International Journal of Application on Sciences, Technology and Engineering
(IJASTE)
Volume 1, Issue 2,2023.ISSN:2987-2499

Encryption of Audio File Using AES and Blowfish Algorithms

Novario Jaya Perdana[1, a)], Bagus Mulyawan[1, b)], Vico Lukianto[2, c)]

Author Affiliations
[1]Information Systems, Universitas Tarumanagara
Jakarta, Indonesia
[2]Informatics, Universitas Tarumanagara
Jakarta, Indonesia

Author Emails
a) Corresponding author: novariojp@fti.untar.ac.id
b) bagus@untar.ac.id
c) vico.535170090@stu.untar.ac.id

Submitted: January-February 2023, Revised: March 22 2023, Accepted: May 23, 2023

Abstract

Cloud storage has a role to boldly store data so that it can be accessed by various users. The amount of data stored, causes this data to be vulnerable to attack. It takes a method that can guarantee the security of the data. AES has become a trusted encryption method because of its computational power. Blowfish as a newer method is also trusted because it is efficient and effective in storing data. A web-based application was successfully created based on this method. This app is used to test the combination of these 2 methods. The data used in this study is audio data. Audio data has a higher level of complexity than text data in general, so it requires additional processing when encrypted. Based on the test results, it was found that, the results of the data survived against security attacks with the plain text analysis method with a decryption rate of 0.049%. In addition, the method also succeeded in encrypting data at an average speed of 14 seconds, and decrypting data at an average speed of 13 seconds.

INTRODUCTION

It has been more than a year, the world has been hit by the Covid-19 pandemic. It started with the discovery of a mysterious disease case in early 2020 in Wuhan, China and spread throughout the world two months later. Until finally the World Health Organization (WHO) declared Covid-19 a pandemic. At that time, almost the whole world had confirmed that there were patients with this virus and decided to implement a policy of limiting community activities or what is often referred to as a lockdown (Katella, 2021; WHO, 2020). To date, there have been more than 200 million confirmed cases of COVID-19 worldwide. Of this number, more than 4 million sufferers are declared dead (WHO, 2021).

Indonesia itself confirmed the first Covid-19 case on March 2, 2020, and finally implemented the PSBB policy a month later (Simanjuntak, 2020). Based on data reported by the Government of the Republic of Indonesia through online media, currently positive confirmed cases of Covid-19 have reached more than 4 million cases. After the confirmation of this many cases surfaced, the government immediately made provisions to limit community activities. All activities carried out at home even for work and worship must be done at home.

All areas of community activity are finally not visible anymore in real terms. All activities move to the online space. No more face-to-face meetings between employees and superiors, students and lecturers, students and teachers, or sellers and buyers. At this time, the role of information technology is needed and becomes the backbone of community activities. Some online media service providers have become very busy. This can be seen in the increase in internet use during the pandemic. Based on data from the Ministry of Communication and Information of the Republic of Indonesia, there has been an increase in internet usage by up to 40% (Kominfo, 2020).

According to a survey conducted by Telkomsel of its customers, the five most popular services during the pandemic were browsing, e-commerce, games, communication and video. Browsing activity increased by 141%, while e-commerce services increased by 120%. Game services also increased by 83%. For communication activities, the use of instant messaging sharing services rose by 65%. Meanwhile, in terms of applications, the most popular during the pandemic is the video conferencing application to support WFH and SFH. Zoom is the most widely used application by Telkomsel customers. Four other video conferencing applications that are no less popular are CloudX Telkomsel, Skype, Microsoft Teams and Google Meet. The most popular applications supporting SFH include Google Classroom which is used by 59% of users, RuangGuru (11%), Sainspedia (20%) and the Ministry of Education and Culture learning portal (6%) (Maulida, 2020).

A transition to remote work on a large scale like this would not have been possible in infrastructure 15 to 20 years ago. Simply put, without the current prevalence of cloud computing, remote system access, and video conferencing capabilities, most workers would not be able to work from home. This increase in online media users has a major impact in encouraging the improvement of the infrastructure of online service providers.

Cloud computing has emerged as one of the most important media nowadays. Its use is important because it covers all joints of online activity. The ease and high level of effectiveness are the reasons why this media was chosen to support activities. The benefits include activating more reliable online trading activities, supporting health services, facilitating remote work, and entertaining people who are forced to stay at home.

