The 2nd East Indonesia Conference and Information Technology (EIConCIT) 2018

Enhancing Cloud Data Security using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms

1st Salma
Electrical and Computer Engineering
International Islamic University
Kuala Lumpur, Malaysia
mirsalma12@yahoo.com

2nd Rashidah Funke Olanrewaju
Electrical and Computer Engineering
International Islamic University
Kuala Lumpur, Malaysia
frashidah@iium.edu.my

3rd Khaizuran Abdullah
Electrical and Computer Engineering
International Islamic University
Kuala Lumpur, Malaysia
khaizuran@iium.edu.my

4th Rusmala
Faculty of Computer Engineering
Cokroaminoto Palopo University
Palopo, Indonesia
rusmala@uncp.ac.id

5th Herdianti Darwis
Faculty of Computer Science
Universitas Muslim Indonesia
Makassar, Indonesia
herdianti.darwis@umi.ac.id

***Abstract*—Cloud computing is an IT model that offers a large number of storage space, unbelievable computing power and inconceivable speed of calculations. There are a number of costumers like corporate components, social media programs and individual customers are all moving towards to the vast area of cloud computing. The importance of cloud computing comes out with the security of data accessibility, reliability and reliability of information. The verification and permission is more necessary to access information as "cloud" is only assortment of actual super computer speed through the world. There are many research has been done on security of file encryption with AES algorithm. There is no any successful attack yet against AES but because of a higher increasing of cybercrime it could be possible attack on it like brute force attack and algebraic attack. Hence, in this research has been proposed a hybrid structure of Dynamic AES (DAES) and Blowfish algorithms. This procedure specifies the security of uploaded file on the cloud with a strong encryption method and also the privacy and reliability of submitted information of a user with considering performance of speed.**

***Keywords*—security, cloud computing, encryption, Hybrid algorithm, AES, DAES, Blow fish.**

I. INTRODUCTION

Cloud computing is rising as [1] a key handling system for sharing resources that consist of facilities, software ,applications, and business procedures. Gartner predicts by 2015, 10% of overall IT protection business abilities will be delivered in the cloud, with concentrate on messaging, web Protection and distant weaknesses evaluation. Other concentrate areas will include data-loss protection, security, and verification, as technological innovation targeted to support cloud processing older [2] Cloud computing offers an extensive advantages for customers like speciously endless storage space, fast computing power, a vast range of programs and the ability of easily sharing information among the world. Consumers can get the advantage of accessibility via internet browser from any place and any time once he/she has access to the internet. A large ATM network ongoing being well-known to as cloud in the early of 90's. Cloud computing is a type of Internet-based handling that provides distributed pc handling sources and information to computers and other devices when needed. It is a model for allowing popular, on-demand access to a distributed pool of configurable handling sources (e.g., pc networks, web servers, storage space, applications and services), which can be rapidly provisioned and released with minimal management effort, Fig. 1. This paper begins with the introduction about the research background in Section I. While in Section II, the cloud services are explained and the cloud security issues are included in Section III. In further sections, explanation of algorithms, literature reviews of previous works are mentioned, and the proposed methodology is included in the next section. This paper is ended up with the conclusion and future works.

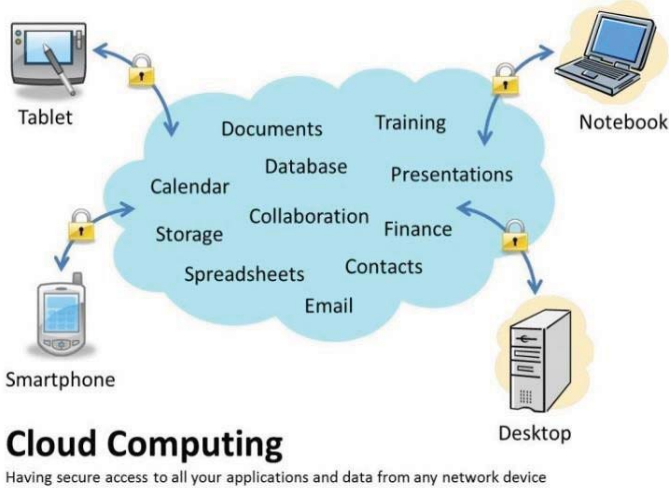

Fig. 1. *Cloud Computing architecture*

II. Cloud Services

There are a lot of researches have been done till now about cloud services. The services can be divided into three main categories: Platform as a service (PaaS), Software as a Service (SaaS), Infrastructure as a service (IaaS). The descriptions are as follows, Fig. 2.

