Salud, Ciencia y Tecnología – Serie de Conferencias. 2024; 3:609
doi: 10.56294/sctconf2024609

Categoría: STEM (Science, Technology, Engineering and Mathematics)

ORIGINAL

Privacy-Preserving Image Storage on Cloud Using An Unified Cryptographic Authentication Scheme

Almacenamiento de imágenes en la nube para preservar la privacidad mediante un esquema unificado de autenticación criptográfica

R. Manivannan[1], G. Venkateshwaran[1], D. Menaga[2], S. Sivakumar[3], M. Hema Kumar[4], Minu Susan Jacob[5]

[1]Department of Computer Science and Engineering, E.G.S. Pillay Engineering College. Nagapattinam, India.
[2]Department of Computer Science and Engineering, St.Joseph's Institute of Technology. Chennai, Tamil Nadu, India.
[3]Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology. Coimbatore, India.
[4]Department of Electronics and Communication Engineering, Sona College of Technology. Salem, Tamil Nadu, India.
[5]Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology. Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119, Tamilnadu, India.

Cite as: Manivannan R, Venkateshwaran G, Sivakumar S, Kumar MH, Jacob MS. Privacy-Preserving Image Storage on Cloud Using An Unified Cryptographic Authentication Scheme. Salud, Ciencia y Tecnología - Serie de Conferencias 2024; 3:609 . https://doi.org/10.56294/sctconf2024609.

Submitted: 06-12-2023 **Revised:** 14-02-2024 **Accepted:** 10-03-2024 **Published:** 11-03-2024

Editor: Dr. William Castillo-González

ABSTRACT

With the proliferation of several cutting-edge technologies such as the Artificial Intelligence (AI), and Machine Learning (ML), Internet of Things (IoT), cloud technology is gaining colossal popularity in recent years. Despite the general publicity on the theme across the digital world, defending user data kept in the cloud database is the most decisive problem. Recent potential cyber attacks reveal that storing private images entails more unique care related to other types of information on the cloud. As the cloud customer who has kept their images has no control over their data the cloud service provider has to ensure better security against cyber threats. Cryptography algorithms are the best choice to secure pictorial data in the cloud. These techniques transform images into an inarticulate form to keep confidentiality over undependable and vulnerable social media .In this paper, we aim to propose an approach for improving image security on the cloud using cryptography algorithms. We developed a cohesive approach, called Unified Cryptographic Image Authentication (UCIA) to protect user images on a cloud platform. The proposed UCIA approach includes two phases: (i)UCIA engenders a cipher text through a Data Encryption Standard (DES) by providing a key and a message as input, and (ii)UCIA implements a Twofish algorithm to encipher the pictures by applying cipher text. The enciphered picture data is then stored in the cloud database and can be recovered when the customer requests it. The effectiveness of both enciphering and deciphering procedures are analyzed using the evaluation metrics including time for enciphering, deciphering, cloud storage, and enciphering throughput. Experimental results reveal the better performance and strength of the UCIA approach.

Keywords: Cloud Computing; Data Encryption Standard; Image Encryption; Twofish Algorithm.

RESUMEN

Con la proliferación de varias tecnologías de vanguardia como la Inteligencia Artificial (IA), y el Aprendizaje Automático (ML), Internet de las Cosas (IoT), la tecnología en la nube está ganando una popularidad colosal en los últimos años. A pesar de la publicidad general sobre el tema en todo el mundo digital, la defensa de los datos de los usuarios guardados en la base de datos en la nube es el problema más decisivo. Los recientes ciberataques potenciales revelan que el almacenamiento de imágenes privadas conlleva un cuidado más singular en relación con otros tipos de información en la nube.

© 2024; Los autores. Este es un artículo en acceso abierto, distribuido bajo los términos de una licencia Creative Commons (https://creativecommons.org/licenses/by/4.0) que permite el uso, distribución y reproducción en cualquier medio siempre que la obra original sea correctamente citada

