TIC-322076 - Analysis of password after encryption by using the combination of AES256 and MD5 algorithm methods.doc

Jan 12, 2022

3625 words / 18687 characters

TIC-322076 - Analysis of password after encryption by using th...

Sources Overview

12%

OVERALL SIMILARITY

1	L Khakim, M Mukhlisin, A Suharjono. "Security system design for cloud computing by using the combination of AES256 and MD5 algorit... CROSSREF	4%
2	Indri Neforawati, Defiana Arnaldy. "Message Digest 5 (MD-5) Decryption Application using Python-Based Dictionary Attack Technique", 2... CROSSREF	2%
3	Leonardus Irfan Bayu Mahendra, Yehezkiel Khakham Santoso, Guruh Fajar Shidik. "Enhanced AES using MAC address for cloud service... CROSSREF	1%
4	Romi Nur Ismanto, Muhammad Salman. "Improving Security Level through Obfuscation Technique for Source Code Protection using ... CROSSREF	<1%
5	andiwasito.blogspot.com INTERNET	<1%
6	pt.scribd.com INTERNET	<1%
7	Asia e University on 2018-06-07 SUBMITTED WORKS	<1%
8	www.cccupclose.com INTERNET	<1%
9	www.nap.edu INTERNET	<1%
10	nozdr.ru INTERNET	<1%
11	Joseph Dedy Irawan, Emmalia Adriantantri, Akh Farid. "RFID and IOT for Attendance Monitoring System", MATEC Web of Conferences,... CROSSREF	<1%
12	sinta3.ristekdikti.go.id INTERNET	<1%
13	University of Sheffield on 2021-04-29 SUBMITTED WORKS	<1%
14	www.zdnet.com INTERNET	<1%
15	repository.out.ac.tz INTERNET	<1%
16	Harrisburg University of Science and Technology on 2020-05-28 SUBMITTED WORKS	<1%

Excluded search repositories:

None

Excluded from document:

Bibliography

Quotes

Excluded sources:

None

Analysis of password after encryption by using the combination of AES256 and MD5 algorithm methods

L Khakim[1*], M Mukhlisin[2], A Suharjono[3]

[1] Computer Engineering, Politeknik Harapan Bersama, Tegal, Indonesia
[2] Civil Engineering, Politeknik Negeri Semarang, Semarang, Indonesia
[3] Electrical Engineering, Politeknik Negeri Semarang, Semarang, Indonesia
*Email : khakimthy@gmail.com

Abstract. The password is very important data in all computer systems. Not a few in some computer applications that secure passwords using only one step. With the development of these technologies, it will also increase the risk of data security in cloud computing, and therefore in this study will be discussed about the security of data that serves as an access into the system using encryption methods advanced encryption standard (AES256) and MD5, where both of these methods will be combined to encrypt the password. From the results of this study, password complexity value after encryption with a combinational method is 5 or very strong.

1. Introduction

Much of the research that discusses cloud technology for various purposes such as the use of cloud technology for smart city projects [1], or the use of cloud to AAMS (Automatic Attendance Monitoring System) which monitors the presence of research students in learning activities [2]. Another study also examines the use of cloud computing to the use of smart agriculture with IOT (Internet of Things) and cloud computing, where utilization is intended to monitor agricultural land for to know moisture content, pH, moisture, etc [3], or research that examines the use of IOT and cloud computing for green house where to utilize these technologies will make it easier to monitor the condition of the home environment such as rain and will automatically get rid of rainwater, where farmers are very difficult to manage rainwater excessive[4].

In terms of security in cloud computing facilities, there are some researchers who have done previous research, where the other research objects are secured or encryption is personal data and general data, where personal data is encrypted by using AES128 and general data encrypted by using MD5, but access into cloud computing system with the fingerprint image, the security level in the study was not secure enough, because the authentication (password) to the cloud computing system only uses encryption techniques MD5, wherein if the data encryption MD5 stored in the database technique of sql injection, and do the decryption, then the password will easily identified[5]. A similar study in a research paper built system serves to secure (authentication) access into cloud computing resource system, in this study, the object is encrypted using AES encryption is the user password used to login to access the cloud computing system[6]. The key used to encrypt the password is the key length of 128 bits. Further research on a system that functions to secure data encryption method, the encryption used is AES and RSA (Rivest-Shamir-Adleman), with a 128 bit key. The system works when the data stored in the cloud storage system, with the work step data from IoT (Internet of Things) will be encrypted by using a key are specified before the data is stored in the storage cloud

storage, with the above encryption, the IoT data will be more safely uploaded with cloud facilities on a public path[7]. From the observation of existing passwords, no one has tried to use a combination of AES256 and MD5 to secure passwords.

