Implementation Of Vigenere Cryptography Algorithm In Lhokseumawe State Polytechnic Storage System

Dede Kurniawan[1], Indrawati[2], Hari toha Hidayat[3]

[12,3] *Department of Information Technology and computer Polytechnic LHOKSEUMAWE*

JLN. B. Aceh Medan Km. 280 Buketrata 24301 INDONESIA

[1]dedekurniawan.dk67@gmail.com

[2]indrawati@pnl.ac.id

[3]haritoha@pnl.ac.id

Abstract— **Cloud Storage is a technology used to store data online. However, this technology also raises issues in terms of security. Therefore, the author wants to create a cloud storage system using cryptographic security to secure data. With cryptographic techniques that regulate cloud storage, users are without worry about borrowing or borrowing data. The cryptographic method applied is the vigenere cipher algorithm which is a type of classical cryptography. Cloud Storage is implemented on public and private networks to conduct data encryption testing. Based on tests conducted, implementation on private networks is better with an average time of 3.84 seconds for encryption and 253.6 milliseconds for decryption. While on public networks with an average time of 45.3 seconds for encryption and 392 milliseconds for decryption. To measure the effectiveness of cryptography, it is done by avalanche affect method which produces a value of 1.4% to 7% with an average of 3.92%.**

Keywords— Cloud Storage, Vigenere Cipher, Private, public, avalanche affect.

I. INTRODUCTION

In the current era of globalization, technological development is very important role in human life. Technology has made it easier and more convenient to do everyday tasks that might not be able to be done at the same time. Examples such as the development of online-based Digital Storage Media. Limited data storage media is a problem that we often experience when storing important data, so it needs special storage to back up temporary data.

Universities need programs or applications to process data, including online KRS systems, mail servers and Web portals from every unit in the university. The data that is processed and stored on the system is increasing, so it requires a large place of deviation. In addition to the need for storage problems that increasingly require services that can guarantee data security, data recovery includes easy access to data wherever and whenever. [1] .

Currently students are still storing data on each computer's hard disk or portable storage space such as a flash or hard drive. Cloud Storage is able to provide a much better service than using ordinary digital storage. This Cloud Storage has the advantage of adjusting to the needs of the user's own side, and also costs far less than replacing the Hardware in many places.

Data stored in cloud storage is very vulnerable to data theft, because cloud storage is stored online and web-based. So, it needs a good security system to save data uploaded to cloud storage. Security in the cloud storage system must be maintained because there are many malicious users who want to manipulate or steal data. Therefore we need a process to secure data by encrypting uploaded files, by applying a method called cryptography.

Based on the background, researchers will analyze the security of data contained in Cloud Storage. Therefore, the author chooses the final project (TA) with the title "Implementation of the Vigenere cryptographic algorithm in the Lhokseumawe State Polytechnic Cloud Storage System".

Based on the problems that have been explained, the formulation of problems that can be formulated include security on cloud storage systems that are still vulnerable to theft, how to secure files uploaded to the cloud system using the vigenere cipher algorithm, to compare the encryption process carried out on public and private networks in the storage system cloud.

The purpose of this study is to secure files uploaded by users by applying the Vigenere cipher cryptographic algorithm so that the files are safe against theft, making comparisons on the speed of the Cloud storage security system on public and private networks, giving users the ability to share files with others from where and anytime they are connected to the internet network.

II. METHODOLOGY RESEARCH

A. Flowchart

Data encryption and decryption are described with the flowchart diagram using the vigenere cipher algorithm. The encryption and decryption flowcharts are shown in figure 1 - 2.