Como el cliente de la nube que ha guardado sus imágenes no tiene control sobre sus datos, el proveedor de servicios en la nube tiene que garantizar una mayor seguridad contra las ciberamenazas. Los algoritmos criptográficos son la mejor opción para asegurar los datos pictóricos en la nube. Estas técnicas transforman las imágenes en una forma inarticulada para mantener la confidencialidad sobre medios sociales poco fiables y vulnerables. En este artículo, pretendemos proponer un enfoque para mejorar la seguridad de las imágenes en la nube utilizando algoritmos criptográficos. Desarrollamos un enfoque cohesivo, denominado Autenticación Criptográfica Unificada de Imágenes (UCIA) para proteger las imágenes de los usuarios en una plataforma en la nube. El enfoque UCIA propuesto incluye dos fases: (i)UCIA genera un texto cifrado mediante un Estándar de Cifrado de Datos (DES) proporcionando una clave y un mensaje como entrada, y (ii)UCIA implementa un algoritmo Twofish para cifrar las imágenes aplicando el texto cifrado. Las imágenes cifradas se almacenan en la base de datos en la nube y pueden recuperarse cuando el cliente lo solicite. La eficacia de los procedimientos de cifrado y descifrado se analiza utilizando métricas de evaluación que incluyen el tiempo de cifrado, el descifrado, el almacenamiento en la nube y el rendimiento del cifrado. Los resultados experimentales revelan el mejor rendimiento y fortaleza del enfoque UCIA.

Palabras clave: Cloud Computing; Estándar de Cifrado de Datos; Cifrado de Imágenes; Algoritmo Twofish.

INTRODUCTION

At present, cloud technology is a groundbreaking computing trend in data-driven businesses since enterprises endure to leverage the frugality and facilities offered by cloud vendors. Cloud computing enables small companies to exploit top-notch infrastructure at low cost. Based on recent statistics, the global industry disbursements on cloud infrastructure are projected to increase from $233,4 bn. in 2019 to $623,3 bn. by 2023,(1) and it is anticipated to touch the landmark of $1 tn. by 2024.(2) Based on the Gartner report, 81 % of industries are exploiting cloud services, and this number is predicted to expand soon to stand themselves in this current competitive market.(3) This will be motivated by some aspects such as an increasing demand to espouse new technologies, as-a-service cloud contributions, and the transformative effects of emerging paradigms such as Block chain, IoT, and AI.

Emerging industry applications across the globe make it obvious that cloud computing can often be the key to becoming more advanced, agile, and effective. The key goal of cloud technology is to offer on-demand computing and storage services to customers on the pay-per-use plan.(4) It enables users to gather, communicate, store, and handle big content forms such as text, audio, images, and video effectively. However, owing to the resource allocation characteristics of cloud platforms, data security, and privacy are important problems and fences for systems to frequently transmit data to the cloud server.

Nowadays, most cloud service providers encourage numerous individuals and organizations to store and handle their images on the cloud server. For instance, Apple allows iOS device users to upload their images on a cloud services suite, iCloud to manage memory on their resource-constrained gadgets.(5) Baidu Cloud facilitates its users to store and retrieve their images to the Baidu Wang Pan, and the archives can be orchestrated inevitably on multiple internet-enabled devices.(6) Nearly all the cloud providers offer enormous processing power at low cost, which tempts users to contract out their complex computational problems.

Cloud computing not only fetches numerous reimbursements and facilities but also brings several security and privacy issues as it encompasses diverse technologies such as communication systems, virtualization, operating systems, databases, transaction management, memory management, concurrency control, load balancing, resource scheduling, etc. Further more, the sub contracting of computing and storage devices brings some complex threats to the cloud platform. The cloud servers are susceptible to serious attacks and security threats continuously.

In 2014, iCloud was plodded and private photographs of around 100 personalities were leaked online.(5) There were two severe threats instigated by mis arrangement of Amazon Simple Storage Service (Amazon S3).(7) In one leak, the personal data of 1000 experts and referring organizations was penetrated. The other threat uncovered the private information of groups, artistes, and associations. Hence, the protection of information in the cloud demands a more powerful method for image security with the least processing cost.

Providing security to user image is a critical and challenging task in a cloud environment. Photographs are the most widely employed communication mode in cloud computing .Based on Business Insider, about 4,7 trillion images were taken in 2023, which is a lot to be stored and processed in a cloud database.(8) Similarly, every day Facebook customers store approximately 900 million images, which is equal to 104 images per second.(9) Though exchanging images is a prevalent web activity, most of the communication systems are apprehensive and provides very low the data security. Hence, the illegal access of images is prevalent, and typically, publics do not aware much when sharing their images.