In this research, the method that will be discussed is data encryption with multiple systems, that is by encrypting data by two methods of encryption is done gradually. In this study, the method to be used to perform the encryption is a type of encryption or hash Message-Digest 5 (MD5) and Advanced Encryption Standard (AES) using a key length of 256 bits. By using the above encryption method, and is done by double encryptions, it is expected that data security will be more safe and secure.

2. Research Methods

2.1. Advanced Encryption Standard (AES)

AES is a contest winner replacement DES cryptographic algorithm held by NIST (National Institutes of Standards and Technology) the United States government on November 26, 2001[8]. Rijndael algorithm is then known as the Advanced Encryption Standard (Imamah et al, 2014).AES cryptographic types are divided into three types[12]:

- AES 128
- AES 192
- AES 256

AES is a block cipher algorithm using permutation and substitution system (P-Box and S-box) not in the Feistel network as a block cipher in general. Grouping is based on the type of AES key length used. The three digit number that is placed behind the AES is the code to determine the length of the key used by each type of AES, besides differentiating key length to use, these numbers also as distinct from the number of rounds used by each type of AES, for the type of AES-128 round used as many as 10 rounds, while AES-192 as many as 12 rounds, and the latter is the type of AES-256 with a round number used is 14 rounds [9]. Encryption of this type have a constant block size, with the size of 128, and a key length of each 128, 192 and 256 bits. Based on a fixed block size, this type of encryption can work on a 4x4 matrix in which each matrix consists of 1 byte or equal to 8 bits. AES-256 work processes can be seen in Figure 1.

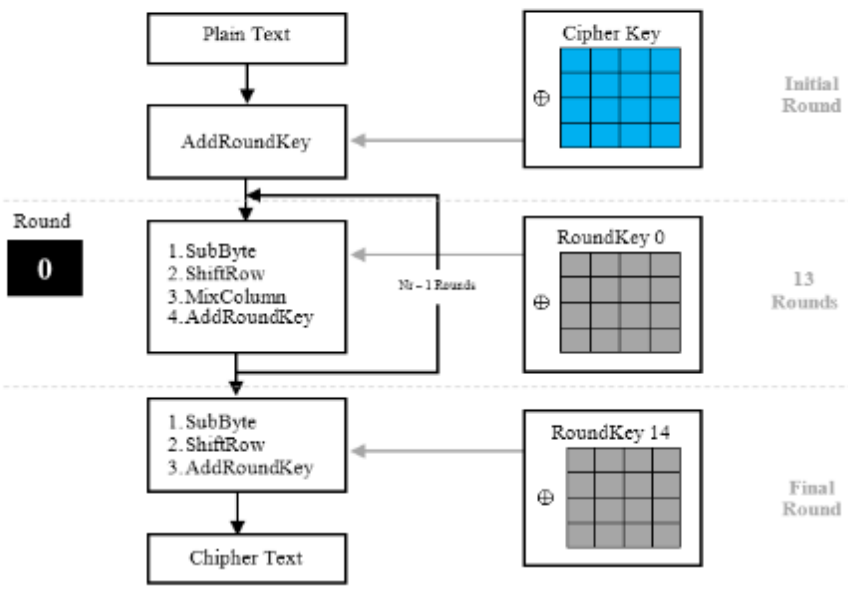

Figure 1. AES Encryption process – 256[10]

Figure 1 is a process of encryption works by using AES with a key 256, whereby the text data to be encrypted with AES, early stages will perform an addroundkey where this stage will perform an XOR between text data with the cipher key, the next will be the process of rotation (round) as Nr-1 times, where the process is done at this stage is the process subbyte, shiftrow, mixcolumn and addroundkey, for the final stage is the process undertaken round subbyte, shiftrow and addroundkey and AES-256 encryption process by the method has been completed.

2.2. *Message - Digest 5 (MD5)*

MD5 is a one way hash function which is an improvement to replace the earlier hash function, namely MD4 were successfully attacked by cryptanalyst, the MD5 algorithm accepts as input a message with any size and produce a message digest of length 128 bits[10]. MD5 is one of the applications that are used to determine that the message sent no change while in the network. MD5 algorithm outline is taking messages have variable length is converted into a fingerprint or message digest having a fixed length is 128 bits. This fingerprint can not be reversed to get the message, in other words no one can see the message of fingerprint MD5.