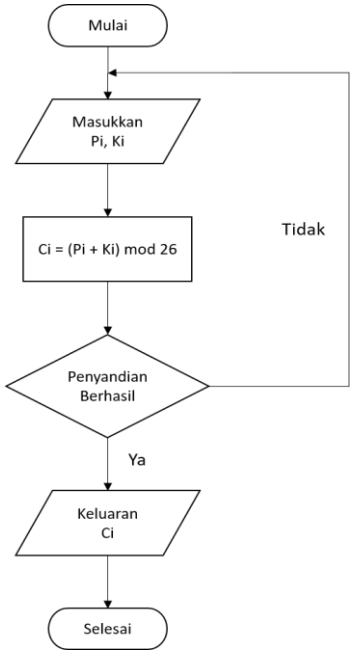

Figure 1. *Vigenere Cipher Encryption*

Here is an explanation of the *flowchart* flow encryption algorithm *vigenere cipher* :

1. First declare the Pi variable as the *plaintext* and also Ki as the *key* to encrypt.
2. Performs calculations using the encryption formula by summing the Pi and Ki values. Then the result is done mod or residual for the one stored on the Ci variable.
3. Checks whether the encryption value was successfully performed. If the condition is true it will continue at a later stage.
4. Whereas if the condition is not correct then the condition will be returned at the time of entering Pi and Ki values.
5. Generates output / *output* with encrypted *plaintext* .

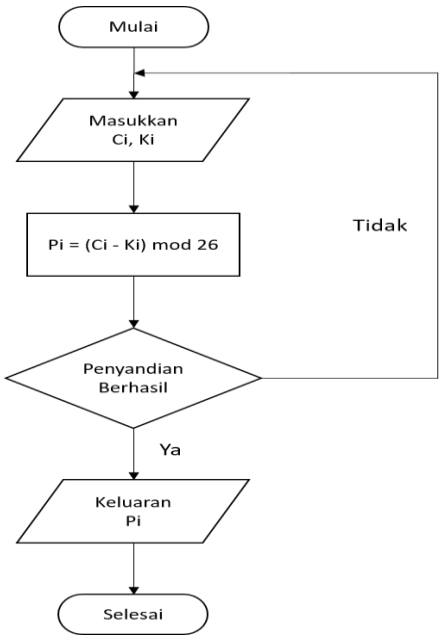

Figure 2. *Vigenere Cipher* Decryption

Here is an explanation of the flow *flowchart* decryption algorithm of *vigenere cipher* :

1. First declare the Ci variable as *ciphertext* and also Ki as the *key* to encrypt.
2. Performs calculations using the decryption formula by decreasing the Ci and Ki values. Then the result is done mod or residual for the one stored in the Pi variable.
3. Checks whether the decryption value is successful. If the condition is true it will continue at a later stage. Whereas if the condition is not true then the condition will be returned when entering the Ci and Ki values.
4. Produces output/ *output* with *chipertext* that has been transformed into a previous *plaintext* .

B. Use Case

In this section use use *Case* to find out the behavior of actors using *cloud storage* Systems.

1. *Use Case* Admin

In *use case* Admin there are 6 *use case* with *include* symbol that leads to *use case* manage data. *Use Case* that leads to *use case* manage data can only be reached through *use case* before, as well as *use case* Manage data and login as shown in Figure 3.

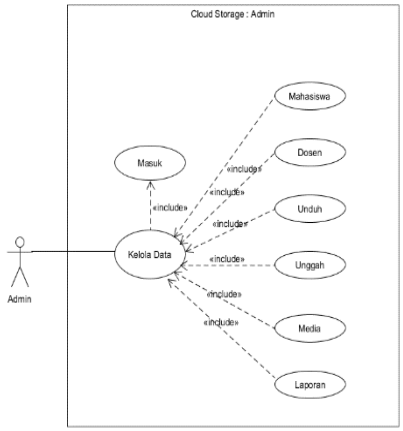

Figure 3. *Use Case* Admins

2. *Use Case* Lecturer

In *use case* lecturer there are 4 *use case* with *include* symbol that leads to *use case* manage data.*Use Case* that leads to*use case* manage data can only be reached through *use case* before, as well as *use case* manage data and sign in. And the *use case* list is an extension or alternate of the *use case* entered as shown in Figure 4.

