IOP Conf. Series: Materials Science and Engineering **732** (2020) 012044 doi:10.1088/1757-899X/732/1/012044

Security system design for cloud computing by using the combination of AES256 and MD5 algorithm

L Khakim[1,*], M Mukhlisin[2] and A Suharjono[1]

[1] Department of Electrical Engineering, Politeknik Negeri Semarang, Semarang, Indonesia
[2] Department of Civil Engineering, Politeknik Negeri Semarang, Semarang, Indonesia

*khakimthy@gmail.com

Abstract. Data is a collection of information that is combined into one and has a very important meaning. In the study, the object to be secured is the password data , the encryption method Advanced Encryption Standard (AES) with a key length of 256 bits, before the data is encrypted with method of AES, the first password will be encrypted using MD5 , and the second one will be encrypted again using the AES256 method. Based on trial data conducted through two sites about the complexity of passwords, it can be concluded that the original data (before encryption) no 1 to 5 increased to 32 bytes after being encrypted by the MD5 method, and its size increased again to 88 bytes after being encrypted by the AES256 method. Data can be obtained by value original data AES256 is 9, 96 times larger than its original size, would be but the value of the complexity of her also increased in line with the increase in the number of characters or the byte size of the data password above, thereby increasing the level of difficulty by the party that will hack the login data in the cloud.

1. Introduction

In companies or businesses that are large enough, the use of data storage systems in a centralized system is very commonly used, usually the centralized system will store almost all data related to the company, such as financial data, company asset data, collaboration data with other companies and also includes personal data of every leader and employee in the company. The system is used to facilitate the process of data collection and archiving of company data, by using the facility, every leader and employee can freely empower data that is commonly used by each section in real-time, thus whenever needed, users can easily utilize the system without a measure of time. With this system, each user can make arrangements about their data that are considered privacy, so that only he can use these data safely, but users can also make arrangements on their data in general, or the data may be used by anyone who already have an account into the system.

In a previous study, the encrypted object uses only MD5, but authentication is added using images, if the encryption of password data stored in the database is stolen by the SQL Injection method and the image that is used as the second authentication is manipulated with a copy image, this can lead to a protection system vulnerability [1].

2. Literature review

The encrypted object uses only MD5, but authentication is added using images, if the encryption of password data stored in the database is stolen by the SQL Injection method and the image that is used as the second authentication is manipulated with a copy image, this can lead to a protection system vulnerability [1].

The system that is made is the stem which serves to secure the data with methods of encryption, the encryption that is used is AES (Advanced Encryption Standard) and RSA (Rivest-Shamir- Adleman), with a key of 128 bits [2]. The system is working at the time of the data stored in the cloud storage system, with the pace of work data sourced from IOT will be encrypted by using a key specified before the data are stored in the storage cloud storage, with the encryption of the above, then the data IOT will be more secure upload with cloud facilities on a common path.

Nature paper research system that is built to function for securing (authentication) access entrance to the stem of resource cloud computing , in a study of this , the object that is encrypted by using encryption AES is password users who are used to doing the login to the stem access to cloud computing [3]. Key that is used to encrypt the password is lock with a long 128 bits.

3. Data security method by using AES256 and MD5 encryption

The step in the research process is illustrated in Figure 1.

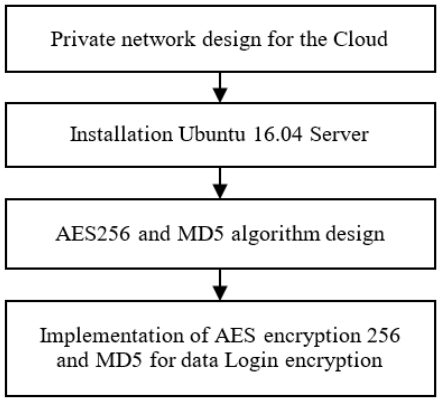

Figure 1. System flow diagram.