A. Software as a Service (SaaS)

It is the best part in the collection and can be found above the PaaS layer. It provides implementation of the result or application or some web programs on the IaaS and PaaS solutions. SaaS provides accessibility to different customers through some system, probably via an online system. The help of this part is recognized and controlled by the consumers. The certificate to these solutions may be a registration centered or an utilization centered. The consumer may increase the solutions (subscription as well as scalability) centered on the importance.

B. Platform as a Support (PaaS)

PaaS can be found above the IaaS in the collection. It deals with an offering growth as well as deployment choices to the customers. It generally provides a setting for creating the applying with some built-in resources which have some predefined features which help the customer to develop the program as per need. Also, once the application is designed, it may be implemented within the same atmosphere. It also facilitates leasing of sources and the customers have to pay as per the utilization.

C. Infrastructure as a Service (IaaS)

This is the bottom-most part of reasoning processing of collection and provides the customers with various components features such as storage space, processor chips, servers, and social media and as well as some application features like virtualization and computer file system. It allows the customers to provide sources when needed.

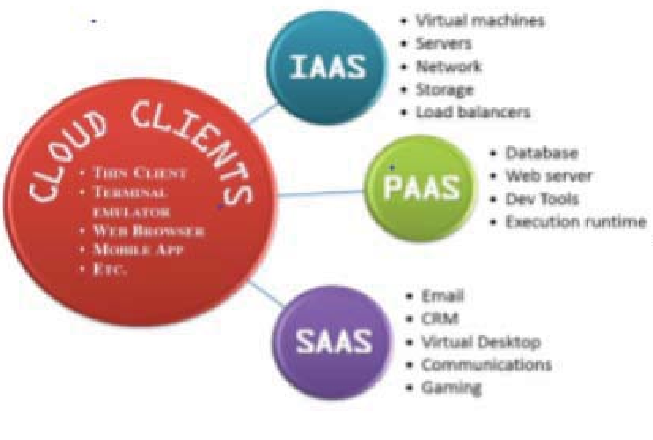

Fig. 2. Cloud Services

III. Cloud Computing Security Issues

One of many issues that have been encountered by most of the cloud service providers is security. As cloud computing opens the possibilities of the services being accessed via millions of machines over the internet, this situation also opens up the possibility of data breaches by an outsider, Fig. 3.

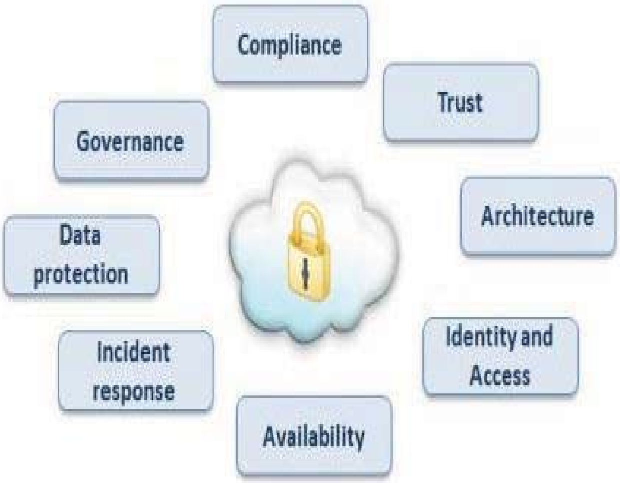

Fig. 3. *Cloud Computing architecture*

If a multitenant cloud service database contains even a single flaw, it is likely possible for a malicious hacker to penetrate the system and this will eventually leads to the client's data being stolen. Another problem would be data loss; data disappearing without a trace. This might due to the carelessness of the service provider itself or even the involvement of malicious hacker in deleting the target's data. Cloud service provider should also worry about the possibility of service traffic hijacking. This might happens if the intruder gains some sort of access to the credential of the system, then he or she might have the access to make transactions, manipulate data, redirect the clients to illegitimate websites or even return falsified information. Another problem when using cloud computing would be malicious insider whom can be an exemployee or even a current employee, a contractor, or even a business partner who have the access to the system with bad intentions. In short, cloud computing is very risky and to invest using the cloud computing as a medium is not a good idea.

