Journal of Theoretical and Applied Information Technology
15th February 2024. Vol.102. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE PERFORMANCE OF THE 3DES AND FERNET ENCRYPTION IN SECURING DATA FILES

SITI MUNIRAH MOHD[1], SHAFINAH KAMARUDIN[2*], NORHANIZAH YAHYA[2], SAZLINAH HASAN[2], MUHAMMAD LUQMAN MAHAMAD ZAKARIA[2], SAHIMEL AZWAL SULAIMAN[3], DJOKO BUDIYANTO SETYOHADI[4]

[1]GENIUS Insan College, Universiti Sains Islam Malaysia, Bandar Baru Nilai, Negeri Sembilan, Malaysia

[2]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, Malaysia.

[3]Centre for Mathematical Sciences, Universiti Malaysia Pahang, Kuantan, Pahang, Malaysia.

[4]Informatics Department, Universitas Atma Jaya Yogyakarta, Yogyakarta, Indonesia.

Email: shafinah@upm.edu.my

ABSTRACT

The number of cyber attacks launched has increased five-fold since the advent of the Coronavirus Disease Pandemic (COVID-19) in 2019. Ransomware is currently one of the highest digital risks as it aids cybercriminals to use persistent threat tools and techniques to get access to targeted networks by way of third parties. Therefore, this study aims to implement the symmetric encryption algorithms known as 3DES and Fernet methods as a means for securing files. In addition, this study evaluates the 3DES and Fernet encryption methods' performance in protecting confidential file. This study significantly contributes in comprehending Fernet and 3DES methods for securing confidential files, identifying the most efficient cryptographic symmetric algorithm for file security, and providing comparative results between Fernet and 3DES. This study applies both 3DES and Fernet in the scenario of client-server architecture in performing encryption and decryption processes. The results from the current study has shown successful implementation of these two encryption methods for both the encryption and decryption processes. In addition, this study evaluates the temporal efficiency for the encryption process. Five different text file sizes ranging from 10KB to 50KB were used for the experimental trial in evaluating the performance of both encryption methods. The outcome reveals that the Fernet encryption method performs better than 3DES.

Keywords: *Fernet Algorithm, 3DES Algorithm, Encryption, Decryption, File Security*

1. INTRODUCTION

After the advent of the Coronavirus Pandemic in 2020, the volume of cyber attacks were recorded to have quintupled[1]. For instance, Malaysia recorded a total of 8,669 cybersecurity incidents throughout 2021, including fraud (6,737 cases), intrusion (1,354 cases), and malicious codes (578 cases)[2]. GLOBAL cybersecurity leader Trend Micro Inc recently disclosed that during the first half of 2021, it stopped a total of 40.9 billion threats in the form of emails, malicious files, and harmful URLs for clients marking an alarming surge of 47% from previous years. Globally, ransomware was the topmost threat in the first quarter of 2021 as cybercriminals targeted many known figures. The standard modus operandi employed advanced persistent threat tools and strategies to steal and encrypt victim's data after collaborating with third parties to acquire access to the targeted networks [3].

By 2019, it was reported that data was stolen from Microsoft Office 365, Box, EE, Mumsnet, Town of Salem, and even a number of German politicians [4, 5]. All personal data, company data, and messages amongst individuals or countries can be classified as confidential. When pertinent data is stolen, there is a likelihood that an unauthorized person may use the victim's information in fraudulent ways, such as applying for a loan using the victim's details [5]. In light of this, cybersecurity, including secure data transmission over the internet, continues to be a major concern for internet users. Thus, methods to protect information and data, particularly confidential data, must be continuously strengthened.

There are many different strategies available to protect confidential data. The use of cryptographic systems is one strategy that can be utilized to protect data and information that is considered to be confidential. Cryptography ensures that the message can only be comprehended by the addressed user. This study aims to explore and implement two symmetric cryptographic systems, the 3DES and Fernet encryption methods. Furthermore, different file size bytes were used in the experiment to compare the performance aspects of these two approaches. The comparison was carried out to determine which encryption technique was better suited for protecting a confidential file. Significant contributions of this study include comprehending Fernet and 3DES methods for securing confidential files, identifying the most efficient cryptographic symmetric algorithm for file security, and providing comparative results between Fernet and 3DES.

