

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 Magistère

Filière : Informatique

Option : Cloud Computing

Thème

---

Authentification Anonyme  
dans un environnement Cloud

---

Soutenu le : xx / xx / 2016

Devant le jury composé de :

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

Année Universitaire : 2015/2016

### *« 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. Il propose plusieurs avantages et plusieurs opportunités dans le futur pour les utilisateurs (le plus souvent les entreprises). 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, dans le but d'assurer une protection optimale des données personnelles des utilisateurs. Cela grâce à une authentification anonyme garantissant une consommation anonyme des services Cloud et 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 d'authentification 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.

*« 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. It offers several advantages and opportunities in the future for users. 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.

## TABLE DES MATIERES

Introduction Générale .....	1
Chapitre 1: Sécurité et Privacy dans un environnement de Cloud Computing.....	4
1. Introduction.....	4
2. Le Cloud Computing .....	4
2.1. Définition.....	5
2.2. Historique .....	6
2.3. Architecture du Cloud Computing.....	7
2.4. Les modèles de déploiement dans le Cloud.....	7
2.5. Les modèles de services dans le Cloud «SPI MODEL».....	8
2.6. Les caractéristiques du Cloud Computing .....	8
2.7. Composants de base du Cloud Computing.....	9
3. Questions clés à propos de la sécurité dans le Cloud Computing.....	9
3.1. Challenges introduit dans un environnement de Cloud Computing .....	11
3.2. Les principales menaces de sécurité dans un environnement Cloud .....	12
3.2.1. Technologie partagée.....	12
3.2.2. Perte de contrôle et Perte de données .....	12
3.2.3. Usurpation d'identité .....	13
3.2.4. API non-sécurisée.....	13
3.2.5. Déni de service .....	13
3.2.6. Les intrus malveillants.....	14
3.3. Les attaques dans un environnement Cloud .....	14
3.3.1. Les attaques externes .....	15
3.3.2. Les attaques internes.....	20
3.4. Mécanismes de sécurité dans le Cloud .....	20
3.4.1. La sécurité physique dans le Cloud .....	20
3.4.2. La sécurité des données dans le Cloud .....	21
3.4.3. La sécurité logique dans un environnement Cloud.....	23
4. Gestion des identités et des accès dans le Cloud .....	25
5. Notion de protection des données personnelles ou « Privacy ».....	26
5.1. Aperçu et définition .....	26
5.2. Propriétés principales de la privacy .....	28
5.3. Privacy dans le Cloud .....	29

6.	Conclusion .....	30
Chapitre 2: Authentification et Authentification anonyme dans le Cloud.....		31
1.	Introduction.....	31
2.	Mécanisme d'authentification.....	31
2.1.	Définitions .....	32
2.2.	Classification des approches d'authentification.....	32
2.3.	Protocoles d'authentification .....	34
3.	Authentification dans le Cloud .....	36
3.1.	Aperçu du processus d'authentification dans le Cloud.....	37
3.2.	Méthodes d'authentification de base dans un environnement Cloud .....	37
3.2.1.	Nom d'utilisateur / Mot de passe .....	38
3.2.2.	MTM « Mobile Trusted Module ».....	40
3.2.3.	Infrastructure à clé publique .....	40
3.2.4.	SSO.....	40
3.2.5.	Authentification biométrique .....	41
3.2.6.	Authentification forte / multi-facteurs .....	41
3.3.	Solutions industrielles d'authentification dans le Cloud .....	42
3.3.1.	Principe de l'identité fédérée .....	42
3.3.2.	Frameworks d'Authentification et d'Autorisation.....	43
3.3.3.	Frameworks de gestion des identités: IAM «Identity Access Management».....	44
4.	L'Authentification anonyme dans le Cloud Computing.....	46
4.1.	Aperçu et définition .....	46
4.2.	Mécanismes d'authentification anonyme .....	47
4.2.1.	Authentification anonyme par mot de passe.....	48
4.2.2.	Authentification anonyme via PKE « Public key Encryption».....	48
4.2.3.	Signature de groupe « Groupe signature ».....	49
4.2.4.	Signature en aveugle « Blind signature » .....	50
4.3.	Anonymat et approches d'authentification dans le Cloud .....	51
4.3.1.	Anonymat et Authentification dans les environnements classiques .....	51
4.3.2.	Anonymat et Authentification dans le Cloud.....	51
	Approche 1: Cloud Anonyme « Anonymous Cloud ».....	52
	Approche 2: PCCP « Preserving Cloud Computing Privacy ».....	53
	Approche 3: Consommation anonyme des services Cloud SaaS.....	55
4.4.	Discussion et Comparaison.....	56

5.	Conclusion .....	57
Chapitre 3: Nouvelle Approche d'Authentification Anonyme Adaptative dans le Cloud .....		58
1.	Introduction.....	58
2.	Généralités: Définitions .....	59
3.	Etude du modèle de l'adversaire et informations sensibles .....	62
3.1.	Classification des menaces et des données sensibles à protéger dans le Cloud.....	62
3.2.	Représentation du modèle de l'adversaire .....	65
4.	Description de l'approche d'authentification anonyme proposée .....	66
4.1.	Architecture générale de l'approche d'authentification anonyme .....	67
4.2.	Acteurs et leurs rôles .....	69
4.3.	Modèle de base .....	69
4.3.1.	Etapas constituant le modèle de base.....	70
4.3.2.	Le gestionnaire d'enregistrement.....	71
4.3.3.	Le gestionnaire de tickets .....	73
4.3.4.	Le gestionnaire de services .....	75
4.3.5.	Protocole d'authentification et de communication .....	75
4.3.6.	Modèle de base : Limites.....	77
4.4.	Modèle étendu .....	78
4.4.1.	Etapas constituant le modèle étendu.....	78
4.4.2.	Les gestionnaires (Différents Managers).....	80
4.4.3.	Protocole d'authentification et de communication .....	83
4.4.4.	Algorithme d'authentification anonyme proposé .....	84
4.4.5.	Modèle étendu : modèle de l'adversaire .....	85
5.	Synthèse et contribution .....	86
6.	Conclusion .....	87
Chapitre 4: Validation et Implémentation du Protocole .....		89
1.	Introduction.....	89
2.	Vérification et Validation du protocole AnonCloud.....	89
2.1.	Du modèle formel à l'automatisation .....	89
2.2.	Outil utilisé lors de la validation du protocole AnonCloud .....	90
2.3.	Modèle de l'adversaire .....	93
2.4.	Propriétés de sécurité.....	95
2.5.	Script d'entrée.....	96
2.6.	Attaques contre le protocole AnonCloud sans clés de sessions.....	100

2.7. Résultat .....	104
3. Implémentation du protocole AnonCloud .....	106
3.1. Outils utilisés .....	106
3.2. Les interfaces .....	106
3.2.1. Interfaces Utilisateurs .....	107
3.2.2. Opérations effectuées par le serveur RTM .....	110
3.2.3. Opérations effectuées par le serveur SM .....	111
4. Conclusion .....	113
Conclusion Générale.....	114
Bibliographie .....	116