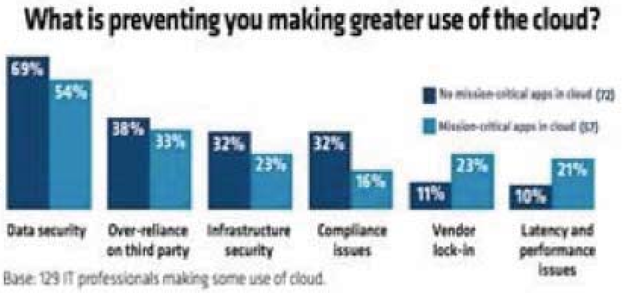

Fig. 4. Prevention of Making Greater Use of the Cloud

According to the threat of security, cloud computing has been continuously increasing. This brings to a serious concern among the consumers regarding the availability of their data as well as the mechanism of access in the environment of cloud computing. Fig. 4 shows the result of a survey done by Leonard 2012, towards 129 IT professionals who have tried to make the best uses of cloud computing services. They have tried to move important functionalities to the cloud and the survey was done after their experiences with cloud. It is clear that based on the survey, data security is of their main concern. This shows that consumers need to be assured regarding the security issues of cloud computing for a much secure cloud computing environment. Therefore, to encounter the problems changes in terms to secure the security of cloud computing for better and safety usage that can ease the clients need to be applied. One way to do this is by encrypting the data so that it is safe and cannot be wrecked by the other malicious attacker. To do this, we will need an algorithm that can encrypt the data and can only be decrypt by the user himself. Hence, the keys to decrypt the data must be kept by the users only and cannot be used by others to prevent data theft.

IV. Algorithms Explanations

A. Advanced Encryption Standard (AES)

AES encrypts and decrypts a 128-bits data block and can use 10, 12 0r 14 rounds. Based on these rounds, 128, 192 and 256 bits key size will be used yet however the round keys are always 128 bits long. There are also three main operations performed in AES algorithm which are Encryption, Decryption and key Generation.

1) Encryption Process

a) The key size as well as the plaintext is obtained for encryption.

b) Pre-Round transformation is performed on the plain text

c) 'n'rounds are performed depending on the key size.

d) The cipher text is obtained after 'n' rounds.

2) Decryption Process

In order to perform decryption, all the steps in encryption is performed in reverse order.

Key Generation:

a) Get the key

b) Number of words needed is computed based on the number of rounds.

c) The first four words of 4 bytes array are created based on the key.

d) The next word is obtained by performing Root word and Sub word.

e) Step 4 is then repeated in order to reach the required number of words.

B. Blowfish

Blowfish is a key symmetric block cipher. It has 64-bit block size and the key length varies from 32 bits until 448 bits. It uses a large key dependent S-boxes as well as experience a 16 round Feistel cipher process. The main three operation of Blowfish algorithm are the same as DES algorithm which are Encryption, Decryption and key Generation. The algorithm steps of Blowfish.

1) Encryption Process

a) X is divided into two parts with equal 32-bit which are XL and XR

b) From round 1 until round 16, new XL=XL XOR XR, new XR=F(XL)

c) XOR XR< and XL and XR is swapped.

d) 3. XL and XR are XOR ed with P17 and P18

e) 4. New XR=XR XOR P17 while new XL=XL XOR P18

f) 5. XL and XR is Combined.

2) Decryption Process

P1 until P18 are used in reverse order but in the same process like in encryption process.

Key Generation:

a) P-array is initialized first and then the S-boxes. The string used must be fixed and consist of hexadecimal digits of pi.

b) P1 is XOR ed with the first 32 bits of key while P2 with the second bits. This step is repeated for all bits of key until the entire P-array is XOR ed with key bits.

c) All-zero string will be encrypt using the keys in step 1 and 2.

d) P1 and P2 is replaced with the output of step 3.

e) The output is then encrypted with the modified sub keys.

f) P3 and P4 are replaced with the latest output.

g) The process is repeated until all entries of P-array is replaced and S-boxes are all in order.

V. Previous Work

It is suggested in [3] that a simple information protection design in which that information is secured is proposed using Innovative Security Standard (AES) before it is released in the cloud. This guarantees information privacy and protection.

A security mechanism AES has been proposed in this research. Although it has been done well about data leakage but it has not been identified about specific attack and also computational cost is higher [4].

A privacy-preserving public audit system for information space for storage protection in cloud processing is designed, although the computational time is improved but the comfort is maintained where information is saved in the cloud by using the most popular algorithm AES [5].

An apparent data ownership to provide the reliability of information is suggested by [6]. It is a cooperative apparent information ownership strategy in multiple clouds. It provides quantify ability of service and information migration, and flexible store and preserves the clients' information. It desires less expense so as that interaction quality is also reduced.

A comparative study has been done in this research among AES, DES and Blowfish algorithms. It can be seen that Blowfish algorithms has best performance on speed among these three but there is no any discussion about security on various attacks and it could be done the performance on networks [7].