The following is the structure of this paper: In Section 2, an overview of the context of the study is presented. In Section 3, the methodology of the study is discussed. The demonstration of the algorithms is presented in Section 4. In Section 5, the results and discussion of the study are presented. Finally, in Section 6, conclusions are presented along with recommendations for further research.

2. BACKGROUND

Security remains a big issue in the digital world. In [6], it mentioned that the requirements of security involves the terms of confidentiality, availability and integrity. Confidentiality measures prevent illegal access attempts to sensitive information. Therefore, the sensitive database and information must be protected from unauthorized access. Availability refers to ensuring that data is consistently and readily accessible for authorized parties and properly that it maintains connected components, including hardware and technical infrastructure, model, and systems to keep data and show the information. Integrity defines the way to maintain the consistency, accuracy, and trustworthiness of the said data.

Therefore, cryptography was introduced to ensure the security of data. Cryptography refers to secure information and communication techniques based on mathematical concepts and a set of rule-based calculations called algorithms to transform messages in such a way that is difficult to decipher for unauthorized users[7]. Cryptography is derived from Greek terms "kryptos" and "graphos", which refer to secret writing [8]. Cryptography involves the process of encryption and decryption [8, 9]. The goal of cryptography is to enable secure communications despite the presence of adversaries or other potentially harmful third parties in the environment [6].

Encryption is the process of converting plaintext into ciphered text (unreadable format) in order to make it difficult for unauthorized recipients of a message to understand the information being transmitted [6, 9]. Therefore, only authorized parties are able to access the ciphered text, by converting the message into its original form. This process is known as decryption [10]. Thus, cryptography allows the secure protection of data without granting unauthorized parties unrestricted access or the ability to view protected files and documents[11].

The most common cryptographic system is symmetric and asymmetric key encryption algorithms[5, 12, 13]. Symmetric key encryption algorithm implements the same key for message encryption and decryption. Only the authorized sender and recipient who communicate with each other can read the confidential messages (encrypted messages) by using a similar secret key. The message security can be increased by allocating the keys to different parties. The strength of symmetric key encryption heavily relies on the secrecy of the encryption and decryption keys. DES, 3DES and AES are examples of symmetric key encryption algorithms [14].

The symmetric key encryption algorithm can be further divided into block cipher and stream cipher. A block cipher works with a single data block at a time. The plain text or message is divided into blocks; and each block is processed separately using a key and a cryptographic algorithm. Meanwhile, the stream cipher enables algorithms to perform encryption and decryption of shared data using a symmetric key mechanism. In contrast, asymmetric key encryption algorithms employ two separate keys, public and private keys. The public key is used for the encryption process. The decryption process requires the private key, which is only held by the individual authorized to decrypt the message. Examples of asymmetric key encryption algorithms are RSA, Diffie-Hellman algorithms and digital signature [14].

This study concentrates on symmetric algorithms, which are known for their rapid implementation, efficiency, and effectiveness [14]. The following describes several examples of symmetric cryptographic systems.

2.1 Decryption Encryption Standard

In 1974, IBM and United States government worked together to develop the Decryption Encryption Standard (DES), which was jointly developed to make communication more secure [12, 15], which utilizes a total of 16 iterations, or rounds, of substitution and transpositions (permutation) process to encrypt information. The block size is limited to 64 bits. The key, which governs the transformation, is also made up of 64 bits; however, only the users can only select 56 of these bits to be considered as the actual key bits. The remaining eight bits are used as parity check bits and are in actuality, redundant [16]. In the past, DES was typically utilized for non-digital media as well as banking systems. However, because of its short key length, the National Institute of Standards and Technology (NIST) started a programme to replace DES starting in 1997 [15]. Therefore, DES is considered to be a cryptographic algorithm which is not ultra secure[12].

