Journal of Information Security and Applications 63 (2021) 102975

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Secure encryption key management as a SecaaS based on Chinese wall security policy

Saad Fehis [a,*], Omar Nouali [b], Tahar Kechadi [c]

[a] Ecole nationale Supérieure d'Informatique, BP 68M, 16309, Oued-Smar, Alger, Algeria[1]
[b] Research Center on Scientific and Technical Information Algiers, Algeria[2]
[c] University College Dublin School of Computer Science and Informatics, Dublin, Ireland[3]

ARTICLE INFO

Keywords:
Cloud computing
SecaaS
Encryption key management system
Chinese wall security policy

ABSTRACT

Cloud computing has become very popular and many mobile IT users are accessing business data and services without going through corporate networks. In this context the common security mechanism of most services and interactions is based on the encryption/signing keys, which themselves depend highly on the cryptographic key management system (*CKMS*) itself. Outsourcing CKMS to the cloud Computing as a trusted security as a service (*CKMS_SecaaS*) remains a real challenge, which we deal to the establishing of the trust between customers and service providers problems. To deal with this challenge we have proposed an approach that provides a CKMS_SecaaS based on the trusted platform module (*TPM*), which is the foundation for the trust, keys generation, and SecaaS authentication.

In this paper, we propose an approach for keys security based on Chinese Wall Security Policy (*CWSP*) as a dynamic firewall mechanism, which it is for access and information flow control. We note that, the TPM with CKMS_SecaaS are considered a real shared environment, they host and manage a lot of objects (*keys and related data*), objects belong to different users groups, and they are considered sensitive data (*encryption keys*). Therefore, the CWSP is a very interesting candidates to our context, which it provides the creation of walls between companies' objects based on an access control rules.

1. Introduction

Providing an IT services today is enhanced thanks to the evolution in computing architecture known as Cloud Computing (*IaaS, PaaS, SaaS*) [1]. Cloud computing has many advantages such as : Resources usage flexibility (*CPU, storage, network*), pay as you use, high performance of its resources, and no maintenance, thereby increasing number of its users and cloud-based services (*such as salesforce.com or Google Apps*). This means that many mobile IT users will have access to business data and services without going through corporate networks.

Consequently, the need for enterprises to place security controls between mobile users and cloud-based services or between services themselves will increase too. As a result, new offers of a Security as a service (*SecaaS*) will emerge [2]. These services include identity and access management (*IAM*), and cryptographic key management system (*CKMS*), etc. [2,3]. In this context, the security of the majority services and interactions is based on the encryption/signing keys, which are themselves dependent on the security of CKMS itself. Therefore, CKMS as a SecaaS (*CKMS_SecaaS*) is the main focus of this work.

Cloud computing is a multi-tenancy environment, it is based on shared of pooled of resources [4]. It has many security issues, which it is one of the main problems when adopting SecaaS in the Cloud-Computing [5,6]. In this context, the most related works to SecaaS revolve around definitions, modeling specification, or the implementation of the security services [3,7–12]. They consider the provider as a trusted party, or ignored its trustworthy. However, in the real-world, this is not always true (*Encryption key is a sensitive data*).

Therefore, the purpose or the challenge matter of this work is to consider the creation (*or implementation*) of trust between customers and providers which has an important impact in outsourcing the SecaaS to Cloud Computing. Consequently, establishing trust between customers and service providers is crucial, and it is an urgent need.

So, we need to seek answer to these inquiries: (**1**) The CKMS_SecaaS is trusted service and not a malware (*authentication problem*), (**2**) Keys

* Corresponding author.
E-mail addresses: s_fehis@esi.dz (S. Fehis), onouali@cerist.dz (O. Nouali), tahar.kechadi@ucd.ie (T. Kechadi).
[1] www.esi.dz.
[2] www.cerist.dz.
[3] www.ucd.ie.

https://doi.org/10.1016/j.jisa.2021.102975

Available online 26 October 2021