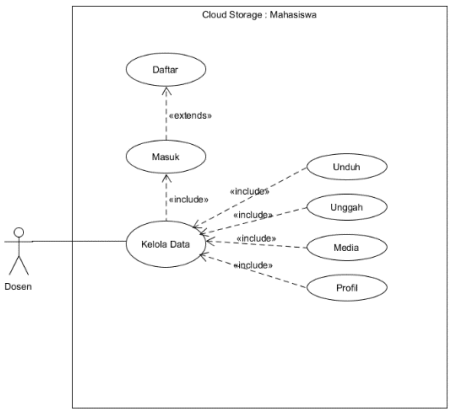

Figure 4. *Use Case* Lecturer

3. *Use Case* Student

In *use case* student there are 5 *use case* with *include* symbol that leads to *use case* manage data. *Use Case* that leads to*use case*manage data can only be reached through*use case*before, as well as *use case* manage data and sign in. And the *use case* list is an extension or alternate of the *use case* entered as shown in Figure 5.

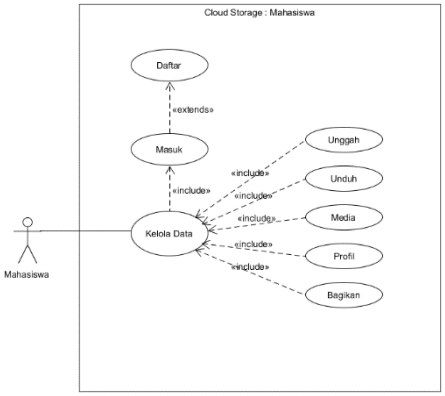

Figure 5. *Use Case* Student

III. RESULTS AND DISCUSSION

The results of the encryption and decryption testing of the value data in the academic information system by using the *vigenere cipher* algorithm, the encrypted value data.

1. User Interface Page

Cloud Storage System created there is a *user interface* as a visual of the *website*. The app has several pages such as login pages, lists, porches, uploads, shares, and other pages. The explanation of the use of each of these pages will be described as follows.

a) Login pageviews

On this page the user performs authentication process in the *cloud storage* application. To authenticate, the user is asked to enter a *username* or Nim and also a *password* to be able to log on to the main *cloud storage* page. The login Page view can be seen in Figure 6.

Figure 6. Sign-in Page view

b) Home Page view

On this page is displayed file – the file is published by the user. Users can download as shown in Figure 7.

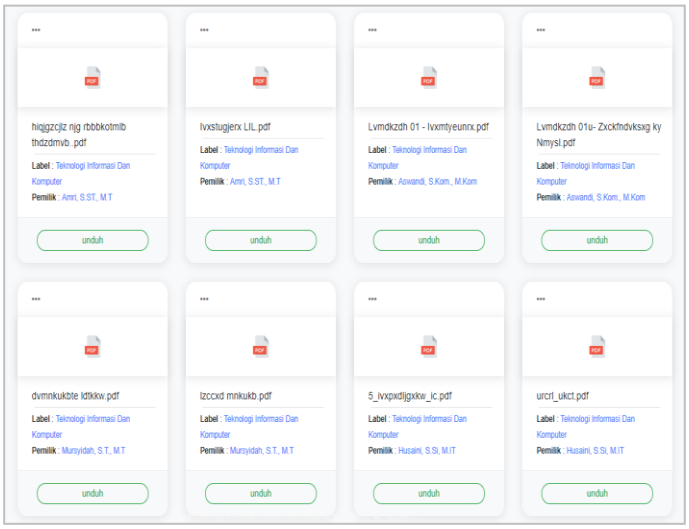

Figure 7. Home Page View

Here is a pop-up form to ignore the *report* or reporting on deviant content uploaded by other users as shown in Figure 8.