2.2 Advanced Encryption Standard

Advanced Encryption Standard (AES), also known as the Rijndel algorithm, was published by the National Institute of Standard and Technology (NIST) in 2000 [12, 15, 17]. This algorithm is a well-established algorithm in the categories of symmetric key encryption algorithms. AES operates on block ciphers that divide the data into 128, 192, and 256-bit blocks. Block ciphers use a series of substitution and permutation operations to encrypt data, known as S-boxes [12, 18, 19]. Furthermore, the length of the key determines the number of operation cycles. A key with 128 bits requires ten rounds, a key with 1920 bits requires 12 rounds and a key with 256 bits requires 14 rounds. The AES is more secure and more rapid when compared to DES. AES also has the advantage of higher resistance to cyber attacks, the ability to support extended key lengths, and has undergone extensive testing to assure its security. In addition, AES has been implemented and evaluated on various devices, including Internet of Things (IoT) devices [6, 20].

2.3 3DES

3DES was suggested by IBM (International Business Machines Corporation) in 1998 as a successor for DES. 3DES includes improved key size and applies the DES algorithm three rounds in each data block. The key length for the 3DES is 112 and 168 bits, the number of rounds is 48 and the block length is 64 bits [2]. This algorithm aims to increase protection and security through its longer key size relative to DES. 3DES is more challenging to crack than DES [14]. However, it is more time-consuming than DES in terms of the application of the encryption process[12]. The 3DES encryption method is the abbreviation of Triple Data Encryption Standard. This method is the updated version of DES, using three cycles of the DES algorithm in each data block. Whereas DES employed a56 bits key size, 3DES utilized a 168 bits key size. The following is the mechanism of 3DES[21]:

1. 3DES has three different keys.
2. Key 1 and Key 2 are different, but Key 1 and Key 3 are the same.
3. All keys are identical.

2.4 Fernet Encryption Method

The Fernet encryption method, also known as Fernet algorithm, is similar to an AES algorithm. Fernet provides the rotation of keys that are generated through "MultiFernet during ciphering or encrypting plain[22, 23]. In order to decrypt the encoded text, Fernet executes an inverse function conversion of ciphered text to plain text, and the output is presented as a "string" value from bytes. There are three main steps in a Fernet encryption and decryption sequence as shown below[22, 23]:

Step 1 : Generate the key.

Step 2 : Assign the key value to the selected variable.

Step 3 : Convert the plain text into ciphered text.

Fernet provides users with a highly secured key superior to existing symmetric algorithms such as AES. Additionally, to prevent private communications and data from being eavesdropped, Fernet encryption also gives strong encryption in data manipulation without a key in various situations such as[22]

- Sign-stamping (signature through SHA56 and HMAC).
- Time-stamping.
- Random allocation for security.
- Generation of key through a secure mechanism and adopting a secure algorithm towards encrypting messages (PKCS7 padding and AES under CBS-mode).

The previous works have conducted a study of AES, TDES and other symmetric key cipher excluding Fernet on the basis of encryption time with the variations of file features including data type, data size, data density and key sizes [24]. In [25], a study evaluated the execution time, memory utilization and ciphertext size on the process of encryption and decryption processes for symmetric algorithms known as AES, 3DES, Blowfish and Twofish. Additionally, previous work comparing the AES, DES and Blowfish cryptographic algorithms for small and large data files also raised concern about the execution time and memory used[26]. Therefore, selecting of appropriate parameters is necessary while performing a study related to the performance of symmetric cryptographic algorithms.

3. METHODOLOGY

The steps involved in carrying out this study are shown in Figure 1. Firstly, the requirements for both software and hardware are identified. Table 1 shows the details of the requirements used in this study. Figure 2 shows a flow diagram which has been illustrated based on the client-server architecture). There are two spilt algorithms being implemented for this study: (1) the Fernet encryption method and (2) the 3DES encryption method. Both algorithms are programmed in Python. The testing is carried out to ensure that the algorithms are able to produce the desired results. The experiment is conducted using five different file sizes to evaluate the performance of these methods. The parameters used in evaluating the performance are the encryption and decryption times. Finally, the data gathered is analyzed and interpreted.

