

Combination Scheme of Aes Encryption and Error Correction Turbo Code for Cryptography of Cloud Storage

Dwi Kuswanto¹, Aeri Rachmad²

Informatics Engineering Department
University of Trunojoyo Madura
Bangkalan, Indonesia

¹dwi.kuswanto@trunojoyo.ac.id, ²aery_r@yahoo.com

Abstract-Cloud computing is a technology model in which resources such as computer components (processor, memory, network, storage) are no longer real problems, but abstract. One cloud service is Cloud Storage. With Cloud storage facilities, users can store digital data that is kept secret securely via the internet network. But because every data is sent through a communication line, there are obstacles in the form of noise, where noise can change and reduce the quality of the transmitted data. In general, if there is an error in the data, the system will directly send back the data to be sent back. This certainly will cause delay in the data sent. To reduce the problem, it is necessary to build a cryptographic technique used to keep data and error correction systems confidential to improve the efficiency and accuracy of the information sent. To overcome the above problems can be done through AES Cryptography techniques combined with the Forward Error Correction (FEC) Turbo Code method. The simulation results show that the data is encrypted and uploaded to Dropbox and runs well. Then the results of the analysis show that the percentage of data in the form of text, images and sound will return 100% at SNR 14 dB. In addition, there is a decrease in the Bit Error Rate (BER). In the avalanche effect simulation based on the data types in the text data, the highest avalanche effect is 56.6460% with the same data conditions, but the input buttons are different. For image data, the highest avalanche effect was 55.0781% with different data conditions but the same key was entered. As for the voice data, the highest avalanche effect is 49.6094% with different data conditions but the key is in the same input. In testing the data execution time, the greater the encrypted data the longer it takes for encryption and decryption. Thus the combination of encryption with Turbo Code can overcome the above problems.

Keywords—AES; Turbo Code; Cloud Storage;

I. INTRODUCTION

Cloud Storage is one of the technologies that is currently widely used to store data. Every data that is processed in the transmission in the cloud is also vulnerable to anyone. Another problem lies in the communication system. In communication channels generally cause errors in the form of noise interference and weakening of the signal during attenuation. This disturbance causes errors in receiving data. Data will experience a reduction in bits during transmission so that when the data reaches the recipient, the data is not the

same as the data sent. In addition, this will also cause delays in data transmission. To reduce problems, it is necessary to build a system of error correction with cryptographic techniques. In error correction communication systems are used to improve the efficiency and accuracy of the information sent.

These disturbances cause errors in receiving data. The data will experience a reduction in the bit-bit during transmission so that when the data reaches the recipient, the data is not the same as the data sent. In general, if there is an error in the data, the system will directly send back the data to be sent back. This certainly will cause delay in the data sent to reduce the problem, it is necessary to build an error correction system with cryptographic techniques to encrypt data. In the error correction communication system is used to improve the efficiency and accuracy of the information sent. Many cryptographic techniques can be used, one of which is the Advanced Encryption Standard (AES). AES cryptography is still classified in cryptography that is still safe. Security from AES is supported by the use of very large keys (128 bits, 192 bits, and 256 bits). While the error correction technique used is the Forward Error Correction (FEC) method. FEC is a method to increase data reliability in telecommunication data by correcting bit errors during transmission. Turbo Code is one of the FEC methods discussed in this study.

In this study, researchers combined AES cryptography techniques with Forward Error Correction (Turbo Code) techniques with the aim of keeping data confidential in cloud storage and increasing data reliability and accuracy. Then the cryptographic combination will be simulated for encryption and decryption of text, image and sound data in cloud storage. Then it was tested using several parameters such as BER (Bit error rate) on types of text, image and sound data, Avalanche Effect on text data types, images and sounds, execution time (encryption time and decryption time) type text data, images, and sound.

II. LITERATURE REVIEW

A. Data Communication

Data communication is the process of delivering information from one place to another. There are several elements that must be available, namely data sources

(source), transmission media that carry data sent from the data source to the third element, namely the receiver (receiver). If one element does not exist, communication cannot be done [4]. The following is a general description of data communication, there are five components contained in communication.