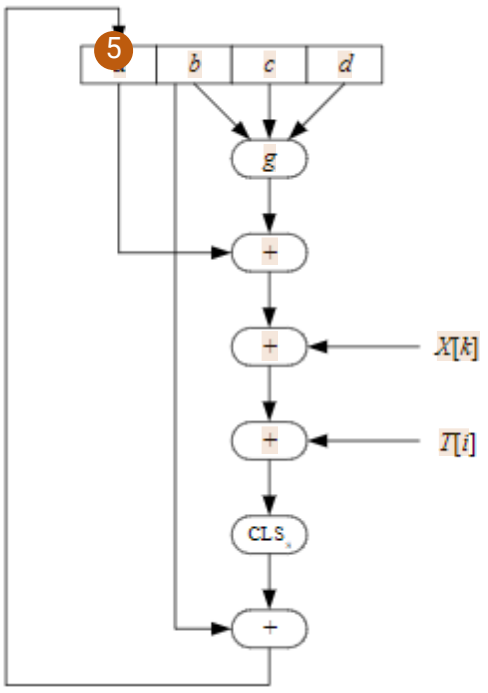

Figure 2. Basic Operation Message Digest [11]

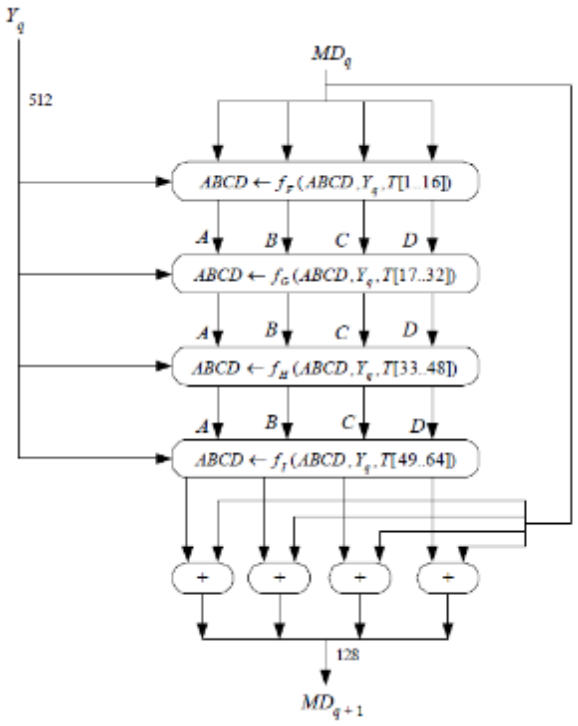

Figure 3. Processing block of 512 bits (Process HMD5)[11]

MD5 basic operations shown in Figure 2 can be written as an equation shown in equation (1).

$$a \leftarrow b + CLSS\ (a + g\ (b, c, d) + X\ [k] + T\ [i]) \qquad (1)$$

Information :

a, B, c, d = Four 32-bit variable buffer (Containing buffer grades A, B, C, D)
g = One of the functions F, G, H, I
CLSS = Circular as s bit left shift
X[K] = Groups to-32-bit*k* of blocks of 512 bits *message* all q. The value of k = 0 to 15
T[I] = Elements *T* all i (32 bit)
\+ = Operation summation modulo 2^{32}

HMD5 process shown in Figure 3, in which messages are divided into L pieces each block length of 512 bits (Y0 to YL - 1). Each block is 512-bits processed together with the buffer MD into outputs 128-bit, and this is called the HMD5, Process HMD5 consists of 4 pieces of rounds, and each round perform basic operations MD5 16 times and each of the basic operations wears an element T [i]. So each round taking 16 element T [i] or (T [i]). In Figure 3, YQ stated 512-bit block q all of the messages that have been added bits booster and additional 64 bit length value of the original message. MDQ is the value of 128-bit message digest of the process HMD5 to-q. At the beginning of the process, MDQ MD buffer containing initialization values.