A direct and simple method to protect sensitive data from cyber attacks is to encipher it with powerful algorithms. However, enciphering process can obscure the validation procedure substantially if it is not properly applied. This work develops a unified cryptographic image authentication approach to protect user images on a cloud platform. We employ the Twofish algorithm for enciphering JPG pictures. This algorithm is suitable to secure images in cloud platform due to its high performance and superior level of security. No one can generate a cyber attack to breakdown the Twofish.[10] However, this algorithm will offer the better enactment if the key does not change frequently. Therefore, the sub keys of the Twofish are saved in EEPROM or FLASHPROM of customer end devices for future computations. Hence, if an invaders can snip the sub keys, then they can compute the key easily. To handle this problem, we assimilated DES with the Twofish to protect the uploaded images from being exposed. The major contribution of this work is three-fold:

- We developed a cohesive approach, called UCIA which integrates DES and Twofish algorithms to protect user images on a cloud platform.
- This work generates a secret key through a DES by providing a key and a message as input.
- We apply the Twofish algorithm to encrypt the pictures using the cipher text generated by the DES algorithm. The encrypted picture data is then stored in the cloud database and can be recovered when the customer requests it.
- We implement the proposed UCIA approach using Net Beans IDE 8,2 to analyze the effectiveness of the algorithm.

This article is organized as follows: Section 2 presents some earlier works relevant to this study. Section 3 discusses the intended algorithm. Section 4 discusses the results obtained from the experiments. We conclude this study in section 5. Styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

Related work

This section reviews some prevailing cryptographic algorithms employed for enciphering photographs in a cloud computing environment. To provide more secure image transmission in this thriving epoch of the internet, a large number of investigators have developed efficient enciphering algorithms to prevent personal photographs from cyber attacks in last decade. Quenaya et al. proposed animage enciphering method through the Advanced Encryption Standard (AES) by applying an image pattern.[11] The authors proved that the proposed algorithm outperforms other conventional cryptographic approaches for image security in cloud computing.

Ashwaq et al.[12] proposed the Blowfish algorithm to increase the performance and security of image-enciphering systems. The intended model uses a block block-based image-enciphering method integrated with chaotic map features. This approach employs an adjustable key with a size of up to 448 bits. It utilizes a Feistel register which repeats meek operation 16 times. This algorithm delivers safety against cyber attacks and works faster than other traditional approaches. Adeniyi et al.[13] proposed an enhanced Blowfish algorithm by varying the configuration of the F function to encipher and decipher images. Then, the effectiveness of the original and enhanced Blowfish algorithm will be gained with respect to temporal overhead. Zefreh et al. developed an approachto protect user images in cloud platform through recursive cellular automata replacement. This techniqueuses dynamic keys to produce the enciphered result from the input image. This method has been efficiently employed in diverse practical applications.[14] Numerous efforts and studies are ongoing for image security on this platform. Though several cryptographic approaches for securing user photos in the cloud have been developed, we have not touched a par where secured image transmission could occur.

Ucia model for image security

In this research, we propose an image security model by changing user photographs into a non-understandable form using a cohesive DES-Twofish integration. Users who plan to upload and store their photographs in the cloud can use this method to encipher their photographs when storing them in a cloud server. The cloud user is the proprietor of the image. A Secret key is essential for enciphering the photographs. The Twofish algorithm is suitable for enciphering photos in the cloud computing platform. None the less, it will realize better enactment when the does not vary repeatedly. Typically, the enciphering supplied to the Twofish is kept in EEPROM or FLASHPROM of user devices for further processing. Therefore, an attacker can steal the keys from the storage medium, then he/she can use for illegal activities. To handle this problem, this work assimilates some enrichments in the Twofish to protect the photos from being divulged to the invader. Hence, this work exploits DES to encipher the supplied to the Twofish algorithm.

The overall structure of the developed unified cryptographic image authentication to protect user images on a cloud platform is shown in figure 1. Our proposed UCIA is applied to securing user photographs in two phases. In the first phase, UCIA generates for the Twofish algorithm by applying DES by supplying a message and a as input. In the following step, the enciphered content from DES (i.e., for Twofish) is employed by the Twofish algorithm for enciphering the user photographs.DES is the most basic chunk cipher developed by IBM, and successively ratified by the National Bureau of Standards.[14] DES receives 64 bits (8 picture elements simultaneously) as an input chunk and achieves an initial permutation. The outcome gained from this preliminary transformation is then divided into two sub blocks. These sub-blocks are finally transformed to get final enciphered message after executing 16 iterations with different keys (48 bits).