In this study, the secret key for encryption AES256 used for encryption combinations was the user password that had been inputted by the user during the login process, with such a concept, the security assurance for the AES encrypted data will be more secure and will be very difficult to do a breach or theft of login data, for more detail on the concept of the system to be designed, Can be viewed on the system flowchart in Figure 2.

There is some data that will be used to test AES and MD5 encryption research, the following data used for testing, is shown in Table 1.

Table 1. Test data.

No	Password	Size
1	123456	6
2	987654321	9
3	Sistem123	9
4	1122334455	10
5	kosongan12345	13

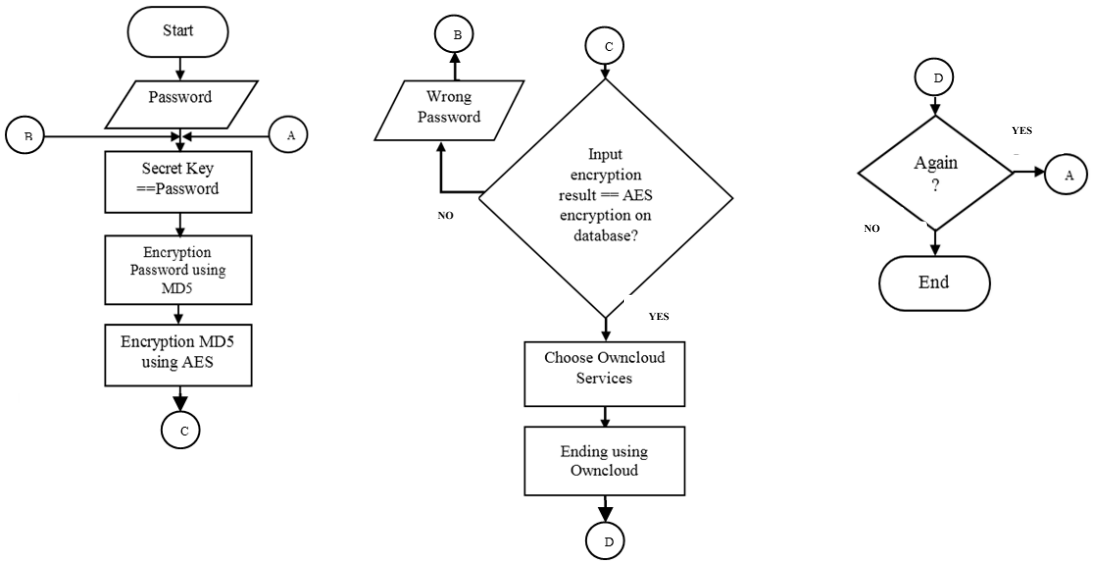

Figure 2. Flowchart how AES and MD5 encryption combinations work.

4. Private cloud

Private cloud is a service-based local network, which serves every need requested by each client, private cloud is usually built by an organization or a company that has shared resources to connecting between computers with each other. It is built with the aim of reducing the cost of domain leasing, storage, and so on. In this study, private cloud was created using Linux based operating system, and the version used is Linux Ubuntu 16.04 LTS (Long Term Support), and the cloud computing application used is own cloud with version 10.1.0 (Stable). Owncloud is a website-based cloud computing application that provides cloud storage services that enable to store files within a server computer, where each connected computer can view, open, and download any files stored in the Owncloud. Each user can manage the privacy of the personal files stored in the owncloud, whether the file can be accessed by all users, or only certain groups that can utilize the source, or could be the file can only be utilized by the file owner.

The process to be done early is to perform the installation process of Linux Ubuntu 16.04 LTS, after finishing the installation process, the first step is to do the network settings/IP address (Internet Protocol). By utilizing the local network that is located in the UPT Information System environment at Polytechnic Harapan Bersama Campus, then the IP used for server computer Owncloud is 192.168.0.100/24. The next step is to install a controller application that is SSH, the SSH serves to control (remote) all the resources on the server computer, the next step is to install a support application such as Apache , PHP 7.0, MySQL and PHPMyAdmin after all is installed, the next step is the installation of the main application, namely owncloud, this application that serves the management of resources owned by all users, here are available several settings, such as user settings, storage capacity that each user can use, and other settings.