2.3. *Model Combinational Encryption Method*

In the method used to carry out the process of this study, the researchers conducted the design of systems for data encryption is enabled as entry or login into the cloud system. The method used is to combine the two methods of securing data between the encryption or MD5 hash with AES-256 encryption method. Where both the data security method will encrypt user password data that serves as entry or login into the cloud system. The encrypted password data will be stored into the database. Furthermore, by using these data will be analyzed on an increase in the characters making up the encrypted password, the computing time encryption process with combinatorial methods, analysis and

estimation of the time required to do the password cracking process which has done the encryption process with combinatorial methods. For the programming language used to design this encryption system, using the programming language PHP (PHP preproceccor).

In conducting this research, there is some equipment that will be used to support the success in getting the data, tools and materials as well as the software used is:

- Toshiba Satellite C640
- Proceccor : Intel Pentium 2.0 GHz (Dual CPU)
- Hard drive : 320 Gb
- RAM : 2 Gb (2048 Mb)
- Display (LCD) : 14 Inches
- Operating system : Windows 7 Professional 64 Bit
- Software Server : XAMPP 5.6.8

In this research data used as the test data shown in Table 1.

Table 1. Data Testing

No	Username	Password	Number of Characters
1	pengguna1	coba* 1	6
2	pengguna 2	coba ** 1	7
3	pengguna 3	coba ** # 1	8
4	pengguna 4	coba ** ## 1	9
5	pengguna5	coba *** ## 1	10
6	pengguna6	Coba * 1	6
7	pengguna7	Coba ** 1	7
8	pengguna8	Coba ** # 1	8
9	pengguna9	Coba ** ## 1	9
10	pengguna10	Coba *** ## 1	10

In Table 1 represents the test data whose number is 10 data to be used as data for testing, where test data consists of a combination of lowercase, uppercase, numbers and symbols, as well as the number of characters that range from a character which amounted to 6 to with 10 characters.

The workings of the security system for the process of password encryption methods combinational shown in Figure 4, that is a flowchart working system login with the method of combinational where for technical system works is the password data to be stored in the database, will be encoded in advance by the method MD5, next to the security process that goes along, the result of the encryption beforehand will do the encryption process the second stage by using AES256, where encryption with this method requires a key for encryption methods AES256, here keywords used are the initial input the password typed user prior to encryption. Furthermore, after the final data is encrypted with AES256 method, the data is stored into the database MySQL.

3. Results and Discussion

For the first analysis are analyzed on the computational time required to perform the encryption process using combinational encryption method between MD5 and AES256. Here are the results of testing of the computing time can be seen in Table 2.

In computing the time test results in Table 2, it can be seen for 10 data computation time testing and testing performed 5 times, then obtained the approximate time the fastest computing average on test data number 4 with the computation time is 0.00088 seconds, and time is the longest computation on test data numbers 2, 3, 7 and 9 with the computation time is 0.0012 seconds.

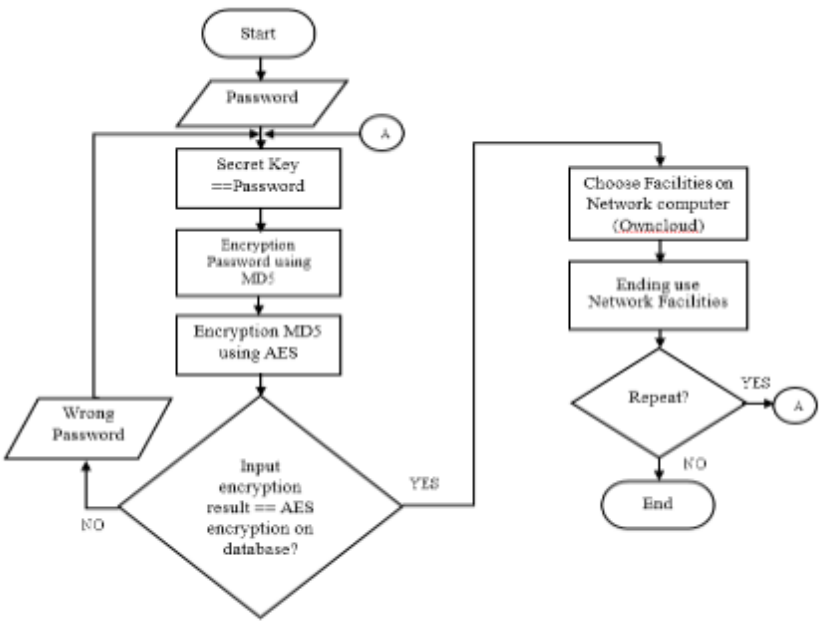

Figure 4. Workflow login system with combinational encryption method among the encryption methods combined with the MD5 and AES256 encryption method

