Rijndael Encryption Technique for User Authentication in Cloud Computing

[1]Firkhan Ali Bin Hamid Ali and [2]Md Yazid Mohd Saman
[1]Fakulti Teknologi Maklumat & Multimedia, Universiti Tun Hussein Onn Malaysia. 86400 Parit Raja, Johor, Malaysia
[2]Jabatan Sains Komputer, Universiti Malaysia Terengganu K. Terengganu Malaysia
(Email: firkhan@uthm.edu.my)

1. Introduction

Cloud Computing (CC) refers to applications & services that run on a distributed network [1,2]. It uses virtualized resources and hosted services are accessed or delivered over the Internet. The main two characteristics of cloud computing are: (a) virtualization - resources are virtual and limitless (b) abstraction - details of physical systems on which the software are run are abstracted from users. There are three categories of CC: (a) Infrastructure-as-a-Service (IaaS), (b) Platform-as-a-Service (PaaS) and (c) Software-as-a-Service (SaaS).

The US NIST definition of CC is that it is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3]. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. Figure 1 shows the model of CC.

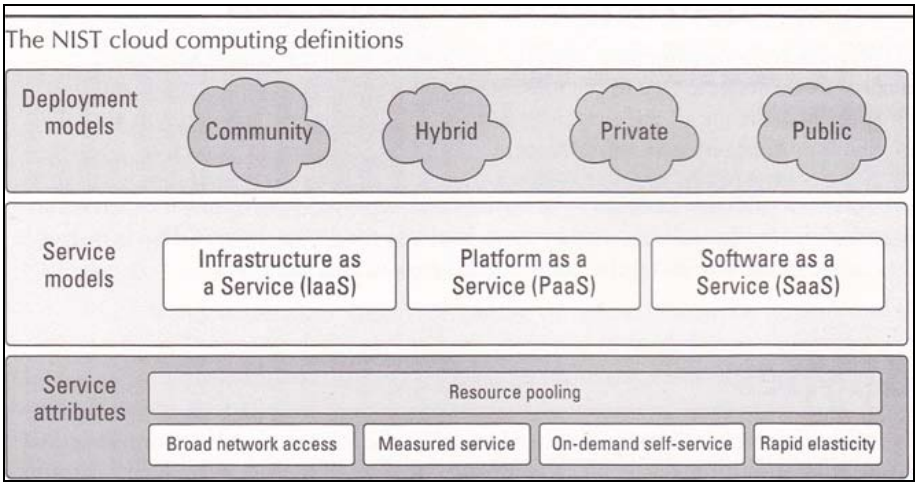

Figure 1: Cloud Computing Model [1]

Figure 2 show the four deployment models of CC. They are Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud [1, 2]. A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. For a Private cloud, also called internal cloud or corporate cloud, it refers to a term for a proprietary computing architecture. It provides hosted services to a limited number of people behind a firewall.

The combination of at least one private cloud and at least one public cloud gives the Hybrid Cloud. It can be an on-premises private cloud or a virtual private cloud located outside the enterprise data center. The simplest macro views of a hybrid cloud - a single on-premises private cloud and a single off-premises public cloud.