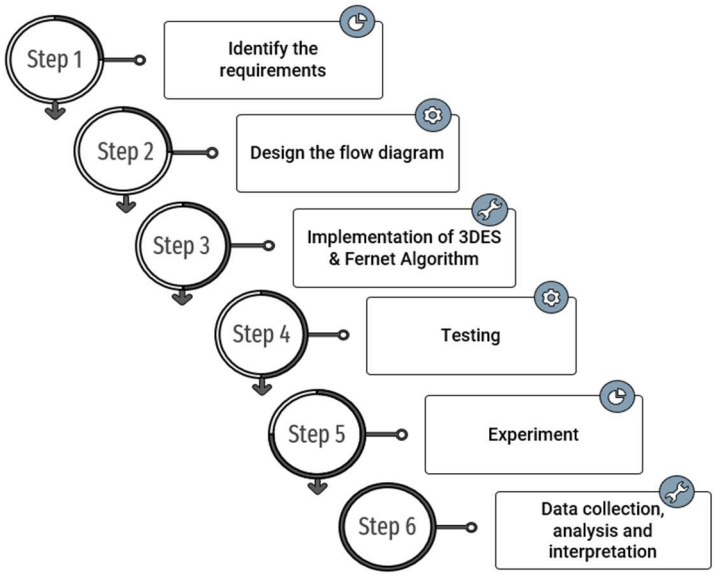

Figure 1. The methodology

Table 1: The requirements for 3DES and Fernet algorithms implementation

Requirement	Description
IDE	PyCharm 2022.3.1 (Community Edition)
Programming Language	Python
JDK Version	Runtime version: 17.0.5+1-b653.23 amd64 VM: OpenJDK 64-Bit Server VM by JetBrains s.r.o.
Operating System	Windows 11 Home Single Language
Processor	11th Gen Intel(R) Core (TM) i3-1115G4, 3.00 GHz
RAM	8.00 GB, 3733MHz
Graphics	Intel® UHD Graphics

Journal of Theoretical and Applied Information Technology
15th February 2024. Vol.102. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

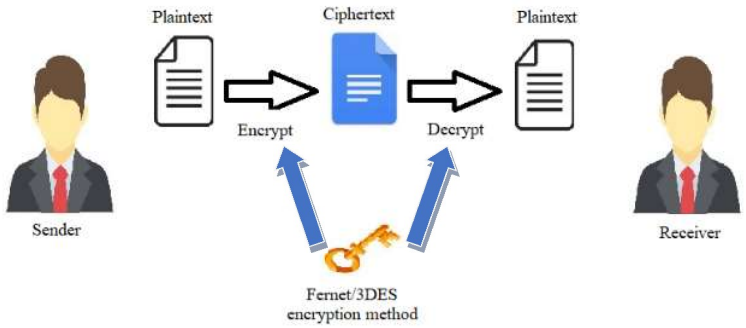

Figure 2: The flow diagram of the Fernet and 3DES implementation algorithms

4. THE DEMONSTRATION OF 3DES AND FERNET

The algorithm is tested in order to ensure the process of encryption and decryption procedures are functioning as intended. Figure 3 is an example of a plaintext that was used in this study. The example of the ciphered text that has been produced as a result of utilizing the 3DES method is presented in Figure 4. Meanwhile, Figure 5 shows an example of the ciphered text after utilizing the Fernet encryption method. As was anticipated, the decryption process resulted in a successful output as well. This demonstrates that both algorithms performed as expected.