Table 2. The test results of computation time with combinational encryption methods MD5 and AES256

No	Password	Computing Time (s)					
		Testing 1	Testing 2	Testing 3	Testing 4	Testing 5	Average
1	coba* 1	0,001	0,001	0,001	0,001	0,001	0,001
2	coba ** 1	0,001	0,001	0,001	0,002	0,001	0,0012
3	coba ** # 1	0,001	0,002	0,001	0,001	0,001	0,0012
4	coba ** ## 1	0.0009	0.0009	0.0008	0.0009	0.0009	0,00088
5	coba *** ## 1	0.0009	0.0009	0.0009	0.0009	0.0009	0,0009
6	Coba * 1	0,002	0,001	0.0009	0,001	0,001	0,00118
7	Coba ** 1	0,001	0,001	0,001	0,002	0,001	0,0012
8	Coba ** # 1	0.0009	0.0009	0,002	0.0009	0.0009	0,00112
9	Coba ** ## 1	0,001	0,002	0,001	0,001	0,001	0,0012
10	Coba *** ## 1	0.0009	0.0009	0.0009	0.0009	0.0009	0,0009

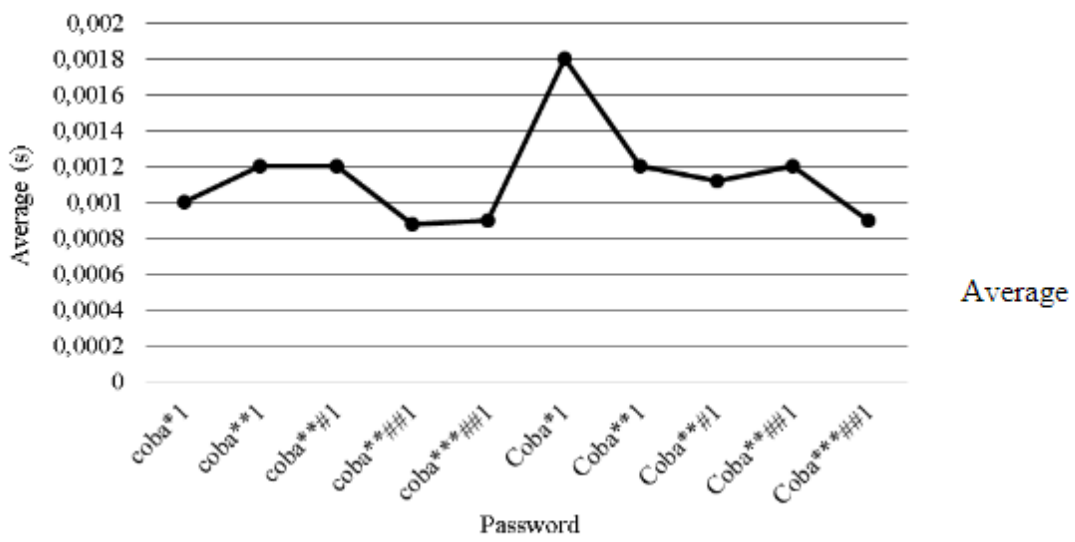

Figure 5. Average computing time for the encryption process by the method of combinational MD5 and AES256

In Figure 5 tests passwords coba*1 shows the computation time of 0.001 seconds, while the testing of the password coba**1 showed a slowdown in the computing time on testing coba*1 became 0.0012 seconds, the last time in the third test in trying to password data coba**#1, while in the test data coba**##1 password try to accelerate the computation time becomes 0.00088 seconds, the last time until the test data password coba*** ##1, and the end of the test on the password data Coba***##1 to

accelerate to 0.0009 seconds. Changes acceleration computing time can be caused by several factors, including too many server serves request from the client, or other causes.

After designing and testing systems combinational encryption method, then obtained the test results in Table 3, shows the increase will occur after the character encoding method MD5 and AES256. All input or password data with the number of characters ranging from 6, 7, 8, 9, and 10 characters, will increase for the same amount ultimately, ie to 32 characters. While data encryption with password after MD5 methods, will increase again after the result data encoded with MD5 method, amounting to 32 characters to 64 characters encrypted with AES256 method or after encryption with combinatorial methods. This proves that with the increasing number of characters of a keyword or password.