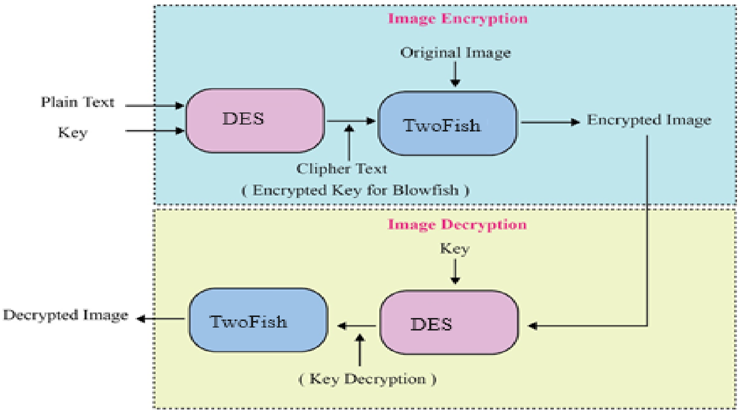

Figure 1. Block diagram of UCIA model

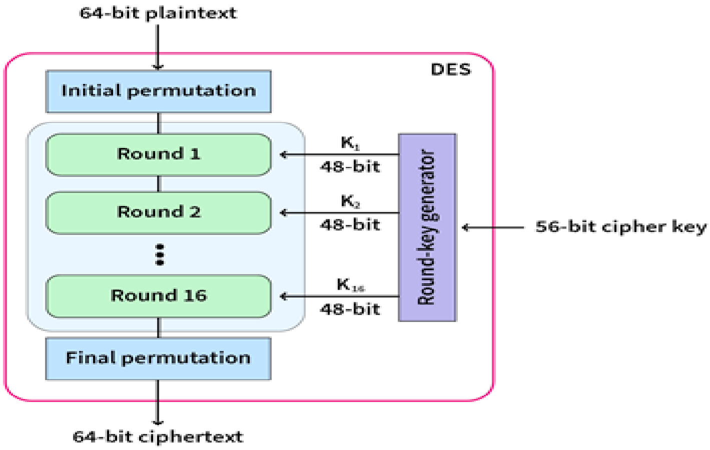

Figure 2. The DES algorithm for creating

The functional unit in DES contains an extensive transformation block (32 - 48 bits), a unit for XO Ring operation and replacement operation (48 - 32 bits), and finally direct transformation box. The initial key dimension is 64 bits where 8 bits are employed for parity error detection operation and the residual 56 bits are calculated using Transformation Choice 1 (TC1). This data block is then divided into two parts and switched multiple times to obtain keys with 56 bits (16 sub keys). From these sub keys, 16 keys (each 48 bits length) are calculated using Transformation Choice 2 (TC2). Deciphering employs the same process as enciphering performs, but with the order of sub keys is inverted.

Twofish is a secret key cryptographic algorithm. With a size of 128-bit chunk and flexible enciphering key length, Twofish is one of the powerful enciphering algorithms. By exploiting its large chunk length, this algorithm is protected from brute-force cyber attacks, as such a cyber attack would need an incredible amount of computational capacity to decipher a 128-bit enciphered message.The Twofish algorithm contains some vital elements including Feistel system, S-boxes, Maximum Distance Separable (MDS) vectors, Pseudo-Hadamard transform (PHT), whitening, and key schedule unit.

The feistel network is the basis of many block ciphers used to transform any operation (f function) into a permutation. S-boxes are responsible for nonlinear replacement functions. This algorithm implements 4 predefined, bijective, key-oriented, 8×8 bit s-boxes. These modules are generally employed in chunk ciphers. The twofish algorithm employs a single 4×4 mds vector over a finite galois field.[28] Using this matrix each byte is transformed into a polynomial. Pht is a rescindable conversion of a bit string that delivers cryptographic dispersion. This algorithm employs a 32 bit pht to blend the results from its two 32 bitsparallel operations. This algorithm performs xor operation with the key value a fore and after the first and last iteration using whitening method. The key allocation unit transforms the key bits into round keys that can be employed by the algorithm for computation.

The enciphering procedure in Twofish algorithms is as follows: (i) two words with the size of 32 bits are given to the F function in each round; (ii) the input is divided into four8-bit strings, which are then transferred using four key-oriented S-boxes; (iii) the MDS syndicates the four result strings into a word with a size of 32-bit; (iv) the PHT functional module is used to combine two words; and (v)two round sub keys are formed using the results obtained from PHT module and it is XORed with the right half.