dec1_crime.txt - Notepad

File Edit View

```
Crime Prevention Programs and Criminal Rehabilitation 1500

The success of the human civilization is largely attributed to the establishment of laws and the subsequent following of
This system is known as the criminal justice system and its major role is to deliver justice by punishing offenders and d
This can be achieved through crime prevention strategies. This paper will analyze the various crime prevention programs a

Crime Prevention
Defining Crime Prevention
Crime prevention is one of the major goals of a good criminal justice system. To fulfil this goal, the system has various
In the context of the criminal justice system, crime prevention refers to the efforts that are taken to change the behavi
Crime prevention programs are defined as "focused efforts to change, restrict or create a routine practice in a crime pre

Types of Crime Prevention Programs
Shock programs have been used as a prevention tool by the criminal justice system. In this program, offenders are sent to
The offender is given a taste of prison and he/she is likely to avoid behavior that might cause him/her to be sent back i
The criminal justice system offers repeat offender prevention programs for young offenders who are likely to become harde
Such behavior might include substance abuse, family problems, school problems and delinquent behavior. The programs aim t
Proactive measures such as random drug tests and surveillance are undertaken with the offender's knowledge. In addition t
A successful prevention program adopted by the criminal justice system is day reporting. In this program, the offender is
The counselling services offered in this program help the offenders to deal with the psychological issues that might cont
The criminal justice system also implements electronic monitoring programs to prevent crime. In this program, offenders a
These programs have significant advantages as they enable the offender to continue playing an active role in the society
Mackey and Levan (2012) observe that the offender remains rooted in his/her community where he/she is able to work, stay

Criminal Rehabilitation
Defining Rehabilitation
Rehabilitation is a significant goal of the criminal justice system since it is desirable that the offenders successfully
Rehabilitation aims at increasing self-restraint, providing work skills, and educational services to offenders. This is d

Methods of Criminal Rehabilitation
Rehabilitation considers that it is hard for most inmates to abruptly shift from the strict schedule imposed in prison to
Gabor (2011) reveals that the criminal justice system has endorsed a number of reintegration programs that aim to reorien
Most of these activities include community service where the offender gets to interact with the rest of the society (Gabo
A rehabilitation service offered by prison facilities is hosting community resource fairs within the prison. Mohr (2013)

Here they share material to aid offenders in their search for employment after they are released. The offenders are provi
Another rehabilitation program offered by the criminal justice system aims at assisting offenders who have drug problems.
Most addicts are therefore likely to end up in correctional facilities due to their involvement with drugs. Jones (2009)
In addition to this, drug use contributes to the increase in criminal activity. Drug users are known to engage in crime b

Conclusion
This paper set out to discuss various crime prevention programs and rehabilitation efforts used by the criminal justice s