To analyze the complexity of a password before and after encoded and encrypted with MD5 and AES256. To get the data in Table 3, the researchers use an application or software available on passwordmeter.com page. On that page is no facility that serves to calculate and analyze a password data. Here are the results of the analysis can be shown in Figure 6.

Table 3. Improved password after encryption with MD5 and AES256

No	Password	Encryption		Number of Characters		
		MD5	The combination of MD5 and AES256	Early	MD5	The Combination of MD5 and AES256
1	coba*1	ed4f8383ae58af05da4da669fde25cad	t11hYjJiYOgLOJ2/1pU2t25nN+tz/2v34T2VoBu6t4h95NTF+Abb1PMvsTH9XV2q	6	32	64
2	coba**1	7b13b2e8c8923c380fea089cb7328b14	8sVQwi20EHxvp7Zpcgb10w3Es5EqFWCCMXWlMdldkhHrRzjQYWMODwNrJ5qfU2D1	7	32	64
3	coba**#1	91a868102f0124ae6c1521cbc87718dd	3ihzQrrDF/bg7BrKTRgx4KiuCoHxLHITr/Zt2s1nuXA6vdt5VQEHKEKDwxLC6uY1	8	32	64
4	coba**##1	d4c0a43b189b881cb35aefb0704887f9	OYDGqRdgylmcukcc8fweKKAaKAKVakC6WszFpUVjbDg8I85YulwR8RlFJDJcUfxQ	9	32	64
5	coba***##1	c3ea1d93b065fbfe665b6b8a51c6f685	RyG+wy+9oTaP09/EUA008Ia0f4Adz8BFI+VruuZZbS+QLXuebJRIzAzSVyAbqrkN	10	32	64
6	Coba*1	2a4597cace46c97851b68031a5d87e46	nIbnPGEfnIFhtCe/YT44EilddIbCgMZcGHdvgU+9U5nL7ZQTDxLRK3b64j3bWQT3	6	32	64
7	Coba**1	a7cc3e9229e0238a03f587aea59ce823	nHflmFZQZdtKA1WbshgT3N82w/wC+Nr5NdEDgmy58K6OQFUYt7cqThEj3s3TLVth	7	32	64
8	Coba**#1	a7cc3e9229e0238a03f587aea59ce823	jEok42EVHeLV92jXsMOJVChPtmQO2wlXaA4SO6tKVbCoUUuyBzPrQ/B4/CiMZiH5	8	32	64
9	Coba**##1	2b5b8be65ec0e48a69e5df2a7b3c75c0	LBQ7BByqJacn5gvRDVylPrvGt7A432U4xj3W7dueCwdB2LChAmACZUQl0p4jykJi	9	32	64
10	Coba***##1	182b44764bf3655de064cd3a5038f637	xS6vZRtN8IvUQJECXKo4hT1/84iWEA0/Bxc0PVStj1SdLEs+X3oteEWpeGTHngGv	10	32	64

Figure 6 shows the increase and decrease in the number of characters before and after the process of encoding methods MD5 and AES256 encryption method. In Figure 6 (a) is the data of the original password (early), where the password data has not been carried out the process of encoding and encryption, from Figure 6 (a) is shown that the password is number 1 to 5 all aspects such as the number of characters, the character of capital, minor characters, number and complexity there are a few number of characters in it, with the exception of the number of capital letters is none in the password data from number 1 to 5, while data on number 6 to 10 of all aspects of the above are the number of characters in it. Furthermore, in Figure 6 (b) is the password data after the encoding process with MD5 method, where the increase of the most prominent was the increase in the number of characters, of all the password data increased to 32 characters, for the characters capital letters no increase to the password data number 1 through 5, but decreased to 0 (zero) in the password data no 6 to 10 and the decline also occurred in the character of the symbol, everything becomes 0 (zero), to other aspects of the majority have increased between 4 to 20 times that of the previous data. Furthermore, in Figure 6 (C) is the password data after AES256 encryption process method which previously had been done by the method MD5 encryption process, where all aspects have increased

dramatically, to the amount of the overall character of the password data has increased to 64 characters.