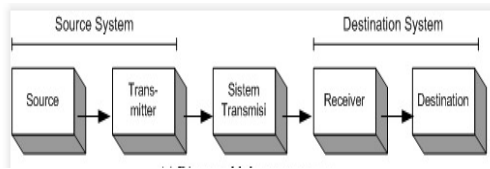


Fig. 1. . DataCommunication Model [4].

B. Advanced Encryption Standard (AES)

AES is a type of cryptographic technique established by the United States standard institution named NIST (National Institute of Standards and Technology). AES was taken from the selection of the competition held by NIST and determined by Rijndael as the AES algorithm.

AES uses components that always have an inverse with a 128-bit block length. The AES key can have a key length of 128, 192,256 bits. AES encoding uses a repetitive process called round. The number of rounds used by AES depends on the length of the key used. The round key is generated based on the given key [5].

C. Turbo Code

Turbo Code is a new paradigm for forward error correction. This Turbo Code managed to achieve error correction performance nearing the limits of Shannon's theory. For the BER value (bit error rate) and the rate of code 1/2, Eb / No is 0.7 dB [6].

1) Turbo Encoder

In the encoder, the input will be divided into two lines. The first path leads directly to the output. While in other lines will be passed through interleaver. Interleaver is in charge of scrambling input into certain models. The output of the interleaver is then passed through two encoders. The encoder is in the form of Recursive Systematic Convolutional (RSC). In the redundancy encoder is applied to this process. The output of the two encoders is in the form of bits, if one encoder produces a low bit then the output from the other encoder produces high bits [7].

2) Turbo Decoder

At the decoder, symmetric databits and databits from the two encoders are input. In the process the decoder will decode various entries into the sequence. Then the data will be processed through feedback feedback. The decoder will repeat the process to translate the input provided. After several repetition processes, it can estimate the data that has been sent [7].

D. Avalanche Effect

One characteristic to determine whether or not a cryptographic algorithm is to look at the Avalanche Effect. Small changes in plain text with a total of 128 bits and keys will cause significant changes to the generated cipher text. Or

in other words, changing one bit in plaintext (with a total of 128 bits) and key (a maximum of 128 bits) will result in changes in many bits in the cipher text [15.]. An Avalanche Effect is said to be good if the bit changes produced range from 45-60% (about half, 50% are very good results). The more bit changes that occur, the harder the cryptographic algorithm will be solved [13]. The value of Avalanche Effect is formulated as follows [14]:

$$Avalanche\ Effect = \frac{\sum \text{changed bits in cipher text}}{\sum \text{Total of bits in cipher text}} \times 100\% \quad (1)$$

E. Bit Error Rate

The Bit Error Rate or commonly abbreviated as BER, is the number of bits received from the data stream through a communication channel that has changed due to high noise. The signal indicates, the information received on the receiver side undergoes many changes during transmission. The working principle of calculating BER here is generally an XOR function between two data, where if the XOR result is 1, then there is one error bit. The BER calculation continues, until all the bits in the information signal are transmitter-XOR with the signal resulting from demodulation on the receiver side. Percentage of BER is calculated based on the ratio between the number of bits that are errors with the total number of bits [6]. The general equation of BER can be written in the following equation [16]

$$BER = \frac{\sum \text{Number of bits error}}{\sum \text{Number of bits}} \quad (2)$$

F. SNR (Signal Noise to Ratio)

SNR (Signal To Noise Ratio) is the ratio of signals received to surrounding disturbances. The following are the quality categories of SNR. The following is the SNR calculation formula in decibels (dB) [15]:

$$SNR = 10 \log_{10} \left(\frac{S}{N} \right) \quad (3)$$

G. Cloud Computing

Cloud Computing consists of two words, Cloud and Computing. Where Cloud means cloud, but what is meant here is the internet network, while Computing means Computing, which when combined means cloud computing. Cloud Computing is a computational / computing model where resources such as processor / computing power, storage, network and software become abstract and are provided as services on the network / internet using remote access patterns.