The paper has noted that crime prevention programs are aimed at ensuring that crimes are not committed by offenders in th
The paper has discussed rehabilitation, which is meant to restore offenders to normal life after they have served their s

Berenji, B. (2014). Recidivism and Rehabilitation of Criminal Offenders: A Carrot and Stick Evolutionary Game. PLoS ONE,
Gabor, T. (2011). Evidence-based crime prevention programs: A literature review.
Jones, M. (2009). Prison overcrowding: the sentencing judge as social worker. Widener Law Journal, 18(1), 491-498.
MacKenzie, D.L. (2003). Criminal justice and crime prevention.
Mackey, D., & Levan, K. (2012). Crime Prevention. NY: Jones & Bartlett Publishers.
Mohr, G. (2013). Integrated Criminal Justice Systems: Working Collaboratively to Reduce Recidivism. Corrections Today, 75
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Figure 3: Fernet decrypted text file

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

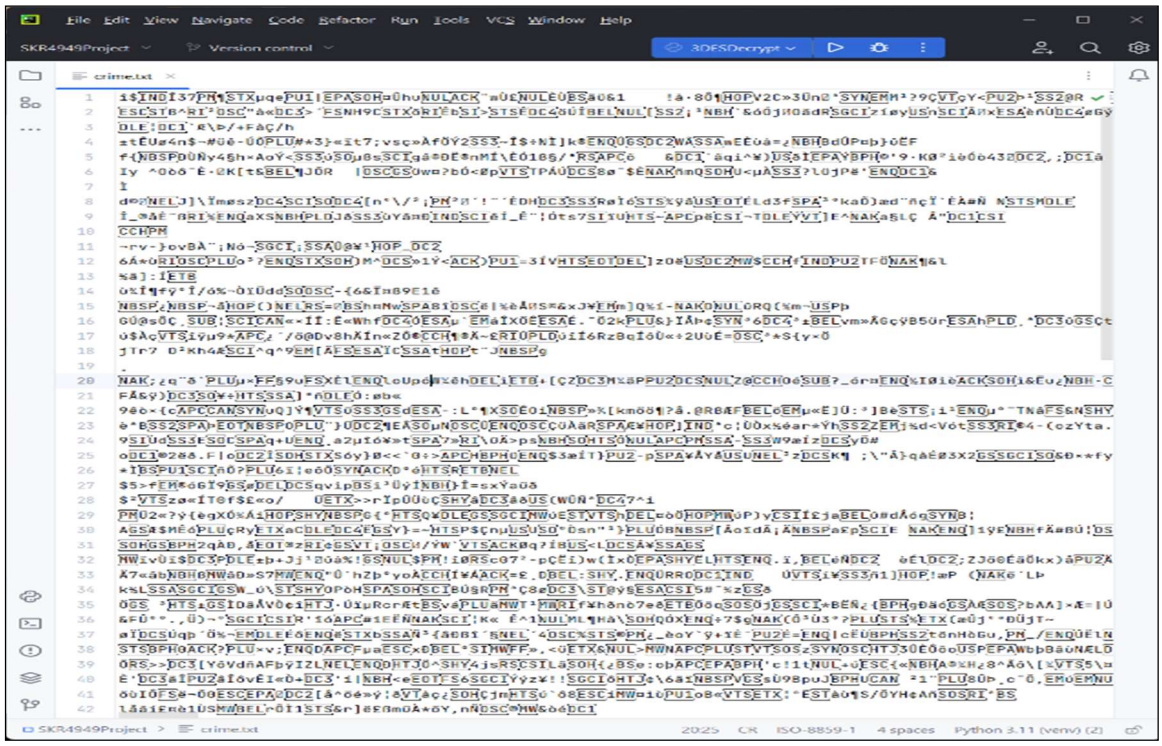

Figure 4: 3DES encrypted file

Figure 5: Fernet encrypted file

5. RESULTS AND DISCUSSION

The performance of both these methods is evaluated by considering the time taken to encrypt the file based on the different file sizes. Table 2 shows the time taken to encrypt the plaintext to ciphered text using the 3DES encryption method. The findings show that the longest time taken was 10.011ms for a file size of 50KB. Furthermore, the average time taken by using 3DES ranged from 3.9486 to 8.7320ms. The findings showed that as the file size increases, the average time also increases in correlation.

Table 3 displays the performance of Fernet encryption algorithms in terms of the time required for the encryption procedure. The longest time taken for a 50KB file was 5.377 ms. The findings showed that the average time increases (2.8954 to 4.0396ms) as file sizes increases. Based on Table 2 and 3, the 3DES method takes around twice the amount of time when compared to the Fernet encryption method.

The duration of time required to decrypt an encrypted file using the 3DES method at the receiver end is presented in Table 4. The time is measured for the file conversion from a ciphered text file into a plain text file. Finally, Table 5 presents the

decryption time of the encrypted file using the Fernet algorithm in the receiver end after the file is transferred from ciphered text to plain text.

According to the present findings, a 10KB file consumes approximately roughly the equivalent amount of time, with a 1ms difference for both methods. However, this study shows significant differences in the amount of time needed to encrypt a file as its size increases. This study highlights that Fernet performs better than 3DES.

Table 2: The 3DES encryption time(ms)

Text File Size (KB)	Encrypt Time (ms)					Average (ms)
	Test 1	Test 2	Test 3	Test 4	Test 5	
10	3.833	3.939	4.099	3.949	3.923	3.9486
20	5.627	5.643	5.654	5.179	5.500	5.5206
30	6.328	6.141	6.195	5.980	6.302	6.1892
40	7.516	7.473	7.135	7.693	6.996	7.3626
50	8.297	8.581	10.011	8.480	8.291	8.7320

Table 3: Fernet encryption time (ms)

Text File Size (KB)	Encrypt Time (ms)					Average (ms)
	Test 1	Test 2	Test 3	Test 4	Test 5	
10	2.893	2.802	2.894	2.996	2.892	2.8954
20	2.890	2.981	3.050	3.098	3.080	3.0198
30	3.191	3.033	3.381	2.844	3.068	3.1054
40	3.214	3.304	3.154	3.134	3.247	3.2106
50	4.158	3.530	5.377	3.674	3.459	4.0396

Table 4: 3DES decryption time in milliseconds

Text File Size (KB)	Decrypt Time (ms)					Average Decrypt Time (ms)