5. AES and MD5 encryption

AES (Advanced Encryption Standard) is a cryptography algorithm named Rijndael which was created by Vincent Rijmen and the Belgian John Daemen [4]. The Rijndael algorithm is then known as Advanced Encryption Standard (AES) [3], through a decision issued by the Federal Information Processing Standards Publications (FIPS PUBS) in which the agency is the National output of The Institute of Standards and Technology (NIST) after being approved by the trade Secretary in accordance with section 5131 International Technology Management Reform Act 1996 (Public Law 104 – 106) and Computer Security Act 1987 (Public Law 100 – 235) [6] Explained That the standard cryptography algorithm-based encryption is Advanced Encryption Standard (AES), belonging to the category Computer Security Standard. With the announcement, it is standardized that the algorithm used to

encrypt a cryptography-based data is Advanced Encryption Standard (AES). Cloud Computing has divided its services into three parts, [1]:

- SAAS (Software as a service),
- PAAS (Platform as a service),
- IAAS (Infrastructure as a service).

Service in the above is provided by cloud computing service that has been integrated with Internet network. Based on the results of a survey conducted by the PEW Research Institute, the American population almost reaches 69% using the cloud computing service. Large companies such as Asian Paints, Tata Elxi, Bharti, Infosys, Ashok Ley-Land, Maruti residing in India and approximately 1500 other companies have also made use of the cloud computing service [5]. Increasing fans of cloud technology due to several advantages, including [3]:

- More efficient because it uses minimal budget funds for its resources,
- The operational and management process is easier, because the personal system and the corporate system connected in a cloud can be monitored and managed easily,
- Easy in scalability.

But lately, many parties are preach about the journal or publication warn about the risks and threats and the security of cloud computing. The loss of data due to leakage rights of access or mechanism of authentication that is not good or susceptible to breach is alleged to be the most vulnerable risk and threat to cloud computing [6-8]. Therefore it is designed a method of data security with encryption method that will encrypt data-cloud computing user data that is the personal data of the owner of the cloud access rights.

The MD5 (Message – Digest algorithm 5) was designed by Ronald Rivest in 1991 to replace the previous hash function, which is MD4 that was successfully attacked by Cryptanalists. The MD5 algorithm receives input in the form of a message with arbitrary size and generates a message digest that is 128 bits long. MD5 is one of the applications that is used to know that the messages sent there are no changes while on the network. The MD5 algorithm is in the outline of taking a message that has a variable length changed to ' fingerprint ' or ' essence of the message ' that has a fixed length of 128 bits. This ' fingerprint ' is not reversible to get the message, in other words nobody can see the message of the MD5 ' fingerprint '. MD5 has been utilized in an assortment of security applications, and MD5 is also commonly used to test the integrity of a file. Message Digest 5 (MD5) is one of the most widely used one-way hash functions.

6. Test result and discussion

Next step after the installation and implementation of MD5 and AES encryption algorithms, then the step to be done is to test the encryption that has been made, and proceed with the analysis of the trial results that have been obtained.

6.1. Step testing

The testing step in this research is done by comparing the strength (strength) of the combination of letters, numbers, and symbols in each test data before the data is encrypted or after it is encrypted. Data comparison test results can be seen in Table 2.

Table 2. Comparison of password values before encryption and after encrypted.