H. Dropbox

Dropbox is a web-based service operated by Dropbox, Inc. Dropbox uses a cloud computing system that allows users to store and share data and data with other users on the internet using data synchronization. Dropbox was founded in 2007 by Massachusetts Institute of Technology (MIT) graduates Drew Houston and Arash Ferdowsi with initial capital obtained from Y Combinator. Dropbox provides free and paid services with a variety of options. When compared to other similar services, iPad offers

a relatively large capacity for users on a variety of operating systems. Besides being accessible in the browser, Dropbox also provides a client application that can allow users to process data and automatically synchronize on dropbox on the internet [9].

III. RESEARCH APPROACH

This chapter discusses the process of designing a combination of AES and Turbo Code cryptography for encryption and decryption in cloud data storage.

A. Application Contexts Diagram

This section describes the application context diagram of the application diagram.

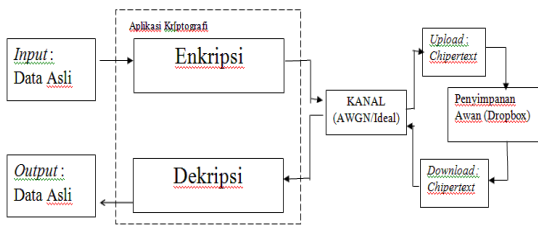


Fig. 2. Application Contexts Diagram

In the context diagram above is a form of application workflow encryption and decryption of data in securing data on cloud storage. Users will enter in the form of large data. After the user selects the data, enter the encryption process performed by the cryptographic application. From the encryption process produces an output in the form of ciphertext and the data will be stored in cloud storage. In the process of downloading data, ciphertext will pass the decryption process first and then the data can be seen by the user. For the implementation of AES-Turbo Code encryption and decryption is done in the cryptographic application section.

B. Flowchart Application

In this section it is explained in the flowchart shown in Fig. 3.

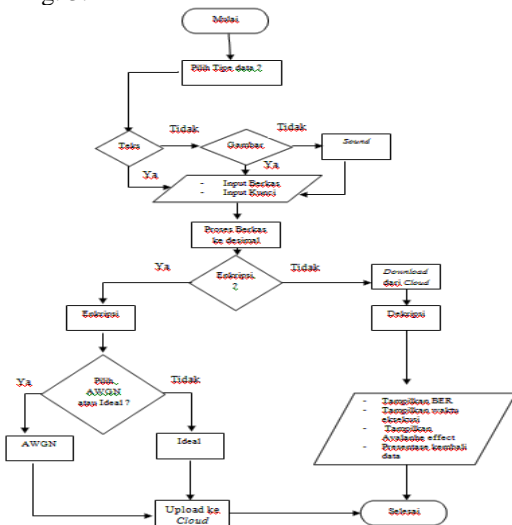


Fig. 3. Flowchart Application Combination Scheme AES and Turbo Code.

C. Flowchart Algorithm Combination Scheme AES and Turbo Code

In this section, it is explained about combining the AES algorithm with Turbo Code which is contained in the flow diagram found in Fig. 4.