	Test 1	Test 2	Test 3	Test 4	Test 5	
10	2.519	1.604	1.430	1.721	1.400	1.7348
20	2.420	2.464	2.704	2.423	3.954	2.7930
30	3.550	3.447	3.375	3.402	4.547	3.6642
40	4.385	4.415	4.611	4.558	4.863	4.5664
50	5.939	5.332	5.702	6.396	5.333	5.7404

Table 5: Fernet decryption time in milliseconds

Text File Size (KB)	Decrypt Time (ms)					Average Decrypt Time (ms)
	Test 1	Test 2	Test 3	Test 4	Test 5	
10	0.473	0.541	0.512	0.571	0.453	0.5100
20	0.472	0.478	0.556	0.559	0.531	0.5192
30	0.445	0.511	0.460	0.488	0.518	0.4844
40	0.503	0.446	0.559	0.579	0.493	0.5160
50	0.534	0.485	0.453	0.532	0.537	0.5082

5. CONCLUSION

This study was conducted to demonstrate the Fernet and 3DES encryption method in securing files. The algorithms were developed using the Python programming language and the cryptography library. The different file sizes used were in order to explore the performance of Fernet and 3DES encryption methods. In this study, the Fernet algorithm performs significantly better than the 3DES algorithm, mainly emphasizing time efficiency without comprising data security. This is due to fact that the Fernet algorithm is based on the AES cryptographic system, which is known as a powerful and complex algorithm. This study has significantly proved that Fernet is better compared to 3DES for securing confidential files. In the future, the combination of Fernet with other cryptographic methods can be explored to further strengthen security and deter cybersecurity breaches.

ACKNOWLEDGEMENT

This work was financially supported by the Universiti Sains Islam Malaysia and Universiti Putra Malaysia. Universiti Malaysia Pahang and Universitas Atma Jaya Yogyakarta are acknowledged for their technical support and assistance.

DECLARATION OF COMPETING INTEREST

It is declared that there are no competing interests that could potentially influence the research work described in this paper.

REFERENCES:

[1] World Health Organization. "WHO reports fivefold increase in cyber attacks, urges vigilance." https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed May 1, 2023).

[2] MalayMail. "Malaysia experienced 57.8 million virus cyber attacks in Q1, says US cybersecurity firm Fortinet." MalayMail. https://www.malaymail.com/news/malaysia/2022/06/07/malaysia-experienced-578-million-virus-cyber-attacks-in-q1-says-us-cybersecurity-firm-fortinet/11070 (accessed May 1, 2023).

[3] C. S. Cheah. "Cyberattacks surge in 1H 2021 as Trend Micro blocks 41 billion threats." https://focusmalaysia.my/cyberattacks-surge-in-1h-2021-as-trend-micro-blocks-41-billion-threats/#:~:text=In%20Malaysia%20specifically%2C%20Trend%20Micro%20found%20that%3A%201,by%20160%25%20from%201H%202020%20to%206.6%20million (accessed May 4, 2023).

[4] Tech Advisor Staff. "The Biggest Data Breaches. Tech Advisor. ." https://www.techworld.com/security/uksmost-infamous-data-breaches-3604586/ (accessed December 3, 2021).

[5] E. K. Wijaya, R. Kumala, and B. Soewito, "Improving Security and Imperceptibility using Modified Least Significant Bit and Fernet Symmetric Encryption," *Journal of Theoretical and Applied Information Technology,* vol. 100, no. 17, pp. 5660-5671, 2022.

[6] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things,* vol. 22, p. 100759, 2023/07/01/ 2023, doi: https://doi.org/10.1016/j.iot.2023.100759.

[7] K. Richards. "What is cryptography?" https://www.techtarget.com/searchsecurity/definition/cryptography (accessed April 29, 2023).