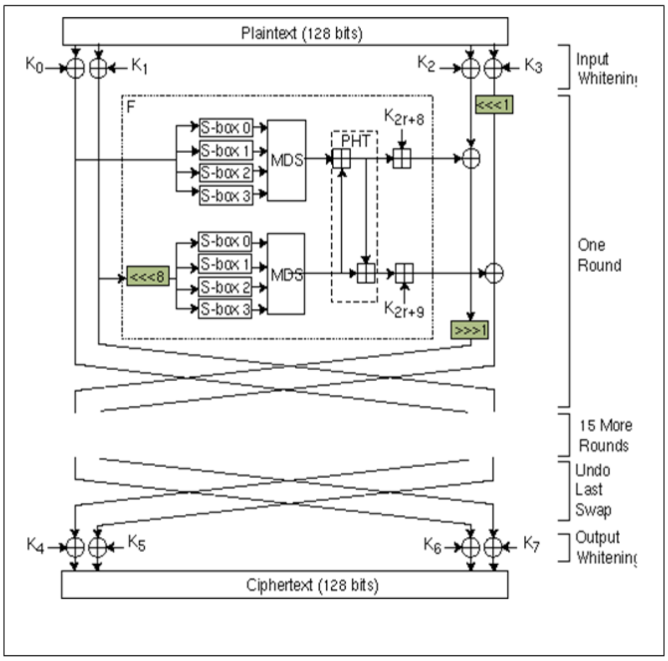

Figure 3. The Twofish algorithm for image security

RESULT AND DISCUSSION

Our UCIA encryption model is implemented through JAVA programming in the Net Beans IDE 8,2 platform. This work exploits Java crypto and safety packages to carry out experiments. These tools deliver security infrastructure attributes such as authorization and authentication, key generation and management, encryption, and decryption. The user pictures of different sizes are used as input. The enciphered picture information is stored as a file and it is delivered for deciphering process. Both enciphering and deciphering procedures are studied and assessed using the evaluation indicators including the timing overhead for storage, encryption, decryption, and throughput.

- Cloud storage overhead: The overall temporal overhead to upload and download pictures in a cloud database.
- Encryption overhead: The overhead due to enciphering any image before uploading.
- Decryption overhead: The overhead is due to decrypting any image before downloading.
- Throughput: It is defined as the ratio between input sizes to encryption overhead. It specifies the performance of the enciphering process. As the throughput is improved, the power dissipation of this enciphering method is reduced.

A comparative analysis with existing image enciphering techniques including Twofish,(10) DES,(16) TDES,(17) and AES(18) algorithms will prove the performance and reliability of our UCIA approach with respect to evaluation measures.

The enciphering procedure in Twofish algorithms is as follows: (i) two words with the size of 32 bits are given to the F function in each round; (ii) the input is divided into four8-bit strings, which are then transferred using four key-oriented S-boxes; (iii) the MDS syndicates the four result strings into a word with a size of 32-bit; (iv) the PHT functional module is used to combine two words; and (v)two round sub keys are formed using the results obtained from PHT module and it is XO Red with the right half.

The temporal overheads of cloud storage for different dimensions of JPG pictures are given in table 1. The study considers approximately 2,2Mb/s data rate for uploading and 7,3Mb/s downloading rate. Figure 6 shows the effectiveness of image-enciphering algorithms considered in this study with respect to timing overhead to store the picture in the cloud (i.e., computational overhead) for various dimensions of the picture. The empirical outcomes exhibit the dominance of DES-Twofish integration over other algorithms regarding the computational overhead.

Figure 5 shows the performance of UCIA approach regarding minimum storage overhead. From this figure, it can be witnessed that the computational overhead of the UCIA model was much reduced than all other algorithms.

Therefore, the amalgamation of DES and the Twofish model delivers much more reliable outcomes for protecting user photographs than the other algorithms. More precisely, the cohesive DES-Twofish not only increases the enactment of the enciphering part of the algorithm but also delivers better outcomes for storage. This evaluation proves that the cohesive DES-Twofish is a very optimal choice to protect images stored in a cloud environment.

(c) Original image

(b) Encrypted image

(a) Decrypted image

Figure 4. Image enciphering/deciphering using the UCIA algorithm

Table 1. Timing overhead of different algorithms for cloud storage

Image Size	Cloud storage overhead (second)				
	UCIA	TWOFISH	DES	TDES	AES
8 KB	0,470	0,475	0,731	1,470	1,356
40KB	1,045	0,731	1,356	1,470	1,157
100 KB	1,157	1,073	1,889	2,093	1,330
400 KB	2,091	3,033	3,382	3,468	3,229
652 KB	2,724	3,506	3,521	3,695	3,494
1 MB	3,065	4,310	5,224	5,381	4,436
11 MB	5,232	5,660	9,764	9,858	5,766
144 MB	6,046	6,740	9,173	10,037	7,374