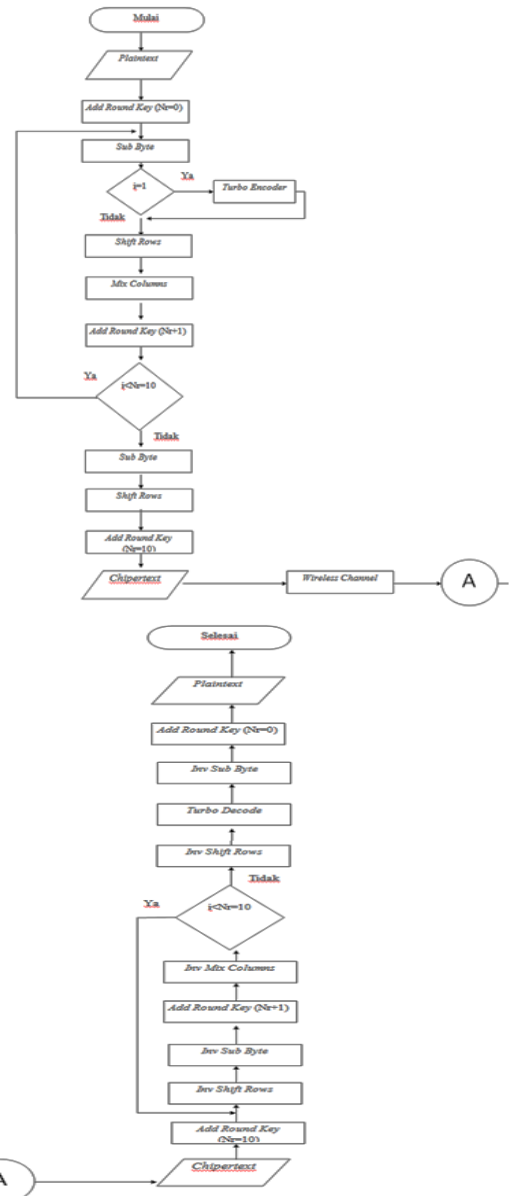


Fig. 4. Flowchart Algorithm combination Scheme AES and Turbo Code[10].

On the Turbo Code the decoder will return and that has been affected by noise. This is where the iteration of the decoder is run. Convert bytes to data: It is a process of returning data in the form of numbers into a complete data.

IV. RESULT AND ANALYSIS

The next stage is testing the combination of AES and Turbo Code. This test is conducted to determine the performance of AES and Turbo Code combinations on AWGN and Ideal channels. As well as security from a

combination of AES and Turbo Code. There are several things that are measured namely BER performance, avalanche effect and execution time.

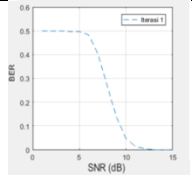
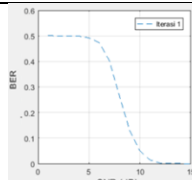
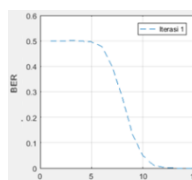
A. Performance BER (Bit Error Rate)

BER testing is a test that is done in order to find out the error bits on the AWGN channel and the ideal channel. The BER test is carried out on a different data with the SNR and decoded iterations as above. The following is the result of the BER performance testing of different data:

1) Performance BER on AWGN Channal

The following is the result of the simulation on the AWGN channel (see in Table I).

TABLE I. PERFORMANCE BER (BIT ERROR RATE) ON AWGN CHANNEL.

Graph	Parameter Performance	Output
	- Text data - Size 5142 byte - Channal AWGN - SNR (0dB - 15dB) - Iteration Decoder = 1	On SNR to 0 to 5th SNR there is no decrease in BER. A significant decrease occurred in the 5th to 12th SNR. Then at SNR to 13 to 15, the BER graph that occurs is a constant decrease at point 0. This indicates that the datais free from bit errors.
	- Image data - Size 8550 byte - Channal AWGN - SNR (0dB - 15dB) - Iteration Decoder = 1	On SNR to 0 to 5th SNR there is no decrease in BER. A significant decrease occurred in the 5th to 13th SNR. Then at SNR to 13 to 15, the BER graph that occurs is a constant decrease at point 0. This shows that the datais free from bit errors.
	- Sound data - Size 6048 byte - \channal AWGN - SNR (0dB - 15dB) - Iteration Decoder = 1	On SNR to 0 to 5th SNR there is no decrease in BER. A significant decrease occurred in the 5th to 13th SNR. Then at SNR to 13 to 15, the BER graph that occurs is a constant decrease at point 0. This indicates that the datais free from bit errors.

B. Performance BER on Ideal Channal

In the ideal channel BER performance against various types of data can be seen in the picture below:

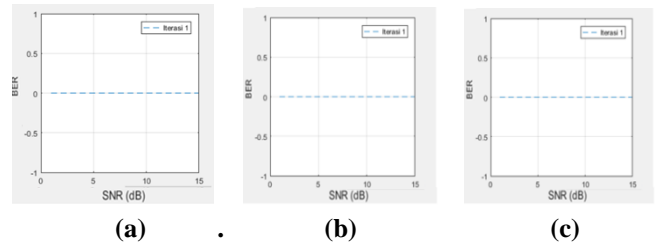


Fig. 5. Graph BER on Ideal Channal Graph BER data type Text (a), Graph BER data type Image (b) and Graph BER data type Sound (c).