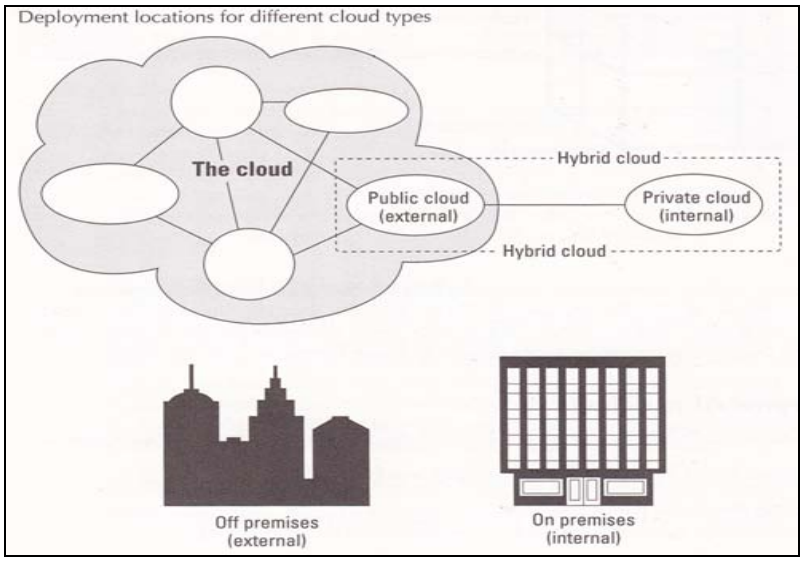

Figure 2: Cloud Deployment Models [1]

2. Security in IaaS @ CC

The Infrastructure as a Service (IaaS) model is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components [1,2,3]. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Some examples of IaaS service providers are Amazon Elastic Compute Cloud (EC2), Eucalyptus, GoGrid, FlexiScale, Linode, RackSpace Cloud and Terremark. In Figure 3, the Cloud reference Model is shown [1]. It shows that for the IaaS category, the needs for authentication and security are highlighted [4].

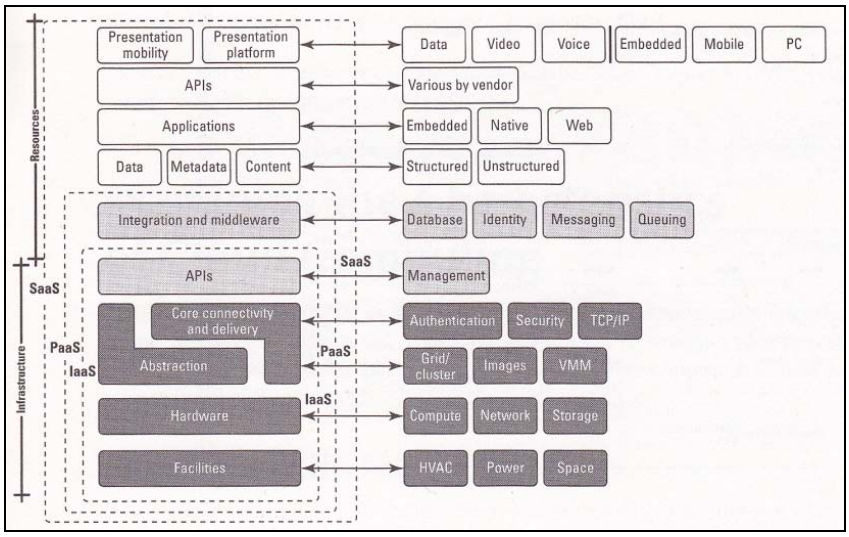

Figure 3: Cloud Computing Model [1]

3. Development of PMS-R

A system called Password Management System (PMS-R) has been developed. This could be deployed on the IaaS category of CC. This system focuses on managing password for all files in computers. This could be useful for the authentication of users in the Cloud. It has been developed based on Rijndael's encryption technique [5].

< half-page details of Rijndael's encryption technique>

This system is able to secure the usage of password for files and software from any threats. This system has one main password for all computers' files. This is important to avoid any failure occur in this system. There are several modules in this system as state in Table 1.

Table 1: Modules in PMS-R

Index	Module	Decription
1	Registration	This is a first module that experience by user to access other modules in PMS-R system. User information is required in this module.
2	Password Recovery	This module will keep recovery support to get back any lost password.
3	Password Management	This is a main module to secure all files with one encryption password.

The system is able to have a systematic password management system. With that, it will secure all the files by using encrypted password. This information system had provided user-friendly interface to perform all the functions in the modules. The modules are including user log in, registration, password recovery and password management with encryption functional. Figure 4 shows the new user registration interface for this system. A user is allowed for a one time registration only. He needs to provide individual information during the registration. With that, a user can use all the functions that have in this information system. He can manage all file with the encryption password through this system.