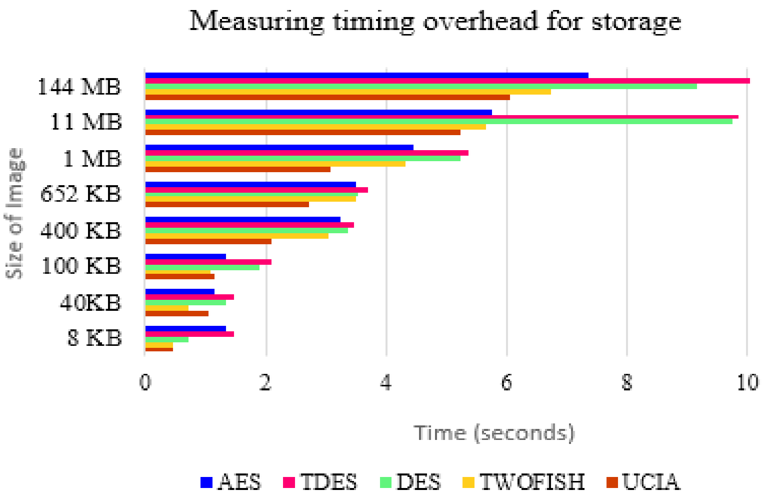

Figure 5. Timing overhead for cloud storage

Table 2 and figure 6 demonstrate the enciphering overhead of all algorithms for input photographs with various dimensions. It can be observed that the evaluation metrics measured by a cohesive DES-Twofish algorithm are better related to all other algorithms. Consequently, the outcomes indicate that the combination of DES and Twofish provides improved outcomes (i.e., minimum overhead) related to the basic DES, Twofish, and all other cryptographic methods considered in this study. Furthermore, it is noteworthy that integrated DES-Twofish shows improved results than DES and Twofish in almost all of the cases. This reveals that the combination of DES and Twofish has considerably improved the enactment of the picture-enciphering process.

Figure 7 and table 3 show the deciphering overhead of all algorithms for diverse sizes of user photographs. It can be observed that the evaluation metrics gained by the cohesive DES-Twofish algorithm are greater than all other algorithms. Therefore, the outcomes display that the amalgamation of DES and Twofish has achieved minimum overhead related to the original DES, Twofish, and all other methods employed for comparison. Besides, it is evident that cohesive UCIA using the integration of the DES and Twofish algorithms provides reduced overhead as compared to AES, DES, TDES, and Twofish algorithms in all the trials. This proves the effectiveness of the proposed UCIA approach in image security.

Table 2. Timing overhead of different algorithms for the encryption process

Image Size	Encryption overhead (second)				
	UCIA	TWOFISH	DES	TDES	AES
8 KB	0,049	0,289	0,480	0,702	0,977
40KB	0,453	0,575	0,555	1,118	1,139
100 KB	1,037	1,586	1,916	1,952	2,164
400 KB	1,316	1,867	1,885	2,075	2,119
652 KB	1,842	2,254	2,428	2,437	2,899
1 MB	2,911	3,289	3,950	4,925	5,754
11 MB	3,283	4,216	4,615	5,742	5,816
144 MB	3,923	4,266	5,767	6,578	6,915

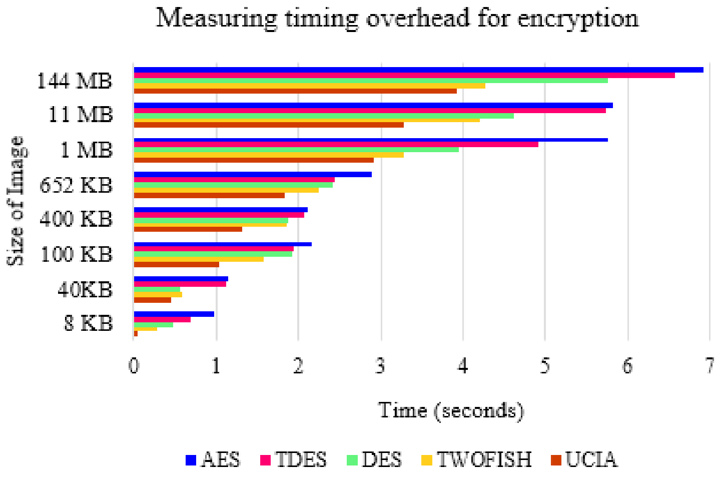

Figure 6. Timing overhead for the encryption process

Table 3. The overhead of the decryption process

Image Size	Decryption overhead (second)				
	UCIA	TWOFISH	DES	TDES	AES
8 KB	0,041	0,275	0,317	0,328	0,336
40KB	0,254	0,365	0,387	0,770	0,361
100 KB	0,559	0,752	0,953	1,006	1,197
400 KB	0,882	0,852	1,161	1,284	1,354
652 KB	0,638	1,254	1,672	1,930	2,626
1 MB	0,923	1,617	1,852	3,408	3,408
11 MB	1,264	2,017	2,431	2,721	3,518
144 MB	0,525	2,027	2,502	3,212	3,760