In the picture above (Fig. 5) shows a flat line because the ideal channel is a channel with ideal conditions so that dataent and received is not damaged in the databit.

1) Performance Avalanche Effect

Following are the results of the Avalanche Effect test can be seen in table II.

TABLE II. THE RESULT TEST OF AVALANCE EFFECT AES-TURBO CODE.

Scenario	Condition data	Data Type	Key	Avalanche Effect
1	Same Key and different data, size with 128 bit	Text	12333	47.6563%
2	Different Key and Same data, size with 128 bit	Text	12334	56.6460%
			12333	
3	Same Key and Different data, size with 128 bit	Image	12333	55.0781%
4	Different Key and Same data, size with 128 bit	Image	12334	50.3906%
			12333	
5	Same Key and Different data, size with 128 bit	Sound	12333	49.6094%
6	Different Key and Same data, size with 128 bit	Sound	12334	44.5313%
			12333	

In table II it can be seen that, of the six scenarios that were tested, they had different avalance effects for each data. In the text data, the highest avalance effect is 56.6460% with the same data condition, but the key entered is different. For image data, the highest avalanche effect is 55.0781% with different data conditions but the key entered is the same. Whereas for sound data, the highest avalance effect is 49.6094% with different data conditions but the key entered is the same.

2) Performance Encryption and Decryption Time

This simulation was carried out by comparing the time of execution to various types of data and channel types. This simulation is done with input data namely data type (text, image, and sound), SNR 15 dB, and 1 iteration. The following is a table of the results of the simulation that have been conducted:

TABLE III. TIME ENCRYPTION AND DECRYPTION AES-TURBO CODE ON IDEAL CHANNEL.

Data Type	Size Data(byte)	Time (sec)	
		Encryption	Decryption
Text	5142	33.8018	33.3823
	17314	101.48	120.334
Image	1587	13.8812	9.48505
	8550	52.0146	55.2579
Sound	6048	39.1264	38.8202
	23680	152.985	172.009

TABLE IV. TIME ENCRYPTION AND DECRYPTION AES-TURBO CODE ON AWGN CHANNEL.

Data Type	Size Data(byte)	Time (sec)	
		Encryption	Decryption
Text	5142	27.317	33.7881
	17314	85.7838	121.532
Image	1587	6.69505	9.08504
	8550	39.3284	125.292
Sound	6048	28.2518	39.7171
	23680	119.56	171.275

V. CONCLUSION

From the results of the research that has been done, some conclusions can be drawn as follows:

- Data text type, image and sound that are encrypted with a combination of AES and Turbo Code then simulated by adding the AWGN on the data type can be decrypted again at SNR > 10dB with an average percentage of the text data type of 99.45%, image of 99.37% and sound is 99.38%. For SNR <10, the average percentage of each data is for the text data type of 23.49%, the image of 23.76% and the sound of 24.70%.
- The results of the simulation avalanche effect based on the data type that is in the text data obtained the highest avalanche effect of 56.6460% with the same data condition but the key entered is different. For image data, the highest avalanche effect is 55.0781% with different data conditions but the key entered is the same. Whereas for sound data, the highest avalanche effect is 49.6094% with different data conditions but the key entered is the same.
- The time of execution of encryption and decryption on a combination of AES and Turbo Code, the time required for encryption and decryption on the AWGN channel is longer than in the ideal channel. The average time needed is around 6 seconds on the ideal channel while for AWGN channels is around 32 seconds.
- Overall the combination method of AES Cryptography and Error Correction Turbo code is a new cryptographic method that has better performance than AES Cryptography for cloud storage at SNR > 10 dB..
- This research can then be compared with other algorithm (MAP, Log-MAP, Max-Log-MAP & SOVA) turbo code. to find a balance between the performance of decoding and the complexity of implement.[17].