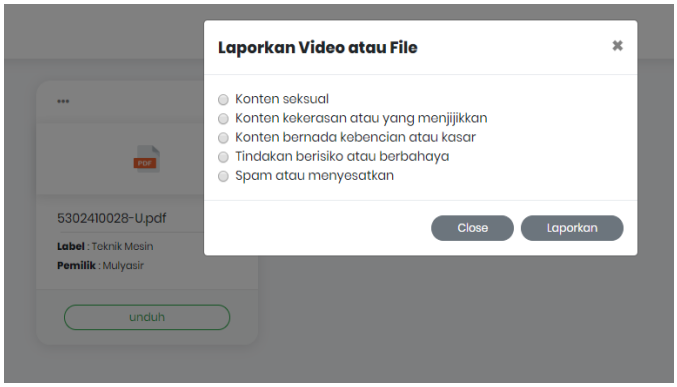

Figure 8. Display Pop-Up reporting

2. *Cloud Storage* security using *vigenere Cipher*

The following is a manual calculation process in the encryption process and decryption on the *vigenere cipher* cryptographic algorithm.

Encryption Formula Vigenere cipher is shown in the equation (1) and (2) and the decryption formula is shown in the equation (3) and (4) :

Pi = (Ci-Ki) mod 26 (1)

Or

Ci = (Pi + Ki) – 26, if the summation of Pi and Ki is more than 26 (2)

Pi = (Ci-Ki) mod 26 (3)

Or

Pi = (Ci – Ki) + 26, if the result of Ci reduction with Ki minus (4)

Description:

Ci = decimal value of the *ciphertext* characters to-i
Pi = decimal value of the *plaintext* character to-I
Ki = decimal value of the key character to-I
Decimal value of character: A = 0 B = 1 C = 2... Z = 25

For example, if the *plaintext* is *CLOUD STORAGE* and the key is cryptography Then the encryption process that occurs is as follows:

Plaintext : *CLOUD STORAGE*
KEY : Cryptography
Ciphertext : mcwjw Gzfrfoo

3. Testing process algorithm *Vigenere Cipher*

Testing done explains how the data security process in *cloud storage* uses the *vigenere cipher* method. Here is the algorithm testing process *Vigenere cipher* on the system created.

a) File Upload page views

On this page, in order to perform a file security or encryption process on the system, the user is required to enter a key with the Public status selection option. In This form consists of input files in the form of documents that want to publish and encryption, type inputs the category of the file content, input status consists of public and private, then the input key to encrypt with the name of the file Uploaded and the last input file caption in the form of *optional*. The page view encryption File can be seen in Figure 9.

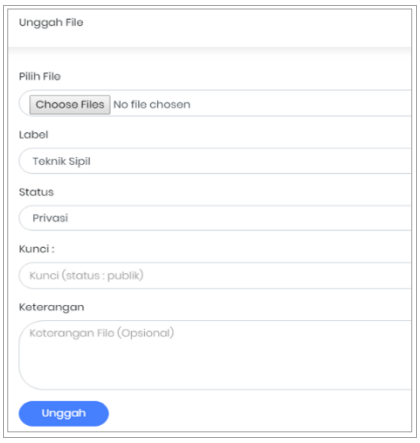

Figure 9. File upload Page view

b) File decryption Display

When a user wants to download a file *published* by another user, a *pop-up* will appear that prompts the user to enter the keyword in order to decrypt the file you want to download. The decryption Page view can be seen in Figure 10.

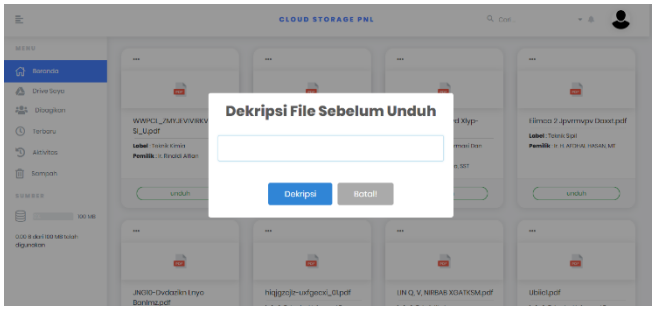

Figure 10. Decryption *Pop-up* view

4. *Cloud Storage* comparison testing using *Private* and *Public* Networks

Testing of the files and the time required for the encryption and decryption process (*upload*) at the time of testing conducted using *private* and *public networks* . Testing was conducted to compare *cloud storage* tested on *private* and *public* Networks and experiment with files *such as* *. *pdf*. *. *doc*, *.*ppt*, *. *avi*, *. *mp4*, *. *mKV*. Test table shown on table1 and A 2 .

