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	Examinateur
Mme BENZAID Chafika	MCA	USTHB, Alger	Examinatrice
Mme BENMEZIANE Souad	CR	CERIST	Invitée

Année Universitaire : 2015/2016

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. 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.

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. 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