Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 135-149
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Implementation of a Hybrid Triple-Data Encryption Standard and Blowfish Algorithms for Enhancing Image Security in Cloud Environment

Mohan Nagamunthala, Ramakrishnan Manjula

School of Computer Science and Engineering, VIT University, Vellore, India
Email: mohan.nihar1@gmail.com, rmanjula@vit.ac.in

How to cite this paper: Nagamunthala, M. and Manjula, R. (2023) Implementation of a Hybrid Triple-Data Encryption Standard and Blowfish Algorithms for Enhancing Image Security in Cloud Environment. *Journal of Computer and Communications*, **11**, 135-149.
https://doi.org/10.4236/jcc.2023.1110009

Received: May 2, 2023
Accepted: October 29, 2023
Published: November 1, 2023

Abstract

In recent years, technological advancements have provided the world with cloud computing which can transfer, store, and process huge data chunks in the form of video, audio, images, and text efficiently. In spite of the universal hype on the subject across the information technology world, protecting sensitive data stored in the cloud server is one of the crucial problems. The large volume and sophistication of cyberattacks conclude to the fact that private pictures need exceptional care than other forms of data on the cloud. Since the user who has stored their private pictures in the cloud has no control over the privacy protection of data, the cloud vendors have to assure a greater level of security in terms of authentication and prevention from cyberattacks. Image encryption algorithms secure visual data by transmuting pictures into an unintelligible form to preserve the confidentiality of pictures over reliable unrestricted social media. This work aims to develop a method for enhancing the security of user photographs on a cloud platform by means of cryptography algorithms. The proposed hybrid technique presents the idea of protecting images in two straightforward steps. First, we generate a chipper text (*i.e.*, secret key) using Triple Data Encryption Standard (TDES) by giving a plaintext and a key as input. Then, the cipher text obtained from TDES is given to the Blowfish algorithm for encrypting the user images. The encrypted image is then uploaded to the database of the cloud server and can be retrieved whenever the user requests it. Both image encryption and decryption processes are analyzed and evaluated based on performance metrics such as cloud storage time, encryption time, decryption time, and encryption throughput. A comparative study with conventional image encryption methods will demonstrate the effectiveness and robustness of our proposed method.

Keywords

Cloud Computing, Image Encryption

1. Introduction

Cloud computing is the hottest trend and an ongoing research topic in the domain of information technology. It is an Internet-based blooming technology that provides abundant services to its customers on demand. Of late, it has gained a lot of attention of researchers from different fields. Albeit cloud computing is barely a decade old, it has influenced the computing industry like no other technology. As stated by Forrester (an American market research company that provides guidance on the prevailing and potential effect of technology to its consumers and the society) in 2010, the cloud computing industry will magnify from a $40.7 billion industry in 2010 to a $241 billion industry in 2020. Google Compute Engine, Microsoft Azure, 10 gen, etc. are the most renowned cloud service vendors [1].

With the hasty progress in cloud computing, a large number of organizations and individuals are encouraged to upload and process their data on clouds. For example, Apple customers store their personal photographs on iCloud in order to save storage space on their local devices [2]. Baidu Cloud enables its customers to upload and download their personal data to the Baidu Wangpan, and the records can be synchronized automatically on manifold internet-connected user terminals. Most of the cloud vendors deliver vast computational resources at lower prices, which entice customers to outsource their substantial computational tasks (e.g., the training of deep convolutional neural networks).

Even though cloud technology offers tremendous benefits and vast openings, it does come with a bundle of security issues as it involves many technologies such as databases, networks, virtualization, operating systems, transaction management, resource scheduling, concurrency control, memory management, load balancing, etc. Moreover, the outsourcing of data storage and processing fetches several complicated security threats in the cloud environment. The cloud servers are vulnerable to severe cyberattacks and security breaches from time to time. For instance, iCloud was hacked in 2014, and personal images of more than 100 celebrities were released online [3]. Moreover, the cloud vendor can never be completely trusted since they may also be interested in user information. Therefore, the retention of data in a cloud environment needs a more secured approach for data storage with minimum computational overhead. It is noteworthy that the accessibility and availability of this information to prospective authorized users have to be made easy.

With the inducement of communication technologies, multimedia was utilized literally in each ounce of information of all the applications developed on the internet including cloud computing. Providing security to such a data element is a crucial and difficult endeavor. Images are the most commonly used modes of communication in almost all fields such as research, medical, or business. According to Business Insider, around 1.2 trillion pictures will be captured this year which is a lot to be processed and managed. The intelligent systems discharging their burden by outsourcing data continuously is not a big deal, but their security is a major apprehension and particularly that of images. Personal pictures are quite sensitive information to customers, and therefore should be protected before being stored on the cloud servers.