No	Variable	O1	O2	O3	O4	O5	AES1	AES2	AES3	AES4	AES5
1	Redundancy	1	1	1	2	1,2	1,8	2	2,2	2	2
2	Complexity	1	1	3	1	2	5	5	5	5	5
3	Before Redundancy Score	-53,5	-34,3	50,7	-0,1	24,5	277	277	277	267	256
4	Original Score	-53,5	-34,3	50,7	-0,1	24,5	277	277	230	255	256
Complexity's Note		1. Very Weak 2. Weak		3. Good 4. Strong			5. Very Strong				

The data is obtained through the site (http://lpc1.clpccd.cc.ca.us), which is a site that provides a means to test the strength and complexity of a password. In the table above shows that the complexity value of a combination of letters, numbers and symbols are higher in value, evidenced by data test no 2 before the encryption with the original data (123456) showed very low complexity value, which is 1 (Very weak), however after the data is encrypted by using MD5 and AES 256 method, the complexity value rises to 5 (Very Strong), for more details about the data comparison before and after encryption, can be seen in the following figure:

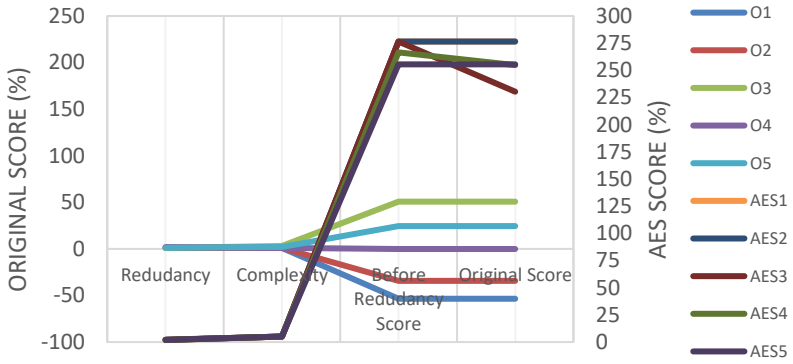

Figure 3. Comparison Chart of data complexity value before and after encryption.

Test are also carried out through several other sites (www.passwordmeter.com) whose function is to know how strong the password we use by measuring some variables used to determine how strong a password is with combinations of letters, numbers and symbols either before being encrypted or after encryption, by following the data results.

Table 3. The result of comparison of passwords through some encryption.

No	Variable	Original					MD5					AES256				
		O1	O2	O3	O4	O5	M1	M2	M3	M4	M5	AE 1	AE 2	AE 3	AE 4	AE 5
1	Number of Characters	6	9	9	10	13	32	32	32	32	32	88	88	88	88	88
2	Uppercase Letters	0	0	1	0	0	0	0	0	0	0	39	46	45	38	45
3	Lowercase Letters	0	0	5	0	8	14	14	8	8	11	36	25	27	34	31
4	Numbers	6	9	3	10	3	18	18	24	24	21	11	15	14	14	10
5	Symbols	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2
6	Middle Numbers or Symbols	4	7	2	8	2	18	16	23	22	21	12	16	15	15	11
7	Requirements	1	2	4	2	3	3	3	3	3	3	5	5	5	5	5
8	Letters Only	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Numbers Only	6	9	0	10	0	0	0	0	0	0	0	0	0	0	0
10	Repeat Characters (Case Insensitive)	0	0	0	10	4	25	26	29	28	31	62	68	71	70	71
11	Consecutive Uppercase Letters	0	0	0	0	0	0	0	0	0	0	14	25	20	12	21
12	Consecutive Lowercase Letters	0	0	4	0	7	6	4	0	3	2	13	10	6	11	9
13	Consecutive Numbers	5	8	2	9	2	11	7	16	18	13	0	2	0	1	0
14	Sequential Letters (3+)	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
15	Sequential Numbers (3+)	4	7	1	0	1	0	0	0	0	0	0	0	0	0	0
16	Sequential Symbols (3+)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Score (%)	4	4	69	0	44	100	100	100	100	100	100	100	100	100	100

From the comparison values for each password, the password will increase to 32 bytes after being encrypted in the first step, using the MD5 encryption method, and then the password size will increase again to 88 bytes after being encrypted with AES256, so AES generates encryption size is 3.62 times larger than the size after MD5 encryption, so AES encryption has resulted data with an encryption size of 9.96 times greater than the data before the encryption process. To find out more clearly the comparison of data before encryption and after encryption, can be seen in the Figure 4.