Comparative analysis between AES and Rc4 algorithm has been done based on variable key size and packet size. It can be seen that rc4 has better performance on time ,memory and also for throughput where AES has poor performance [8].

This paper presents a crucial comparison among AES, DES, Blowfish, RC6, 3DES and RC2 .This comparison has been conducted on different settings for each algorithm such as data blocks, battery power consumption, data size and on encryption/decryption speed. Finally it could be concluded that blowfish has the best performance on changing packet size comparing others algorithm shown in experimental result. The performance could be compare on security on different attack also [9],[10].

In other literature, a strategy that studies the development and processes programming design reliable with the present-used cloud computing system is proposed. It provides illustrations to explicate the method of development and its changing guidelines, as well as the method within that services and resources exchange. It also offers clarification of cloud computing. However social network could increase the QOS through ever-changing the service load are discussed in.

VI. Proposed Work Hybrid Algorithm Process

We endorse a configuration in this unit that hold a securing of Information file which is existing on the information file will be secured based on hybrid of DAES and Blowfish algorithms Fig. 4 and Fig. 5.

To make the AES more secure will enhance slightly in s-box structure. At first will do the transformation and then will process the inverse of multiplication. It could be more secure to AES to break the key by a third party. Thus the client can attain any of the submitted encrypted files and study on it. The benefits of hybrid of DAES and Blowfish are many against unbelievable power attack. The security key dimension used by AES criteria is of the order of the 128,198 or 256 bits which outcomes in massive amount of permutation and mixtures because of this, it is not an easy job the incredible power attack even for an extremely computer.

Where Blowfish has 64-bit block size and the key length varies from 32 bits until 448 bits. It uses a large key dependent S-boxes as well as experience a 16 round Fiestel cipher process.In this work blowfish will be useful to extend the key size. Thus, its make an excellent choice for security of information on the cloud.

General steps for our proposed hybrid algorithm are as follows:

Step 1: Start

Step 2: Initialize block size and key size

Step 3: Select preferred key size or key length.

KL= [KEY size of AES and Blowfish]

Step 4: KL= total of key size of hybrid algorithms

Step 5: Select file to be encrypted

Step 6: Enter the generated key and encrypt

Step 7: Select the encrypted file for decryption

Step 8: Decrypt cipher text to obtain original file

Step 9: Stop.

To be details, this algorithm will be divided into two process; upload and download files which are described in the following subsections.

A. *Upload File*

The steps for the computer file upload process are described as follows:

- Login a registered user with the correct password.
- Else verification error.
- File acquisition from computer that want to upload in the cloud.
- Process with DAES for encrypting the file.
- Get the encrypted file along with a key.
- Add blowfish for hybrid of encryption.
- Determine the hybrid algorithm for security.
- Submit the computer file to the cloud for storage in the cloud successfully.
- Confirm file for the uploading on to the cloud.
- Else delete file.

B. *Download File*

The steps for the computer file download process are described as follows:

- Login user with correct username and password to receive the file from the cloud.
- Check the validity of the user.
- If the user is valid can receive the encrypted file from the cloud
- Else show a message with wrong username or password.
- Apply the decryption algorithm to get the plaintext.

- Receive file. Logout and disconnect the connection with the cloud.

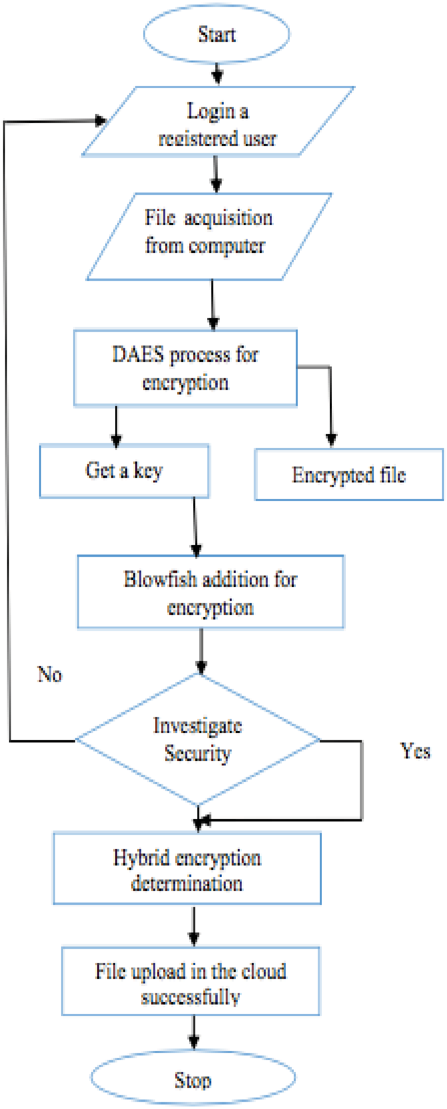
Start
Login a registered user
File acquisition from computer
DAES process for encryption
Get a key
Encrypted file
Blowfish addition for encryption
No
Investigate Security
Yes
Hybrid encryption determination
File upload in the cloud successfully
Stop