Figure 4: Interface for registring new user

In Figure 5, the interface for password recovery is depicted. A user needs to input his name, a question and the correct answer to get back the loss password. The interface for file management with encryption password is shown in Figure 3. User can select any files to secure with this encryption password. The process of encryption and decryption will be doing at this space of interface. In this module, there are several functions such “Secured Files & Folders”, “Unsecured Files & Folder”, “Ungroup Files & Folders” and “Account Info”.

Figure 5: Recovering a password

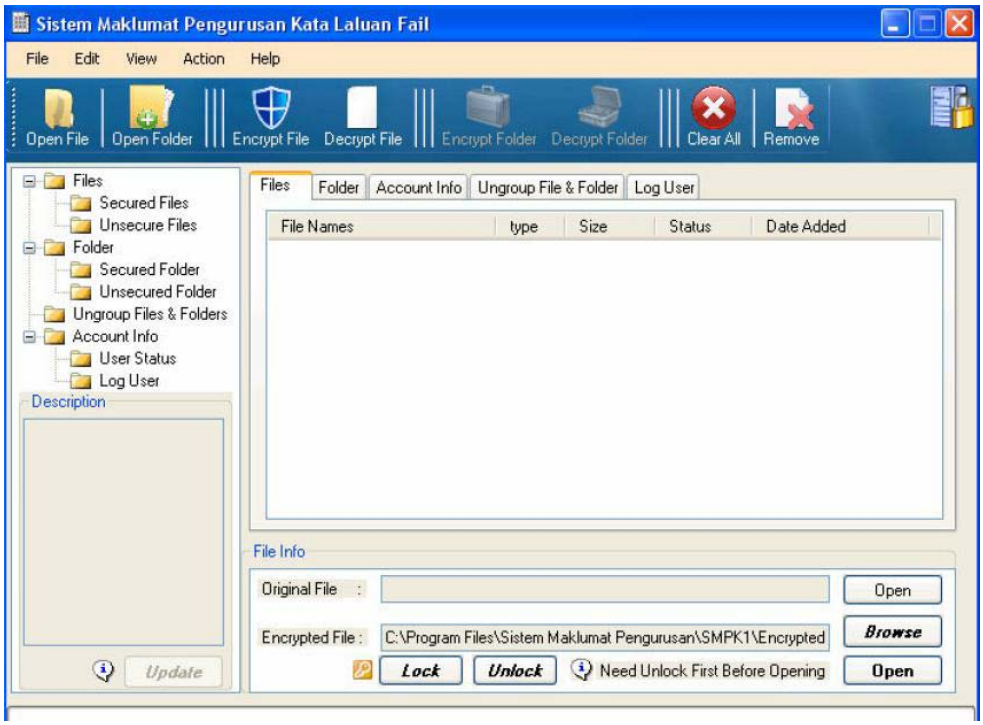

Figure 3: Encrypting password

5. Conclusion

IaaS @ Cloud Computing has provided utility computing, service and billing model, automation of administrative tasks, dynamic scaling, desktop virtualization, policy-based

services and Internet connectivity. However these may pose severe security issues [4]. The Password Management System (PMS-R) developed and discussed in this paper may provide an environment that make it easier for users to manage all the files. With a good encryption technique, it will secure all the files by using encryption and decryption.

6. References

[1] Sosinsky, R (2011), Cloud Computing Bible, Wiley

[2] Buyya, R, Broberg, J. & Goscinski, A. (2011), Cloud Computing, Principles & Paradigms, Wiley

[3] Cloud Computing NIST http://www.nist.gov/itl/cloud/ retrieved on 1 April 2011

[4] Krutz, R. L. and Vines, R. D. (2010), Cloud Security : A Comprehensive Guide to Secure Cloud Computing, Wiley

[5] REF ON Rijndael's encryption technique