Table 4. Estimated time required to perform password cracking before and after the data is encrypted with MD5 and AES256 method

No	Password	Estimated Time (t)		
		Before Encryption (minutes)	Once Encoded MD5 (years)	Combinational Methods MD5 and AES256 Encryption (years)
1	coba*1	2,48	$43x10^{27}$	$269x10^{96}$
2	coba**1	180	$7x10^{30}$	$34x10^{99}$
3	coba**#1	11520	$66x10^{24}$	$172x10^{93}$
4	coba**##1	1051200	$2x10^{30}$	$2x10^{98}$
5	coba***##1	2628000	$2x10^{30}$	$11x10^{87}$
6	Coba*1	4,69	$1x10^{26}$	$146x10^{90}$
7	Coba**1	420	$14x10^{27}$	$57x10^{90}$
8	Coba**#1	41760	$56x10^{36}$	$1x10^{84}$
9	Coba**##1	4204800	$224x10^{33}$	$3x10^{96}$
10	Coba***##1	1261400	$329x10^{24}$	$24x10^{93}$

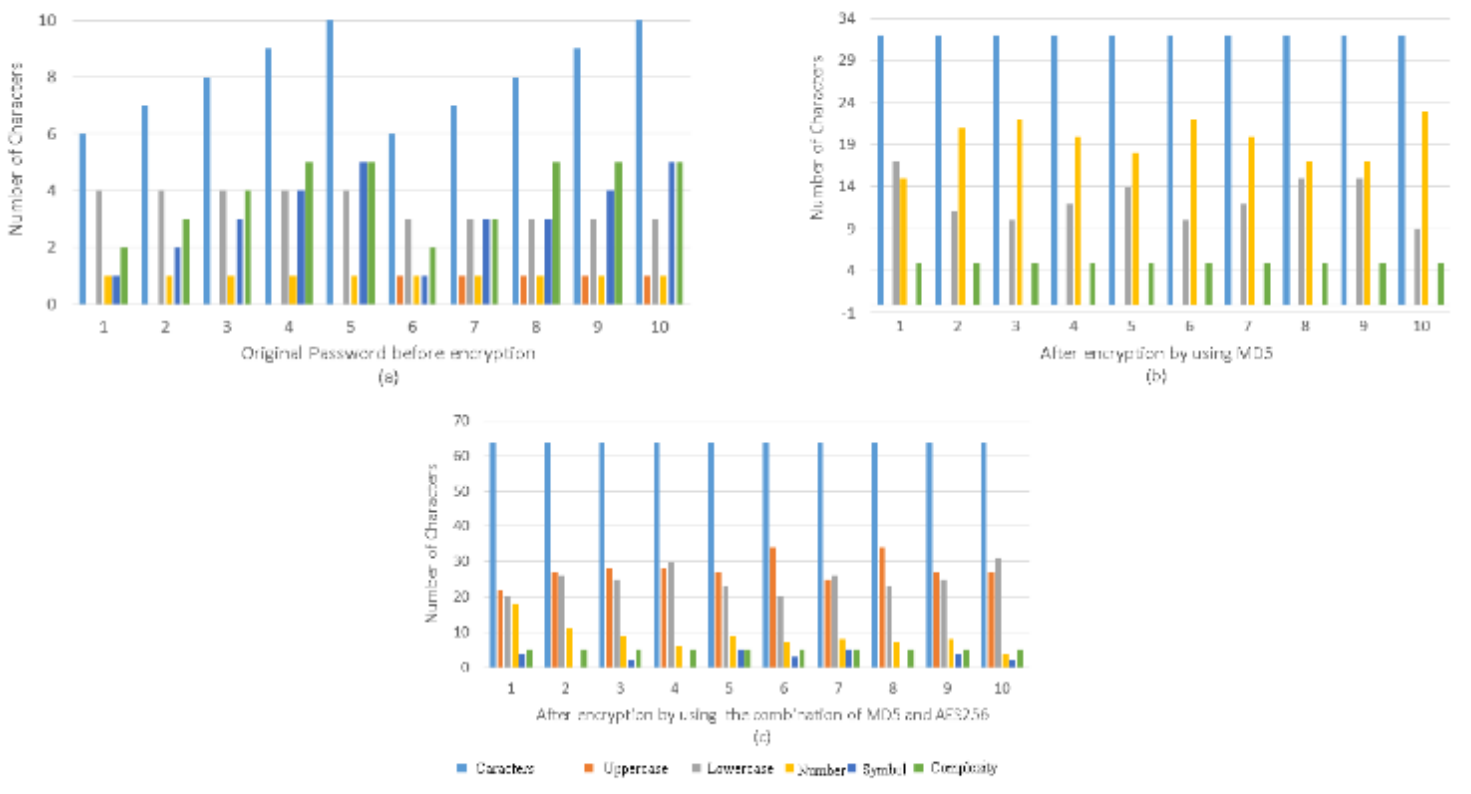

Figure 6. Increases and decreases in the number of characters, uppercase, lowercase, numbers, symbols and complexity of passwords before and after encoding by using MD5 and AES256 encryption method

The next step is analysis to calculate the time required to perform password cracking. The test is performed by using software to calculate the time required for cracking the password data. Software used is available on https://www.my1login.com page.