Although sending pictures is a widespread online activity, the majority of the networks through which the image's transfer is mostly insecure and data security is very low. Therefore, the unauthorized access of photographs is very common, and usually, people do not think much before transferring their pictures [4].

In the term of cloud security, technologists from all over the world have developed and implemented plethora and practical solutions to resolve different security issues in the cloud. A simple and direct way to secure valuable information from espionage is to encrypt it with strong cryptographic techniques. Nevertheless, in such a way the utilization of the stored data would be strongly restricted together with the services provided to users. Numerous methods have been developed to protect crucial data from attacks including Data Encryption Standard (DES), Advanced Encryption Standard (AES) [5], Blowfish algorithm [6], Two-fish algorithm [7], and so on. Even though many algorithms for securing data in the cloud have been proposed that in securing images from espionage are very few [8] [9] [10]. But even with the existence of such techniques, we have not reached a par where a protected communication for the image could exist.

Encryption can complicate the authentication process considerably if it is not correctly implemented. For example, an organization may want to retrieve beneficial information from its massive database in the cloud. But the data on the cloud could be stored in encoded form for commercial requirements, hence hindering its effective utilization. To enable a person unaware of the decryption key to process the encrypted data, several methods have been proposed including hybrid cryptographic encryption, secure multiparty computation, order-preserving encryption, homomorphic encryption, etc.

In this work, we implement an effective hybrid cryptographic method for image encryption over a cloud platform. We implement the Blowfish algorithm for encrypting JPG format images. Blowfish algorithm is appropriate for cloud image security because of its high speed and greater security level. No one had been able to create an attack that could break the Blowfish [11]. But Blowfish will provide the best performance when the key does not vary recurrently. As the result, the sub keys of the Blowfish algorithm are stored in FLASH PROM or EEPROM of the user terminal for further use. Therefore, if an attacker would be able to steal the subkeys from the memory, then he/she could derive the key without any difficulty. In order to resolve this issue, we have combined TDES with the Blowfish algorithm to secure the user image from being unveiled. Our contribution is three-fold:

- We develop a hybrid cryptography technique for improving image security by integrating TDES and Blowfish algorithms.
- We use the Blowfish algorithm to encrypt the image in the user's database. To improve the performance of the Blowfish algorithm, TDES is employed to generate e secret key for encryption.
- We implement the proposed technique using java language in NetBeans IDE 8.2 environment. The experimental results are analyzed and evaluated.

The remainder section of the article is arranged as follows: In Section 2, the security issues in the cloud computing environment are discussed. In Section 3, a summary of previous research related to this work is presented. In Section 4, we discuss the proposed system in detail. In Section 5, results and discussions are presented. We conclude this study in Section 6.

2. Security Issues in Cloud Computing Architecture

There is much hype around cloud computing. Cloud is a collection of servers, computers, and various computing elements. A cloud server (*i.e.*, data center) is fabricated with numerous processing elements, network topologies, switches, storage nodes, and front end to send replies to the received queries [12]. Based on the type of service consumption model used by the customers, clouds are classified as public, private, community, and hybrid. In a public cloud environment, the client company needs not to worry about cloud hosting, administration as well as maintenance and it belongs to the designated cloud vendor. All users share the common infrastructure pool with limited configuration, accessibility variances, and security protections. One of the benefits of a public cloud is that they facilitate scaling seamlessly on demand.

Private clouds are provided by a specific company or their dedicated services. It enables a single-tenant working environment with all the reimbursements, flexible functionalities, and utility/accountability model of the cloud. The private clouds target to resolve the data security and privacy issues and provide superior control, which is naturally absent in a public cloud. The community cloud is shared by many companies having common domain and functionalities. Hybrid cloud, as the name implies, is the combination of two or more public and private clouds that enable transitive information exchange and possibly application compatibility and portability across different service vendors exploiting proprietary or standard methods irrespective of location or ownership. With a hybrid cloud, vendors can use third-party cloud providers in a complete or partial manner, thus improving the flexibility of computing. This model is able to provide on-demand, externally provisioned scale.

Conceptually, the structure of cloud service is classified into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

- SaaS: It provides renting application functionality from a cloud vendor instead of buying, installing, and executing software by the customer. This service executes a list of programs on the cloud server, and it is usually billed to the user according to its utilization [13]. This service can also be accessed by several customers anywhere using the applications available on the network.

- PaaS: This service provides a platform in the cloud, whereupon applications can be developed and deployed. It acts as a database and operating system on the cloud platform [14]. The customer need not pay for this service separately.
- IaaS: Using this service, cloud vendors offer computing resources and storage space on demand. It enables the customers to utilize all the other software services regardless of the type of devices employed [13].