Fig. 5. The process of file upload

VII. Preliminary Results

In this research, we expect to have the result of a security structure of information file in cloud computing based on a hybrid algorithm. The time taken might be less in proportion of a better security against various attacks compared to encrypting using only one type of algorithm as only the chosen characteristics that would be applied in the system. Thus, it should be done to hybrid these algorithms and could be implemented in the future.

VIII. Conclusion And Future Works

Cloud computing is a question that any person can explore. It is like an innovation like any other technology but it has as super- fast technology which contain unlimited storage space, a vast range of program to use. Oppositely, various security threats appear such as confidentiality violation, no availability of information and restricting of information. In this document, we have proposed a structure which encrypted file with hybrid algorithms like AES (DAES) and Blowfish before submitting the file in the cloud. This proposal could be resolve the risk of information file from various attacks like brute force and algebraic attack because it provides a validation of authentication structure to access the file from the cloud. Thus if it is using safely, will provides an awesome advantage and overcome the disadvantages of the risk of security.

Our proposed system can incorporate to exchange data securely with any of social sites in its encrypted form. This Hybrid mechanism can be used to encrypt for any kind of text file, audio and video file too. The simulation tool can be using Cloud Sim in NetBeans IDE.

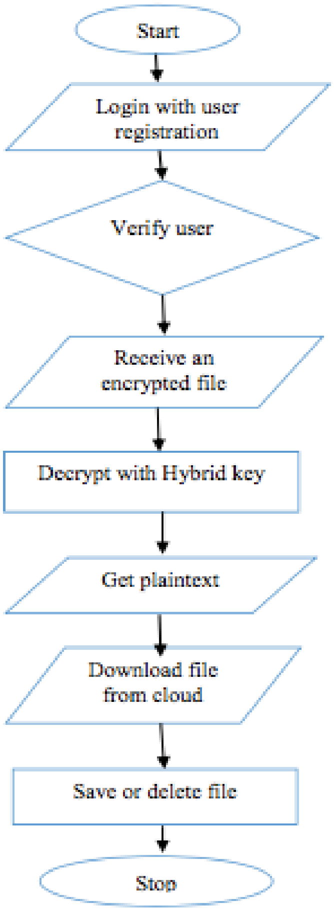

Fig. 6. The process of file download

REFERENCES

[1] R. Gupta, “Enhanced Security for Cloud Storage using Hybrid Encryption,” vol. 2, no. 7, pp. 2710–2713, 2013.

[2] N. Gajra, “Private Cl loud Security : Secured user Authenticatio on by using Enhanced Hybrid Algorithm,” 2014.

[3] A. Sachdev, “Enhancing Cloud Computing Security using AES Algorithm,” vol. 67, no. 9, pp. 19–23, 2013.

[4] S. P. Jadhav and P. B. R. Nandwalkar, “Efficient Cloud Computing with Secure Data Storage using AES,” vol. 4, no. 6, pp. 2–6, 2015.

[5] R. Arora and A. Parashar, “Secure User Data in Cloud Computing Using Encryption Algorithms,” vol. 3, no. 4, pp. 1922–1926, 2013.

[6] P. V Nithyabharathi, T. Kowsalya, and V. Baskar, “To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES,” vol. 3, no. 2, 2014.

[7] J. Thakur and N. Kumar, “DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis,” vol. 1, no. 2, pp. 6–12, 2011.

[8] N. Singhal and J. P. S. Raina, “Comparative Analysis of AES and RC4 Algorithms for Better Utilization,” pp. 177–181, 2011.

[9] D. Salama, A. Elminaam, H. Mohamed, A. Kader, and M. M. Hadhoud, “Evaluating The Performance of Symmetric Encryption Algorithms,” vol. 10, no. 3, pp. 213–219, 2010.

[10] Li, Jin, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang. "Secure attribute-based data sharing for resource-limited users in cloud computing." Computers & Security 72 (2018): 1-12.