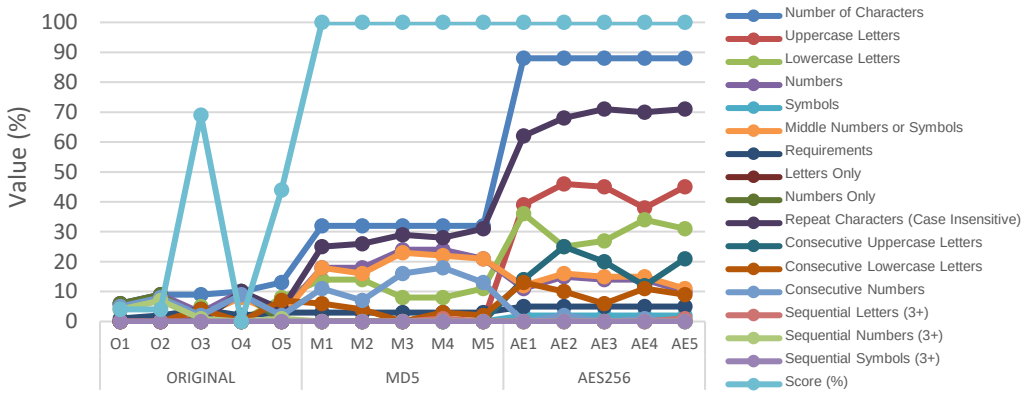

Figure 4. Graphic of Data comparison before and after encryption.

The graph in Figure 4 shown that changes in the final score of a data change drastically as the data has been encrypted by the MD5 (M1) method, but the value of complexity or combinations of letters, numbers and symbols settled in the number 32, but the value would be Increased in point (AE1), where the point of data after MD5 encrypted has been encrypted by using AES256 method, thereby increased the number of character combinations to 88 characters.

7. Conclusions

Based on the data result of the testing are conducted through two websites about the password complexity, it can be concluded that the original data (before the encryption) no 1 to no 5 increased up to 32 bytes after being encrypted by using MD5 method, and The size increased to 88 bytes after being encrypted by using AES256 method, After being encrypted by using AES256 the average result of the data encryption is 2,75 times greater than the data are encrypted by using MD5, and the original data after being encrypted by using AES 256 encryption is 9,96 times greater than the original size, moreover the value of complexity increased as well as the addition of the number of characters or byte size of the data password above, it increased the level of difficulty by the party who will do hacking login data.

References

[1] Ojha S and Vikram R 2017 AES and MD5 Based Secure Authentication in Cloud Computing *International Conference on IoT in Sosial, Mobile, Analytics and Cloud (I-SMAC)* 856-860
[2] Bokefode J D, Avdhut S B, Prajakta A S and Dattatray G M 2016 Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption *Twelfth International Multi-Conference on Information Processing (IMCIP)* 43-50
[3] Imamah, Arif D and Muchammad H 2014 Penerapan AES untuk otentikasi Akses Cloud Computing *Jurnal Simantec.* pp 27-34
[4] Federal Information Processing Standards Publication 2001 *Announcing the Advanced Encryption Standard (AES)* FIPS PUBS **197** (NIST)
[5] Harauz J, Lori M K and Bruce P 2009 Data security in the world of cloud computing *IEEE Security & Privacy* 61-64
[6] Lv Haoyong and Yin Hu 2011 Analysis and research about cloud computing security protect policy *IEEE Computer Society* 214-216
[7] Grobauer B, Tobias W and Elmar S 2010 Understanding cloud computing vulnerabilities *IEEE Security & Privacy* 50-57
[8] Wang Z 2011 Security and Privacy Issues within the Cloud Computing *International Conference on Computational and Information Science* 175-178