ACKNOWLEDGMENT

We would like to thank our colleagues in Faculty of Engineering University of Trunojoyo Madura Indonesia

REFERENCES

- [1] H.J.D. Harahap and M. Khairani, "Implementasi kriptografi AES Rijndael untuk enkripsi and dekripsi pada penyimpanan datacloud (Implementation of Cryptography AES Rijndael for encryption and decryption to datacloud saving)," Jurnal Mahasiswa Sekolah Tinggi Harapan, pp 207, 2016
- [2] D. Kuswanto, Unjuk Kerja *Turbo Code* pada Kanal Flat Fading. (Work of Turbo Code for Fading Flat Canal). Surabaya: Institut Teknologi Sepuluh Nopember, 2004
- [3] MAO, Q., QIN, C., & GUO, B., "Turbo CodeBased Encryption with Error Correction Capability," J. Computational Inf. Sys., vol 7, pp 2876-2885, 2011
- [4] W. Stallings, Data and Data Communications, Eight Edition. .New Jersey: Pearson Education, 2007
- [5] R. Sadikin, Kriptografi untuk Keamanan Jaringan (Cryptography for Network Security), Yogyakarta: Andi Publisher, 2012
- [6] E.K. Adiyanto, Perbandingan Performansi *Convolutional Code* dengan *Convolutional Turbo Code* (Comparison of Convolutional Code with Convolutional Turbo Code) Jakarta: Universitas Mercu Buana, 2009
- [7] E. Kasper, Turbo Codes, 2010.
URL://www.propagation.gatech.edu/ECE6390/project/Fall2010/Projects/group6/ExoBuzz/page1/page10/page10.html, accessed on August 24th 2016.
- [8] I.G.P. Senky, *Spatial Multiplexing Analisis*. 2008. URL://http://lib.ui.ac.id/data?data=digital/126630-R0308117 - Spatial%20multiplexing-Analisis.pdf, accessed on August 24th 2016
- [9] Menken, I, Dropbox Complete Certification Kit - Core Series for IT, Brisbane:Emereo Publishing, 2011
- [10] C.A.M. Hakan, O. Volkan and N. Osman, "UCAN. A combined encryption and error correction scheme: AES-Turbo Code," J. electrical and electronics engineering, vol 1, pp 861-866, 2009
- [11] G. Wibisono and L. Sari, Teknik Pengkodean Sistem Digital. Bandung: Rekayasa Sains, 2011
- [12] H. Yuliandoko and M. D. Ayatullah, "Pengaruh Material (Lilitan) Terhadap Kekuatan Sinyal yang Dipancarkan Antena Helix 2,4 GHz," Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014)
- [13] F Putra, Budiman, & G, Andini, N. 2015. Perbandingan and Analisis Performansi Enkripsi-Dekripsi Teks Menggunakan Algoritma aes and AES yang Termodifikasi Berbasis Android (Comparison and Analysis of Encryption-Decryption Text Performance using Algorithm aes and modified AES with Android based) . *E-Proceeding of Engineering Volume 2*.
- [14] Sugiyanto and R.K. Hapsari, "Pengembangan Algoritma *AdvancedEncryption Standard* pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," Jurnal ULTIMATICS Universitas Multimedia Nusantara, vol 8, pp 131-138, 2016
- [15] A.F. Isnawati, I. Susanto, and R.A. Purwanita., Analisis Jarak Terhadap Redaman SNR(*Signal Noise to Ratio*), dan Kecepatan *Download* pada Jaringan ADSL.JURNAL INFOTEL - Informatika Telekomunikasi Elektronika. 2. 1. 10.20895/infotel.v2i2.78.
- [16] W. Pamungkas, A.F. Isnawati and A. Kurniawan, "Modulasi Digital Menggunakan Matlab," JURNALINFOTEL-Informatika Telekomunikasi Elektronika, 2012
- [17] P. Zhu, J. Zhu, X. Liu, "A Study On Turbo Code Based On AWGN Channel," Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSE), Paris France: Atlantis Press, 2013