In Table 4 are the results of testing the password data to analyze the duration of time it takes someone to do for cracking a password that has been encrypted with a combinational method. In Table 4 the numbers 1, seen initial password data is coba*1, it takes time to do a cracking for 2 minutes and 48 seconds, and after the password in encrypted with MD5 method, the estimated time required to perform the cracking increased to $43x10^{27}$ years, this is a very long time for someone to make efforts for cracking passwords. Not only up phase encoded with MD5 methods, the process security was carried out again by being encrypted password data encryption result with MD5 method using a method of securing the second is with AES256 encryption method $34x10^{99}$ years, this is a very long time compared with the time estimate after the password encrypted with MD5 method.

4. Conclusion

From the above test results, it can be concluded as follows:

a. All password data regardless of the number of characters, the number will eventually be 32 characters after encrypted with MD5 method. And the final amount after the encrypted password data with MD5 method, The final number will be 64 characters after being encrypted with AES256.
b. Character numbers on the initial password which is only one character, will be increased to 15 up to 23 characters once in encrypted with MD5 method. And will decrease the amount of as much as 4 up to 18 characters encrypted with AES256 method. With the value of complexity will be very strong after encrypted with MD5 and its value remains the same to be very strong encrypted with AES256 method.
c. For computation of time in performing the encryption process with combinatorial methods, the shortest time required to perform combinational encryption method is 0.00088 seconds, and the longest is 0.0012 seconds.

5. References

[1] L. Wieclaw, V. Pasichnyk, N. Kunanets, O. Duda, O. Matsiuk dan P. Falat, "Cloud Computing Technologies in Smart City Project," *The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications,* pp. 339-342, 2017.

[2] T. Sharma dan S. Aarthy, "An Automatic Attendance Monitoring System using RFID and IoT using Cloud," *International Conference on Green Engineering and Technologies (IC-GET),* p. doi:10.1109/GET.2016.7916851, 2016.

[3] M. S. Mekala dan P. Viswanathan, "A Survey : Smart Agriculture IoT with Cloud Computing," *International Conference on Microelectronic Devices Circuits and Systems (ICMDCS),* p. doi:10.1109/icmdcs.2017.8211551 , 2017.

[4] S. Vatari, A. Bakshi dan T. Thakur, "Green House by using IoT and Cloud Computing," *IEEE International Conference on Recent Trends In Electronics Information Communication Technology,* pp. 246-250, 2016.

[5] S. Ojha dan R. Vikram, "AES and MD5 Based Secure Authentication in Cloud Computing," dalam *International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*, 2017.

[6] Imamah, A. Djunaidy dan M. Husni, "Penerapan AES Untuk Otentikasi Akses Cloud Computing," *Ilmiah SimanteC,* vol. **4**, no. 1, pp. 3-5, 2014.

[7] J. D. Bokefode, A. S. Bhise, P. A. Satarkar dan D. G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption," *Procedia Computer Science,* vol. **89**, pp. 43-50, 2016.

[8] Federal Information Processing Standards Publication 197, "Announcing The Advanced Encryption Standard (AES)," *National Institute of Standards and Technology (NIST),* pp. 1-3, 2001.

[9] N. Su, Y. Zhang dan M. Li, "Research on data encryption standard based on AES algorithm in internet of things environment," *Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019,* no. Itnec, pp. 2071-2075, 2019.

[10] R. Munir, Kriptografi, Bandung: Informatika, 2006.

[11] R. Munir, "Fungsi Hash Satu Arah dan Algoritma MD5," Bahan Kuliah: Departemen Teknologi Informatika, Institut Teknologi Bandung, 2004.

[12] L. Khakim, M. Mukhlisin, and A. Suharjono, "Security system design for cloud computing by using the combination of AES256 and MD5 algorithm," *IOP Conference Series: Materials Science and Engineering*, 2020, vol. **732**, no. 1, doi: 10.1088/1757-899X/732/1/012044.