When the use of cloud storage is increasing, the biggest challenge faced is how to secure the data stored in it. Data on cloud storage is open so that it can be accessed by multiple devices at once and may be accessed by more than 1 user. Thus, data security is very important. Various methods of securing data in cloud storage are also offered.

Some researchers use blockchain technology for the security process. One of them is He Jiayu et al (2021) who use blockchain technology as a mechanism to encrypt documents in a cloud architecture. He Jiayu proposed an identity-Based Proxy Re-Encryption (IBPRE), Data Owner-Manipulative IBPRE (DOM-IBPRE) scheme, which is achieved by combining IBPRE, blockchain and Inter Planetary File technologies. Systems (IPFS). Another research related to the Blockchain approach is from Ngabo et al (2021). In his article, Ngabo proposes a publicly permitted blockchain security mechanism using elliptic curve crypto (ECC) digital signatures on the database server thereby providing an irreversible security solution.

LITERATURE REVIEW

AES and Blowfish have been acknowledged by researchers as a great encryption algorithm. These two is still in use for today's safety mechanism.

Advanced Encryption Standards

The AES (Advanced Encryption Standard) algorithm is the abbreviation of the standard algorithm for advanced data encryption, which is an algorithm for symmetric key encryption. The AES algorithm is a block algorithm for encryption that is used to supplement the DES algorithm. The AES algorithm uses 128-bit, 192-bit, and 256-bit keys of varying lengths, but its block length may only be 128-bit, and normally 128-bit keys are used. The same key is used in the AES algorithm encryption and decryption process, and the process of grouping and encryption is as seen in Fig.1.

The AES algorithm has impressive results. The AES algorithm is relatively simple in terms of encryption speed. It inherits the value of the speed of DES encryption and has accelerated speed. It has good encryption efficiency and is ideal for vast volumes of data being encrypted and decrypted. Compared to the DES algorithm and the 3DES algorithm, the AES algorithm is enhanced in terms of security, and its security is comparatively high, but still much lower than the RSA algorithm; In terms of key length, the AES algorithm improves the issue of inadequate DES length, which is increased from 56 bits of the DES algorithm to 128/192/256 bits; In terms of resource consumption, the AEES algorithm improves.

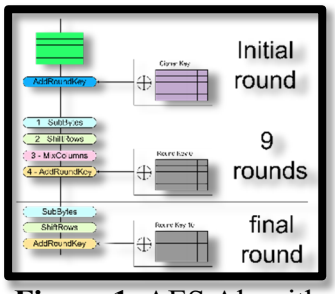

Figure 1. AES Algorithm

However, AES algorithm still has some shortcomings in key management, which makes the security management and distribution of keys a little difficult, which makes it possible for AES algorithm to be cracked under certain conditions. It includes the following two aspects: (1) Since AES uses the same key in the encryption and decryption of data, it is necessary for both parties to agree on the key in advance, and to ensure that the key information cannot be obtained by the third party, otherwise the information may be cracked; (2) Each time the two parties use the AES algorithm, they use a unique key that other people do not know. This will increase the number of keys and cause a management burden.

Blowfish

The Blowfish algorithm has another name OpenPGP.Cipher.4 which is a Symmetric Cryptosystem class encryption, the encryption method is similar to the DES (DES-like cipher) created by Bruce Schneier. Blowfish is included in the 64-bit Block Cipher encryption with key lengths that vary from 32-bit to 448-bit. It consists of three parts, as follows.

Key Expansion

Used to convert a key (minimum 32-bit, maximum 448-bit) into several subkey arrays (subkeys) totaling 4168 bytes. The steps are as follows:

1. 18 subkeys {P[0]…P[17]} are required for both the encryption and decryption steps. Subkeys are used for both processes with the same Subkeys.
2. 18 subkeys stored in a P-array with each element 32-bit
3. Subkeys in hexadecimal form for each subkey.
4. The result of changing Subkeys is stored in a P-array with 18 keys that will be used for the entire encryption process.
5. The next stage is the initiation of substitution boxes, at this stage 4 substitution boxes will be needed in both encryption and decryption processes, each of which has 256 entries, each entry is 32-bit.