The enciphering throughput obtained by each algorithm is listed in figure 8 and table 4. It is found that the cohesive DES-Twofish enciphering algorithm outperforms other existing approaches regarding the enciphering throughput. This is because the DES-based enciphering can improve the performance Twofish enciphering process.

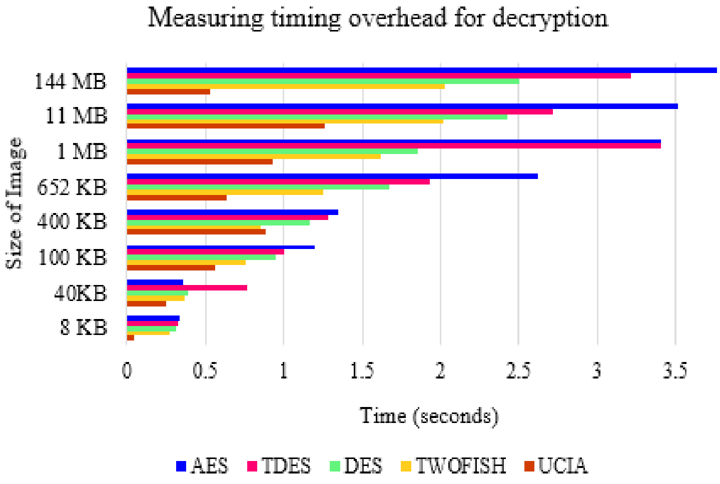

Figure 7. The overhead of decryption process

Table 4. Encryption throughput

Image Size	**Encryption throughput**				
	UCIA	**TWOFISH**	**DES**	**TDES**	**AES**
8 KB	0,163	0,170	0,602	0,684	0,719
40KB	0,353	0,788	1,036	0,496	0,982
100 KB	0,364	0,654	0,828	0,982	0,902
400 KB	0,371	0,705	0,990	0,908	0,979
652 KB	0,354	0,817	0,928	0,996	0,841
1 MB	0,343	0,885	0,833	0,802	0,856
11 MB	3,351	0,779	0,914	0,804	0,987
144 MB	6,707	0,920	0,740	0,877	0,951

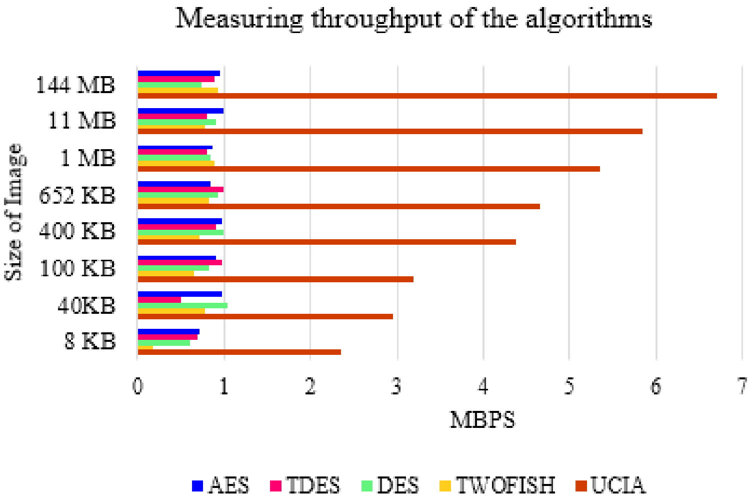

Figure 8. Encryption throughput

CONCLUSION

At present, cloud technology is drawing more attention from researchers and industries owing to its adaptable nature, designing applications across platforms, making forecasts by processing streaming multimedia and analytic data, etc. These characteristics make it an optimum solution for organizations that rely on depends on data analytics. Despite the general popularity on the theme across the digital world, securing user data kept in the cloud database is the most decisive problem. Since the cloud customer who has kept their images has no control over their data the cloud service provider has to ensure better security against cyber threats.