TABLE 1
FILE SECURITY EXECUTION TIME TEST (*PRIVATE*)

Filename	Size (KB)	Key	Encryption (s)	Decryption (MS)
Basis_data. pdf	767	Cloud	1.71	266
Organization-komputer_00. pdf	178	Cloud	1.33	235
Foundation theory. docx	134	Cloud	1.27	276
Paper religion. doc	68 KB	Cloud	1.25	266
Bandwidth. ppt	661	Cloud	1.51	238
Cryptography. ppt	60	Cloud	1.20	256
Tutorial AutoCAD. avi	9,890	Cloud	5.47	237
Multimedia. avi Tutorial	11,118	Cloud	6.16	230
C++. MP4 Programming	10,910	Cloud	5.77	240
Grammar. mp4 problem	8,359	Cloud	4.94	254
Arduino DIY. mkv	17,160	Cloud	8.51	259
Install Arduino. mkv	15,189	Cloud	6.97	287

In table 1 is done testing the execution time on the private network. There are several sections like filename, file size, key, encryption time and decryption time. Based on the tests obtained results with an average encryption time of 3.84 second the average decryption time is 253.6 Millisecond (*private*).

TABLE 2
TEST FILE SECURITY EXECUTION TIME (*PUBLIC*)

Filename	Size (KB)	Key	Encryption	Decryption (MS)
Basis_data. pdf	767	Cloud	3.68 S	430
Organization-komputer_00. pdf	178	Cloud	2.10 S	463
Foundation theory. docx	134	Cloud	2.03 s	367
Paper religion. doc	68 KB	Cloud	4.12 S	357
Bandwidth. ppt	661	Cloud	2.31 S	352
Cryptography. ppt	60	Cloud	2.18 S	421
Tutorial AutoCAD. avi	9,890	Cloud	1.2 m	424
Multimedia. avi Tutorial	11,118	Cloud	1.3 m	403
C++. MP4 Programming	10,910	Cloud	1.4 m	348
Grammar. mp4 problem	8,359	Cloud	1.1 m	382
Arduino DIY. mkv	17,160	Cloud	2.2 m	350
Install Arduino. mkv	15,189	Cloud	1.6 m	407

In table 2 is done testing the execution time on the private network. There are several sections like filename, file size, key, encryption time and decryption time. Based on the tests obtained results with an average encryption time of 45.3 second the average decryption time is 392 Millisecond (*private*).

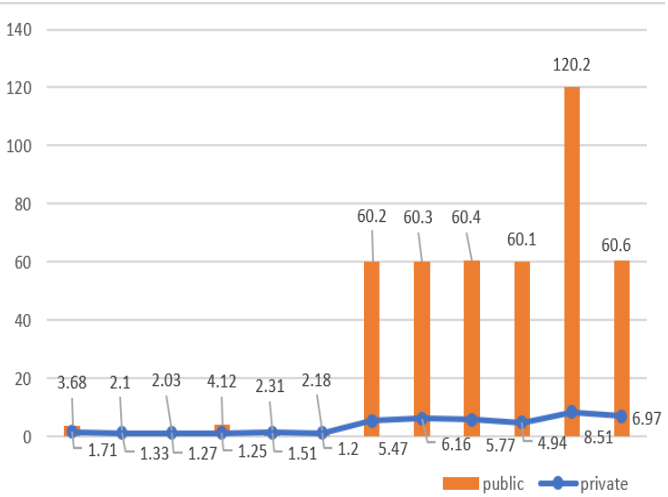

Figure 11. Encryption Time Charts

In Figure 11 is shown a chart with a few shapes that are chart bars and lines, the Blue Line chart indicates encryption execution time on the private network. While the Orange bar chart indicates encryption execution time on the public network in accordance with the test data in tables 1 and 2.