Consists of a simple function iteration (fastel network) as many as 16 rounds. Each round consists of a dependent key permutation and a dependent data key substitution. This encryption process consists of 2 parts, the part consists of:

1. Rounds. This process is repeated until it is 16 rounds, each round (Ri) using plaintext input (P.T.) taken from the previous round and corresponding to the subkey (Pi).
2. Post-processing. The next step is shown in Fig.2.

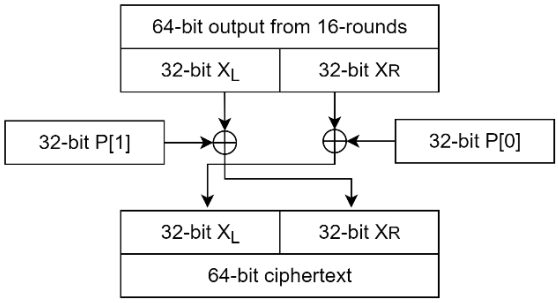

Figure 2. Post-processing round of Blowfish

METHODS

A software is made to test the system used. The system input is in the form of an audio file with the wav extension which was taken by the researcher himself. In addition, sample files from websites with the addresses file- examples.com and freewavesamples.com will also be used. The system that will be designed is a security application for audio files using the Advanced Encryption Standards and Blowfish method based on the website.

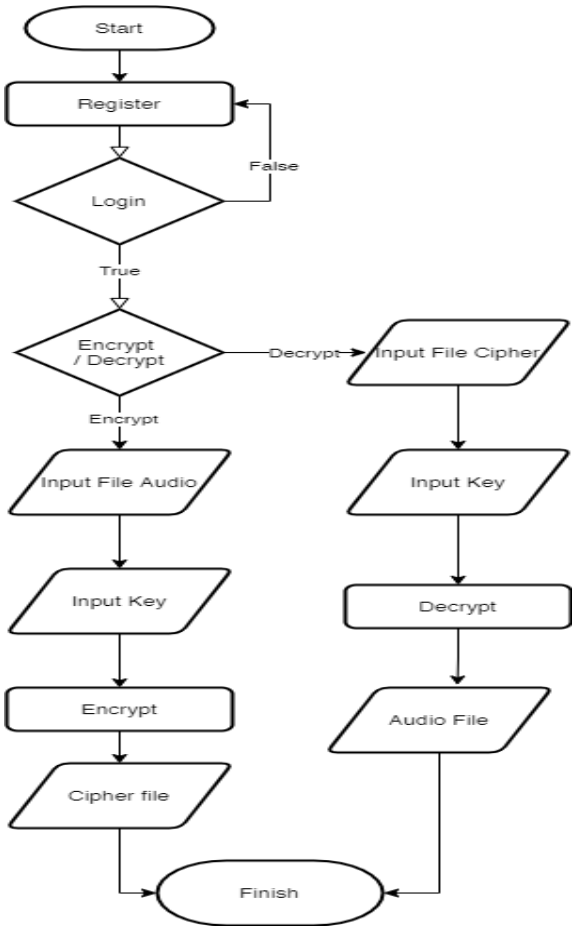

Figure 3. Flowchart of the proposed method

Data Input

There are two types of audio which are divided into two main categories, namely analog audio and digital audio. Analog audio is sound that represents an electric voltage either active or potential that causes variations in pressure and displacement of the wave medium. These waves create maximum compression in cycles measured in Hertz or cycles per second. Digital audio is audio that represents sound as a series of binary numbers or describes sound wave-based similar to that in analog audio.

The difference between analog audio and digital audio is in the waveform, represented by small amplitude samples, which are stacked one after another to produce a representation of the audio signal.

Various audio file formats are commonly used today, WAV (WAVE-Form), AAC (Advanced Audio Coding), MPEG Layer 3 (MP3), Ogg and Ogg Vorbis. These file formats have their respective advantages. In this encryption and decryption application, audio files with the extension wav are used, because wav uses PCM (Pulse Code Modulation) coding in this way, details are not lost when analog audio is digitized and stored. Wav data is uncompressed data, so all audio samples are stored on the hard disk.

RESULT

Tests are carried out on methods and applications. Testing of the method is carried out using Known-Plaintext Analysis (KPA) and analysis of the speed of the encryption and decryption processes. KPA analysis uses the Cryptool application, while the analysis of the speed of the encryption and decryption process is carried out on the application that has been built. In addition to these two analyses, testing was also carried out on all modules in the application that had been built.

