ISSN 2320 2629
Volume 9, No.6, November - December 2020
International Journal of Information Technology Infrastructure
Available Online at http://www.warse.org/IJITI/static/pdf/file/ijiti01962020.pdf
https://doi.org/10.30534/ijiti/2020/01962020

Rijndael Encryption Technique: Authentication for Computer Application

Firkhan Ali Bin Hamid Ali[1], MohdKhairul Amin Bin Mohd Sukri[2], MdSyukri Mohamad[3]
[1]Universiti Tun Hussein Onn Malaysia, Malaysia, firkhan77@yahoo.com
[2]UniversitiTun Hussein Onn Malaysia, Malaysia,
[3]UniversitiTun Hussein Onn Malaysia, Malaysia

ABSTRACT

Password Management System is used for file protection and encryption file process can be done in computer application especially through the cloud computing environment. This approach has been adapted or implemented in various managements to secure application in computing. This system functions to help the application computing users to protect information using priority password without having difficulty. The system had done for protection system information process. An activation to encrypt files to increase the best and systematic services to the organization management in application computing. After all, the result was reached the goals that punctual the file protection to encrypt file through cloud computing environment.

Key words : Password, rijndael encryption, computer application, authentication

1. INTRODUCTION

Application Computing 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 Cloud Computing: (a) Infrastructure-as-a-Service (IaaS), (b) Platform-as-a-Service (PaaS) and (c) Software-as-a-Service (SaaS).

The US NIST definition of Cloud Computing is that it is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as 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 Cloud Computing.

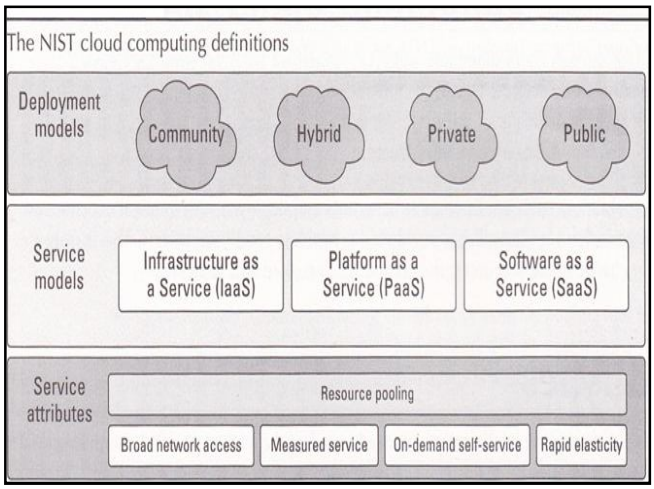

Figure 1: Cloud Computing Model (Sosinsky, 2011)

Figure 2 show the four deployment models of Cloud Computing. 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.

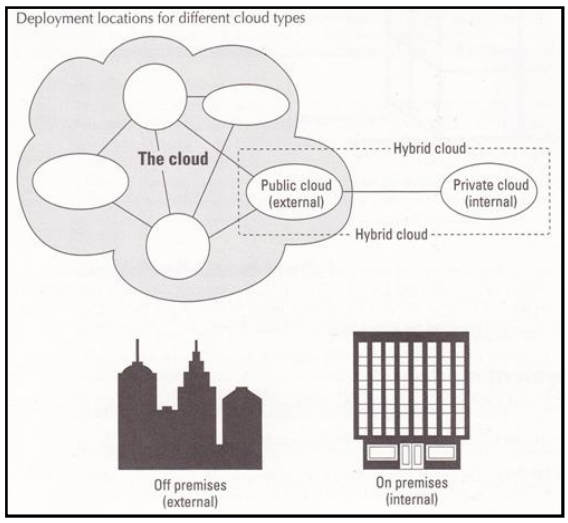

Figure 2: Cloud Deployment Models (Sosinsky, 2011)

2. SECURITY IN CLOUD COMPUTING

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].

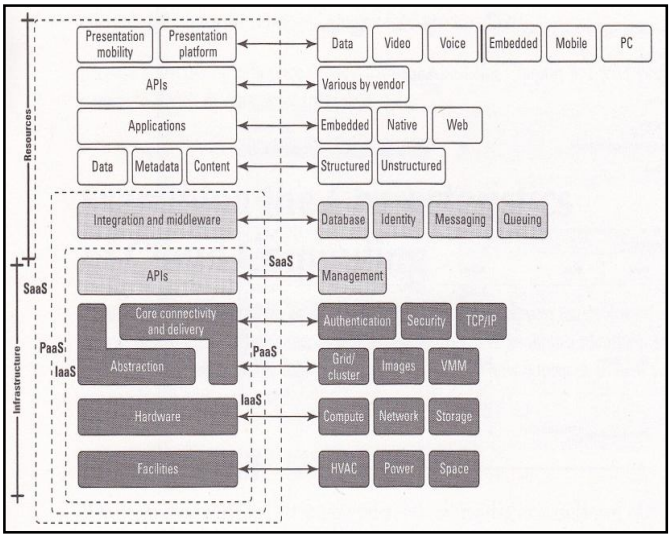

Figure 3: Cloud Computing Model (Sosinsky, 2011)

3. RIJNDAEL BASED PASSWORD MANAGEMENT SYSTEM

A system called Rijndael based Password Management System has been developing. This could be deploying on the IaaS category of Cloud Computing. 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 develop based on Rijndael's encryption technique [5].

Advanced Encryption Standard (AES) is base on the design of Substitution permutation network architecture. Method that use for the process of AES is Rijndael. It determines by much number of blocks with the main size, double of 32 bit from minimum number of 128 bit until the maximum number of 256 bit. Rijndael Cipher is one of the technique for cryptography.