[8] S. Kamarudin and M. M. Ikram, "File Security based on Pretty Good Privacy (PGP) Concept," *Computer and Information Science,* vol. 4, no. 4, pp. 10-28, 2011, doi: 10.5539/cis.v4n4p10.

[9] M. Sudarma and D. P. Hostiadi, "Implementation of Email Security using PGP at Zimbramail Server," *International Journal of Computer Science Issues,* vol. 13, no. 6, pp. 113-119, 2016, doi: 10.20943/01201606.113119.

[10] J. N. Cheltha C, M. Rakhra, R. Kumar, and H. Walia, "A Review on Data hiding using Steganography and Cryptography," presented at the 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Noida, India, 2021.

[11] A. Ghahrai. "How to Encrypt and Decrypt Data in Python using Cryptography Library." https://devqa.io/encrypt-decrypt-data-python/ (accessed April 29, 2023).

[12] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Research on various cryptography techniques," *International Journal of Recent Technology and Engineering,* vol. 8, no. 2S3, pp. 395-405, 2019, doi: 10.35940/ijrte.B1069.0782S319.

[13] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," presented at the 2nd International Conference on Computing and Data Science, Stanford, CA, USA, 2021.

[14] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A Survey on the Cryptographic Encryption Algorithms," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 11, pp. 333 - 344, 2017.

[15] K. Rabah, "Theory and implementation of data encryption standard: A review," *Information Technology Journal,* vol. 4, no. 4, pp. 307-325, 2005.

[16] G. J. Simmons. "Data Encryption Standard." Britannica. https://www.britannica.com/topic/Data-Encryption-Standard (accessed May 13, 2023).

[17] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security,* vol. 16, pp. 1-11, 2017.

[18] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," *Alexandria Engineering Journal,* vol. 72, pp. 37-50, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.aej.2023.03.061.

[19] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," *International Journal of Electrical and Computer Engineering,* vol. 13, no. 2, pp. 708-1723, 2023, doi: 10.11591/ijece.v13i2.pp1708-1723

[20] S. Das and S. Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure," *Computers and Electrical Engineering,* vol. 101, p. 107991, 2022/07/01/ 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107991.

[21] S. M. K. Wani and A. Kumar, "Secure File Storage on Cloud Using a Hybrid Cryptography Algorithm," *International Journal of Research in Engineering, Science and Management,* vol. 5, no. 5, pp. 35-39, 2022.

[22] N. R. Ananthanarayanan and C. Nivetha, "Cipher and Decipher using Cryptography Fernet Application for Secure Data," *International Research Journal of Modernization in Engineering Technology and Science,* vol. 5, no. 5, pp. 5048-5051, 2023.

[23] Pronika and S. S. Tyagi, "Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications,* vol. 8, no. 4, pp. 288-299, 2021, doi: 10.22247/ijcna/2021/209697

[24] R. Masram, V. Shahare, J. Abraham, and R. Moona, "Analysis and comparison of symmetric key cryptographic algorithms based on various file features," *International Journal of Network Security & Its Applications,* vol. 6, no. 4, p. 43, 2014.

[25] H. Dibas and K. E. Sabri, "A comprehensive performance empirical study of the symmetric algorithms:AES, 3DES, Blowfish and Twofish," presented at the 2021 International Conference on Information Technology (ICIT), mman, Jordan, 2021.

[26] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," *International Journal of Information Technology,* vol. 11, pp. 813-819, 2019.