This research uses WAV audio data. There are 10 data obtained from the web. with sizes varying from 140KB to 10MB. The data size does not represent the duration of the audio data because each data has a different duration.

The first experiment is the Known-Plaintext Analysis. This to show the results of encryption and decryption using the original data (plaintext) which is known by the researcher and the final data/encryption result (ciphertext), without the key being known for the encryption and decryption process. Because the data used is audio data, before processing the data is converted to hexadecimal form. This is to facilitate the calculation process because the encryption and decryption process requires numerical data in the calculation.

In this test, it was found that the KPA threat managed to find the original data form for all experimental data, with an average similarity of 0.049%. This shows that the proposed method has succeeded in counteracting security threats in the encryption results. The attack method used is brute force for all data.

The next test is to test the speed of the proposed method in processing data to be encrypted and decrypted. This test uses a speed limit of 1000000 per second. The results shows that the proposed method successfully encrypts audio data with an average speed of 14.35 seconds, and successfully decrypts data with an average speed of 13.25 seconds. This is with a note that the encryption and decryption process of data with a size under 1MB is obtained for less than 5 seconds. The larger the size of the data, it is directly proportional to the speed of the encryption and decryption process. This is because audio data with a larger size means that it has more content, so if it is converted to hexadecimal form, it requires more calculation processes.

Table 1. Audio data retrieved

No	File Name	Duration	Size
1	maybe-next-time.wav	1 seconds	140
2	maybe-next-time-huh.wav	2 seconds	176
3	conga_groove.wav	4 seconds	375
4	Wav_868kb.wav	5 seconds	868
5	file_example_WAV_1MG.wav	33 seconds	1
6	file_example_WAV_2MG.wav	33 seconds	2
7	BabyElephantWalk60.wav	60 seconds	2.5
8	SoftPianoMusic_16000_mono.wav	136 seconds	4
9	file_example_WAV_5MG.wav	29 seconds	5
10	Soft Piano Music_16000hz.wav	136 seconds	8

Table 2. Results of decryption decryption process for all data using Cryptool

N	File Name	Decrypt	Similarity
1	maybe-next-time.wav	120	0,2%
2	maybe-next-time-huh.wav	135	0,1%
3	conga_groove.wav	250	0,1%

4	Wav_868kb.wav	540	0,03%
5	file_example_WAV_1MG.wav	671	0,02%
6	file_example_WAV_2MG.wav	1270	0,04%
7	BabyElephantWalk60.wav	2500	0%
8	SoftPianoMusic_16000_mono.wa	4070	0%
9	file_example_WAV_5MG.wav	4250	0%
1	Soft Piano Music_16000hz.wav	8000	0%
	Average		**0,049%**

Table 3. The results of testing the speed of the encryption and decryption process

No.	File Name	Audio	Size	Encrypt Duration	Decrypt Duration
1	maybe-next-time.wav	1	140	0,604	0,603
2	maybe-next-time-huh.wav	2	176	0,840	0,822
3	conga_groove.wav	4	375	2,085	2,004
4	Wav_868kb.wav	5	868	4,002	3,870
5	file_example_WAV_1MG.wav	33	1	5,215	4,924
6	file_example_WAV_2MG.wav	33	2	10,05	10,0
7	BabyElephantWalk60.wav	60	2.5	20,97	19,4
8	SoftPianoMusic_16000_mono.wa	136	4	20,94	20,8
9	file_example_WAV_5MG.wav	29	5	25,90	26,2
1	Soft Piano Music_16000hz.wav	136	8	52,91	43,7
	Average			**14,354**	**13,25**

CONCLUSION

In this research, a new encryption method is proposed by combining two existing encryption methods, namely AES and Blowfish. From the test results, it is found that the encryption program has been successfully built and has features to encrypt and decrypt audio data. The program also has a feature of sending encrypted data to fellow program users.

The method was successful in security testing, because the ciphertext data was not successfully decrypted using the KPA method with a similarity level of decryption results only 0.049%. The method successfully encrypts audio data with an average speed of 14 seconds, and successfully decrypts audio data with an average speed of 13 seconds.