The process of encryption will convert from the form of plain text to the Ciphertext. If the data in form of Ciphertext is decrypt, it converts data into plain text form.

By using password with Rijndael Cipher, encryption technique will secure all the data in the computer [6]. The process of the technique has state in the following Figure 4.

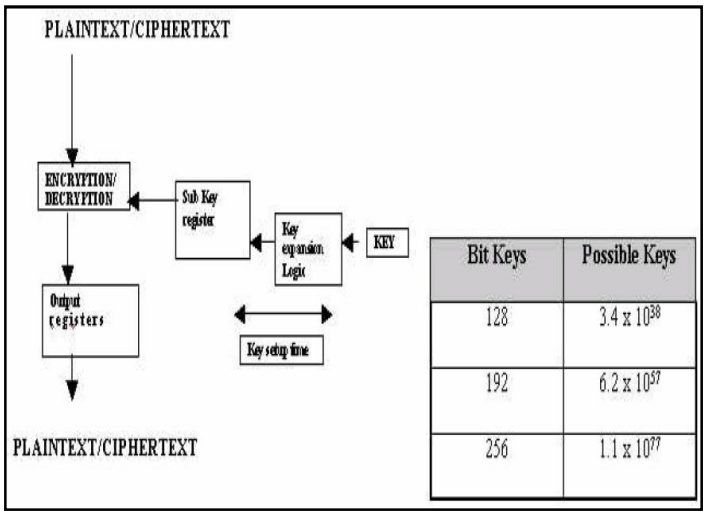

Figure 4: Process of Encryption/Decryption in Rijndael

In Figure 5, it shown about the step for each byte in the array by using a method of substitution box, Rijndael S-Box. This operation had provided a non-linearity form of chipper. The usage of this S-Box is use multiplicative inverse in gf (2 powers of 8) technique.

The avoidance from algebraic behavior in S-Box, it built with combination of reverse function and invertible affine transformation. This transformation steps are know as SubBytes technique.

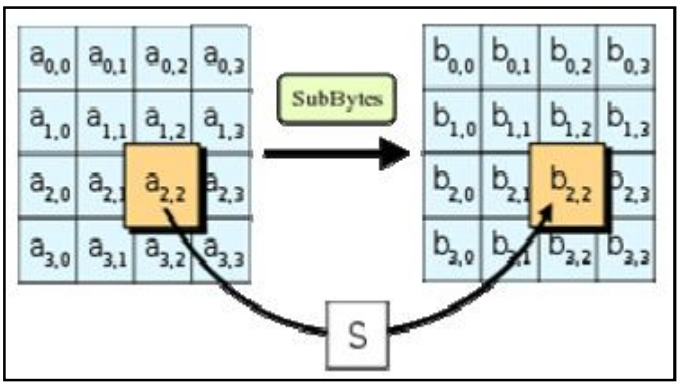

Figure 5: Transformation Steps in SubBytes

In Figure 6 is about the process of combination in reverse function and invertible affine transformation.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 6: Combination of the process S-Box and SubByte

4. IMPLEMENTATION OF PASSWORD MANAGEMENT SYSTEM

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 the 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 7 shows the new user registration interface for this system. A user is allowing 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 7: Interface for registering new user

In Figure 8, the interface for password recovery is depicting. 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 show in Figure 9. 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 8: Recovering a password

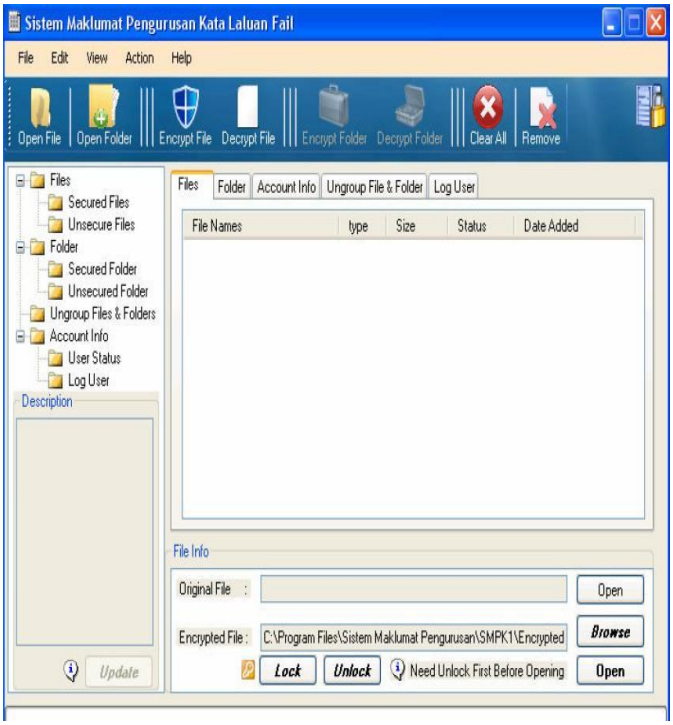

Figure 9: Encrypting password

5. CONCLUSION

IaaS in 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 (Krutz*etc*, 2010).

The Rijndael based Password Management System 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.

ACKNOWLEDGEMENT

Thanks to UniversitiTun Hussein Onn Malaysia for sponsoring this article.

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. J. Daemen, "Computer Security Standard, Cryptography, Advanced Encryption Standard (AES) ", http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (26 November 2001)
6. Jonathan Pierce (2007), An Efficient Heuristic for Security against Multiple Adversaries, http://teamcore.usc.edu/papers/2007/aamas07security.pdf (18 May 2007)