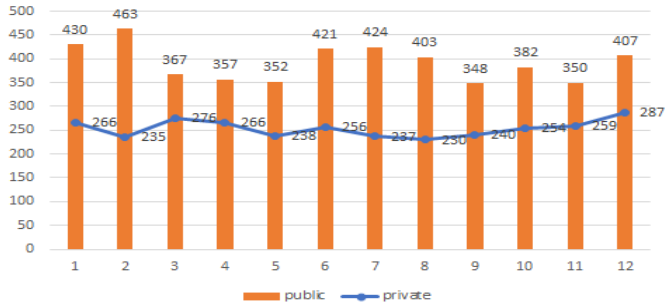

Figure 12. Decryption Time Chart

In Figure 12 is shown a chart with a few shapes that are chart bar and line, Blue line chart showing the decryption Execution time On the private network. While the Orange bar chart shows the decryption Execution time on the *public* Network in accordance with the test data in tables 1 and 2 .

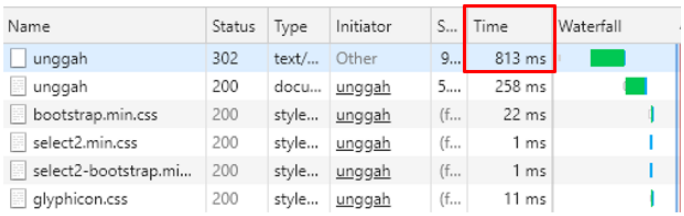

Figure 13. Schema View *Databases*

In Figure 13 is the execution time display of the encryption and decryption process taken through one of the features of the *Google Chrome browser* in the *inspect element network section*. If the value is millisecond, it is converted to seconds first before inclusion in the test table.

TABLE 3
CLOUD STORAGE Encryption Testing

Filename	Size (KB)	Key	Encryption	Decryption (MS)
Basis_data. pdf	767	Cloud	Dlgcv_flhu. pdf	Successful
Organization-komputer_00. pdf	178	Cloud	QCUUQKDOML-mzajxvpf_00. pdf	Successful
Foundation theory. docx	134	Cloud	Nlbxdulb NHQCW. docx	Successful
Paper religion. doc	68	Cloud	Olyuocs Oadol. doc	Successful
Bandwidth. ppt	661	Cloud	DLBXZKOHB. ppt	Successful
Cryptography. ppt	60	Cloud	Mcwjwqrfuik. ppt	Successful
Tutorial AutoCAD. avi	9,890	Learn	-	Failed
Multimedia. avi Tutorial	11,118	123qwerty	-	Failed
C++. MP4 Programming	10,910	Hello 123	-	Failed
Grammar. mp4 problem	8,359	BelaJaR8	-	Failed
Arduino DIY. mkv	17,160	_ Spirit	-	Failed
Install Arduino. mkv	15,189	Storage123	-	Failed

In table 3 is done testing some files that can be encrypted and cannot be encrypted. Files that cannot be encrypted are caused by the encryption key that is inserted does not match the specified validation of the alphabet characters. Then the file does not succeed in encryption when the file size exceeds the maximum *upload* limit of 128 MB.

5. Testing the effectiveness of Cryptography *Vigenere Cipher* on *Cloud Storage* using *avalanche Effect* method

Avalenche Effect is a way of knowing how much bit changes occur to the *ciphertext* due to the encryption process. The larger the *avalanche effect* The better the cryptographic algorithm is.

Avalanche level effect can be calculated by using a formula on equation (5):

$$AE = \frac{\text{Jumlah bit yang tergeser pada cipherteks}}{\text{Jumlah bit cipherteks}} \times 100\% \qquad 5$$

Here are some test samples of *the Vigenere cipher* algorithm on *cloud storage* shown in tables 4 and 5 :

TABLE 4
PLAINTEKS Preliminary comparison

Early Plaintext	Initial Cipherteks	Scratch Cipherteks Binary
Bandwidth	Dlbxzkohb	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000 01100100