ACKNOWLEDGMENTS

This research was supported by Institute of Research and Community Engagement Universitas Tarumanagara. We thank our colleagues from Faculty of Information Technology Universitas Tarumanagara who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

REFERENCES

1. Katella, K. (2021). Our pandemic year—A COVID-19 timeline. Yale Medicine, 9.
2. WHO, B. (2020). Listings of WHO's response to COVID-19. World Health Organization.
3. Pandey, A. K., Mishra, S. S., Wadgave, Y., Mudgil, N., Gawande, S., & Dhange, V. B. (2021). The COVID-19 variants: an overview. International Journal of Community Medicine and Public Health, 8(10), 5148.
4. Simanjuntak, T. R. (2021). Sejarah hari ini: 2 maret 2020, warga depok terkonfirmasi sebagai pasien pertama covid-19. Kompas. Com, 3(6).
5. COVID, S. D. M. P., & PERMAS, A. D. TINJAUAN KEBIJAKAN RELAKSASI PEMBIAYAAN PADA BANK JATENG KCPS.
6. Hastuti, P., Harefa, D. N., & Napitupulu, J. I. M. (2020). Tinjauan kebijakan pemberlakuan lockdown, phk, psbb sebagai antisipasi penyebaran covid-19 terhadap stabilitas sistem moneter. Prosiding WEBINAR Fakultas Ekonomi Unimed "Strategi Dunia Usaha Menyikapi Status Indonesia Sebagai Negara Maju: Pra dan Pasca Covid-19", 57-70.
7. Hastuti, P., Harefa, D. N., & Napitupulu, J. I. M. (2020). Tinjauan kebijakan pemberlakuan lockdown, phk, psbb sebagai antisipasi penyebaran covid-19 terhadap stabilitas sistem moneter. Prosiding WEBINAR Fakultas Ekonomi Unimed "Strategi Dunia Usaha Menyikapi Status Indonesia Sebagai Negara Maju: Pra dan Pasca Covid-19", 57-70.
8. Tanamal, G. (2022). Hubungan antara Kesepian dengan Kecenderungan Nomophobia pada Mahasiswa Universitas Kristen Satya Wacana (Doctoral dissertation).
9. Kushwaha, K. S. (2020). IOT BASED HEALTH CARE SYSTEM PANDEMIC (COVID-19) ASPERENT USING CLOUD COMPUTING.
10. He, J., Zheng, D., Guo, R., Chen, Y., Li, K., & Tao, X. (2021). Efficient identity-based proxy re-encryption scheme in blockchain-assisted decentralized storage system. International Journal of Network Security, 23(5), 776-790.
11. Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics, 10(17), 2110.
12. Rakhmat, E., Dwiyatno, S., Sulistiyon, S., Irawan, A., & Setiawan, F. (2021). Pemanfaatan Aplikasi Owncloud Pada Sistem Keamanan Cloud Computing. Jurnal Sistem Informasi Dan Informatika (Simika), 4(2), 146-155.
13. Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE access, 7, 112713-112725.
14. Sanda, M. U., Dawud, J. A., Ibrahim, U., & Bukar, Y. (2022). Insecticide Production from Orange Peel Oil. International Journal of Pure & Applied Science Research.
15. Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2015). Dual-server public-key encryption with keyword search for secure cloud storage. IEEE transactions on information forensics and security, 11(4), 789-798.
16. Tajammul, M., & Parveen, R. (2019). Key generation algorithm coupled with DES for securing cloud storage. International Journal of Recent Technology in Engineering.
17. Mahardhika, M. A., Purwanto, Y., & Ruriawan, M. F. (2021). Pengamanan Data Cloud Storage Dengan Menggunakan Advanced Encryption Standard Dan Elliptic Curve Digital Signature Algorithm Pada Secure Socket Layer Berbasis Website. eProceedings of Engineering, 8(2).
18. Coronado, A. S. (2013). Computer security: Principles and practice.

19. Johnson, S. (2007). Cryptography for Developers. Syngress Publishing.
20. Schneier, B. (1994). The Blowfish encryption algorithm. Dr Dobb's Journal-Software Tools for the Professional Programmer, 19(4), 38-43.
21. Kabal, P. (2017). Audio file format specifications. MMSP Lab, ECE, McGill University.