Cryptography algorithms are the best choice to secure pictorial data in the cloud. These techniques transform images into an inarticulate form to keep security and privacy over undependable and vulnerable social media. In this paper, we aim to propose an approach for improving image security on the cloud using encryption algorithms. This work develops a cohesive approach, called UCIA to protect user images on a cloud platform. The proposed approach includes two phases. In the first phase, UCIA engenders a secret key through a DES by providing a message and a key as input. In the second phase, UCIA implements the Twofish algorithm to encipher the pictures by applying cipher text. The enciphered picture data is then stored in the cloud database and can be recovered when the customer requests it. The effectiveness of both enciphering and deciphering procedures are analyzed using the evaluation metrics including time for enciphering, deciphering, cloud storage, and enciphering throughput. Experimental results reveal the better performance and strength of the UCIA approach.

REFERENCE

1. Markets and Markets. Cloud Computing Market (November 2022). Available online: https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

2. Yenugula M, Goswami SS, Kaliappan S, Saravanakumar R, Alasiry A, Marzougui M, AlMohimeed A, Elaraby A. Analyzing the Critical Parameters for Implementing Sustainable AI Cloud System in an IT Industry Using AHP-ISM-MICMAC Integrated Hybrid MCDM Model. Mathematics. 2023; 11(15):3367

3. Gartner. Accelerating Shift to the Cloud Means the Market Opportunity for Providers is Narrowing (February, 2022). Available online: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

4. Chauhan M, Shiaeles S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network. 2023; 3(3):422-450.

5. Chang Y-F, Tai W-L, Huang Y-T. Privacy-Preserved Image Protection Supporting Different Access Rights. Applied Sciences. 2022; 12(23):12335.

6. Ngnie Sighom JR, Zhang P, You L. Security Enhancement for Data Migration in the Cloud. Future Internet. 2017; 9(3):23.

7. Manikandan, S, Chinnadurai, M, “Effective Energy Adaptive and Consumption in Wireless Sensor Network Using Distributed Source Coding and Sampling Techniques”,. Wireless Personal Communication (2021), 118, 1393–1404 (2021)

8. Berisha B, Mëziu E, Shabani I. Big data analytics in Cloud computing: an overview. J Cloud Comput (Heidelb). 2022;11(1):24.

9. Molas G, Nowak E. Advances in Emerging Memory Technologies: From Data Storage to Artificial Intelligence. Applied Sciences. 2021; 11(23):11254.

10. T. U. Haq, T. Shah, G. F. Siddiqui, M. Z. Iqbal, I. A. Hameed and H. Jamil, “Improved Twofish Algorithm: A Digital Image Enciphering Application,” in IEEE Access, vol. 9, pp. 76518-76530, 2021,

11. Quenaya, MR, Villa-Herrera, AA, Chambi Ytusaca, SF, Yauri Ituccayasi, JE, Velazco-Paredes, Y, Flores-Quispe, R “Image Encryption using an Image Pattern based on Advanced Encryption Standard,” 2021 IEEE Colombian Conference on Communications and Computing (COLCOM), Cali, Colombia, 2021, pp. 1-6

12. Ashwaq T. Hashim and Ammar H. Jassem and Suhad A. Ali, A Novel Design of Blowfish Algorithm for Image Security, Journal of Physics: Conference Series, 2021, vol. 1818, no. 1, pp. 012085

13. Adeniyi AE, Misra S, Daniel E, Bokolo A Jr. Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data. Algorithms. 2022; 15(10):373.

14. S. Manikandan, K. Raju, R. Lavanya, R.Hemavathi, “Energy Efficiency Controls on Minimizing Cost with Response Time and Guarantee Using EGC Algorithm”,International Journal of Information Technology Insights & Transformations, Vol. 3, No. 1, 2017

15. Matthews, R. (1989). On the derivation of a Chaotic encryption algorithm. Cryptologia, 14, 29–42.

16. A. Bastanta, R. Nuryansyah, C. A. Nugroho and W. Budiharto, "Image Data Encryption Using DES Method," 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI), Jakarta, Indonesia, 2021, pp. 130-135

17. Peram, SR, Vardhan,GH,Neeraj, M, Anand Kumar, B, Analysis of image security by triple DES,Materials Today: Proceedings, Volume 64, Part 1,2022, Pages 808-813

18. Lin C-H, Hu G-H, Chan C-Y, Yan J-J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm. Applied Sciences. 2021; 11(3):1329

FINANCING

There is no funding for this work.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.

Research: R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.

Methodology: R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.

Project management: R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.

Original drafting-drafting R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.

Writing-revising and editing: R. Manivannan, G. Venkateshwaran, D. Menaga, S. Sivakumar, M. Hema Kumar, Minu Susan Jacob.