TABLE 5
PLAINTEKS Preliminary comparison

PlainText	Cipherteks	Bit Cipherteks	Total Bit Difference	AE (%)
Bandwidte	Dlbxzkohy	0110010001101100 01100010 01111000 01111010 01101011 01101111 01101000	5	7
The band	Dlbxzkohl	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	3	4.2%
Bandwidtf	Dlbxzkohz	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	2	2.8%

Bandwidto	Dlbxzkohi	01100100 01101100 01100010 01111000 01111010 01101011 01101111 01101000	3	4.2%

On table 4 is the initial P roses the plaintext value is converted into cipherteks with the *vigenere cipher* Cryptographic method, then the Ciphertext value are converted to number *binary*. Then on table 5 done calculation Grades binary and A Incorporated into the formula *Avalanche affect* in Equation 5 and obtained the final result in the percent of the calculation of the binary value formula avalanche affect.

IV. CONCLUSION

Based on the discussion on implementing the Vigenere cryptographic algorithms in the Cloud Storage application can be concluded as follows:

1. The Vigenere Cipher cryptographic algorithm can be applied to secure files uploaded in cloud storage.
2. The cryptographic security process on cloud storage requires a plaintext extracted from the file name then in encryption with the key entered by the user.
3. Comparison of encryption time – decryption on the private network is better with an average time of 3.84 seconds and 253.6 milliseconds. While on the public network with an average time of 45.3 and 392 milliseconds.
4. The effective test results in an avalanche effect of 1.4% up to 7% with an average of 3.92%.

REFERENCE

[1] S. A. Indrawata Wardhana, "Designing and implementing Cloud Storage architecture at Iain STS Jambi," Manaj. Sist. Inf., vol. 2, No. 1, pp. 244 – 259, 2017.

[2] R. H. Dedi Kurniawan, Rita Afyenni, "the implementation of the AES algorithm in encrypting files integrated with the Android-based Cloud Storage service," ISSN Media Electron., vol. 3, No. September, pp. 4 – 5, 2018.

[3] S. Mahfud, "Building a Search Engine-based Repository system using the algorithm of Knuth Morris Pratt," vol. 1, No. 1, 2018.

[4] T. W. P. Bernard Raditio Parulian, Surya Michrandi Nasution, "Secure Cloud design and implementation using Diffie-Hellman Key Exchange and Triple Des Algorithm (3Des) Design and Implementation Secure Cloud By Using Diffie-Hellman Key Exchange and Triple Des Algorithm (3Des), "vol. 2, No. 2, pp. 3808 – 3815, 2015.

[5] Andriani, "APPLICATION of VIGENERE CIPHER IN DATA SECURITY ALGORITHM IN INFORMATION SYSTEMS," Teknol. Engineering INF. and Komput., vol. 1, No. 17, pp. 1 – 4, 2018.

[6] T. W. P. Eka Cahya Pratama, Surya Michrandi Nasution, "THE PLANNING AND IMPLEMENTATION of SECURE CLOUD USING DIFFIE-HELLMAN KEY EXCHANGE AND SERPENT CRYPTOGRAPHY ALGORITHM," vol. 2, No. 2, pp. 3808 – 3815, 2015.

[7] A. H. B. Ahmad Leo Yudanto, Herman Tolle, "Design of information System application of biomedical laboratory management," J. Begb. Hairdress. Inf. and science of Komput., vol. 1, No. 8, pp. 628 – 634, 2017.

[8] A. Hanani, "Designing Online Academic Information System University 66 Islam Negeri Malang," p. 140, 2008.

[9] A. H. Muhbib, "Dekstop implementation of the inventory system at Hudi Motor Karangrayung Grobogan," EPrints Udinus, pp. 1 – 41, 2016.

[10] YUSDIARDI, "DESIGNING the SALES INFORMATION SYSTEM (CASE STUDY: PT. I-CUBE CREATIVINDO) thesis," 2014.

[11] D. Kuswanto, S. A. A. Tendean, and Mulaab, "the implementation of a Whitespace steganography algorithm and RC6 encryption for the security of the text," Semin. Nas. Hairdress. and Engineering, pp. 1 – 8, 2