESSIAU, Baptiste, *et al.* Aide à la conception et vérification de spécifications formelles de protocoles cryptographiques.

[74] LARAFA, Claire Sondès. *Vérification automatisée des protocoles cryptographiques* [en ligne]. ANSSI Agence Nationale de la sécurité des systèmes d'information, 2014. [Consulté le 01 mars 2016]. Disponible sur : <http://samovar.telecom-sudparis.eu/IMG/pdf/LARAFA_Claire_26mars2014-2.pdf >.

[75] CREMERS, Cas JF. The Scyther Tool: Verification, falsification, and analysis of security protocols. In : *Computer aided verification 20th International Conference*. Springer Berlin Heidelberg, 2008. vol. 5123, p. 414-418.

[76] BASIN, David et CREMERS, Cas. Modeling and analyzing security in the presence of compromising adversaries. In : *Computer Security–ESORICS 2010*. Springer Berlin Heidelberg, 2010. p. 340-356.

[77] JAVELLE, RIPERT, WLOKA. *Lecture 9: Tools and Applications* [en ligne]. 2009. [Consulté le 01 mars 2016]. Disponible sur : <http://www-verimag.imag.fr/~plafourc/teaching /Lecture_Note09/ Lecture9_Javelle_Ripert_ Wloka.pdf>.

[78] CREMERS, Cas. *The Scyther Tool* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <https://www.cs.ox.ac.uk /people/cas.cremers/scyther/>.

[79] KYBURZ, Adrian. *An automated formal analysis of the security of the Internet Key Exchange (IKE) protocol in the presence of compromising adversaries*. 2010. Thèse de doctorat. Master Thesis ETH Zürich, 2010.

[80] Graphviz. *What is Graphviz?* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <http://www.graphviz.org/>.

[81] LUGIEZ, Denis. *Vérification de protocoles cryptographiques, 14eme Rencontre Professeurs et Enseignants-Chercheurs* [en ligne]. 2005. [Consulté le 01 mars 2016]. Disponible sur : <http://informatique-sciences.univ-amu.fr/sites/informatique-sciences.univ-amu.fr/files/ article/14eme-rencontres-expose-lugiez.pdf >.

[82] DOLEV, Danny et YAO, Andrew C. On the security of public key protocols. *Information Theory, IEEE Transactions on Information Theory*, 1983, vol. 29, no 2, p. 198-208.

[83] CREMERS, Cas. *Scyther user manual* [en ligne]. UK : Department of Computer Science, University of Oxford: Oxford, 2014.

[84] LOWE, Gavin. A hierarchy of authentication specifications. In : *Computer Security Foundations Workshop, 1997. Proceedings., 10th*. IEEE, 1997. p. 31-43.

[85] WOO, Thomas YC et LAM, Simon S. A semantic model for authentication protocols. In : *Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on*. IEEE, 1993. p. 178-194.

[86] ORACLE. *S'informer sur la technologie Java* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <https://www.java.com/fr/about/>.

[87] UBUNTU-fr. *Netbeans* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <http://doc.ubuntu-fr.org/netbeans>.

[88] ORACLE. *What Is a Socket?* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <https://docs.oracle.com/javase/ tutorial/networking/sockets/definition.html>.

[89] EasyPHP. *Develop & Host* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <http://www.easyphp.org/>.

[90] TECHTARGET. *VMware Workstation* [en ligne]. [Consulté le 01 mars 2016]. Disponible sur : <http://searchvmware. techtarget.com/definition/VMware-Workstation>.

[91] RIVEST, Ronald L., SHAMIR, Adi, et TAUMAN, Yael. How to leak a secret. In : *Advances in Cryptology—ASIACRYPT 2001*. Springer Berlin Heidelberg, 2001. p. 552-565.

[92] SLAMANIG, Daniel. Anonymous authentication from public-key encryption revisited. In : *Communications and Multimedia Security*. Springer Berlin Heidelberg, 2011. p. 247-249.

[93] LI, Wenjuan et PING, Lingdi. Trust model to enhance security and interoperability of cloud environment. In : *Cloud Computing*. Springer Berlin Heidelberg, 2009. p. 69-79.

[94] GOVINDA, K. et RAVITHEJA, Perla. Identity anonymization and secure data storage using group signature in private cloud. In: *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*. ACM 2012. p. 129-132.

[95] SLAMANIG, Daniel. More privacy for cloud users: Privacy-preserving resource usage in the cloud. *Selected Papers from the 4th Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2011, p. 15-27.

[96] CHAUM, David L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 1981, vol. 24, no 2, p. 84-90.

[97] NEEDHAM, Roger M. et SCHROEDER, Michael D. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 1978, vol. 21, no 12, p. 993-999.

[98] BURROWS, Michael, ABADI, Martin, et NEEDHAM, Roger M. A logic of authentication. In : *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. The Royal Society, 1989. p. 233-271.

[99]: GOUBAULT-LARRECQ, Jean. *Sécurité, modélisation et analyse de protocoles cryptographiques* [en ligne]. France : 2002. [Consulté le 01 mars 2016]. Disponible sur : < http://www.Isv.ens-cachan.fr >.

[100] TURUANI, Mathieu. *Sécurité des protocoles cryptographiques: décidabilité et complexité*. 2003. Thèse de doctorat. IBM Zurich.