There are six precise areas of the cloud platform where devices and software need extensive security consideration [15]. They are: 1) Protect data at rest, 2) Protect data in transit, 3) Authentication of users/processes/applications 4) Strong isolation between data belonging to different users, 5) Cloud legal and regulatory issues, and 6) Event response. For protecting data at rest, cryptographic encryption techniques are definitely the optimal choice. For example, the hard drive builders are now shipping self-encrypting drives that follow trusted storage standards of the trusted computing group [15]. These self-encrypting drives embed encryption hardware into the drive, enabling automated encryption with minimum performance impact or cost. Even though software encryption can also be employed for securing data, it makes the process less secure and slower since it may be possible for hackers to steal the key without being recognized.

Encryption is the best method for protecting data in transit as well. Furthermore, authentication and integrity protection methods guarantee that data is received by the intended destination and it is not altered in transit. Strong authentication is a compulsory prerequisite for any cloud implementation. Authentication is the foundation for access control. User authentication and access control are more imperative than ever since the cloud and all of its data are reachable to everyone over the Internet. The trusted computing group's standard enables real-time interaction between the user and a cloud vendor about authorized users and other security issues. Whenever an access privilege of a particular customer is reassigned or revoked, the customer's identity management system can inform the vendor in real-time so that the user's privilege can be changed or revoked immediately. One of the more obvious issues in the cloud is isolation among its users (who may be hackers or competing companies) to evade unintentional or deliberate access to sensitive information.

Generally, a cloud vendor would exploit a hypervisor and virtual machines to isolate users. At present, several techniques are available to deliver noteworthy security enhancements in virtual machines and virtual network separation. Furthermore, the trusted platform component can offer hardware-based authentication of the hypervisor and virtual machines integrity and thus assure robust network security. Legal and regulatory issues are significant in a cloud platform that has security consequences. To confirm that a vendor has robust practices and policies that address regulatory and legal issues, every user must have the authorities to examine the vendor's practices and policies to ensure their competence. In the case of data deletion and retention, trusted storage, and trusted platform module access methods can act as a major role in limiting access to critical and sensitive information. As part of expecting the unexpected, users need to plan for the likelihood of vendor security breaches or customer misbehavior. An automated response at least computerized warning is the best solution for this purpose.

3. Related Work

This section provides a comprehensive description of various existing methods used for image encryption in the cloud platform. To make image transmission more secure in this booming era of the internet, several researchers have positively implemented several encryption algorithms to avert image transmissions from espionage in the past decade. Zhang and Ding developed an image encryption method based on the Advanced Encryption Standard (AES) algorithm to encrypt and decrypt digital photographs using MATLAB [16]. Initially, the proposed technique converts the pictures into a binary matrix to process it using the AES algorithm. Then, it obtains a gray values matrix of a picture. This matrix is split into a matrix with each unit of 8 bits. Now, each matrix will be encrypted by means of the AES algorithm. All new matrix will be combined to get the encrypted matrix. The results revealed that this AES is sensitive to plaintext even when using a decryption key with a single bit alteration because it will generate an incorrect image in the decryption process.

Pia and Karamjeet implemented image encryption and decryption technique using a 64-bits secret-key block cipher. It is known as Blowfish and developed to improve the performance as well as the level of security [17]. This algorithm uses a variable key with a length of up to 448 bits. It uses a Feistel register which iterates a simple function 16 times. The Blowfish algorithm provides security against hacking and runs faster than other conventional algorithms. Nadeem and Javed carried out performance analysis on various secret key algorithms including DES, 3DES, AES, and Blowfish [18]. These algorithms are deployed, and their performance is analyzed by encrypting input files with different sizes and contents. The results revealed that Blowfish has better performance related to other algorithms. Zefreh *et al.* proposed an image security system using recursive cellular automata substitution and its parallelization. This method employs dynamic keys to generate the encrypted output from the original image. This technique has been effectively used in different technical problems and systems [19]. Several attempts and research works are going on for image protection on cloud computing. Many of these systems with the application of image processing have other uses such as face recognition [20], feature extraction [21], smart campus [22]. Image security using watermarking technology is widely used, where data are overlapped with the contents of digital multimedia [23]. Even though many algorithms for securing images in the cloud have been proposed, we have not reached a par where a protected communication for images could exist.

4. Proposed System

The proposed research work is based on converting images into a non-comprehensible form using a hybrid TDES—Blowfish algorithm. Customers who intended to store and process their image in the cloud can employ this technique to encrypt their image before outsourcing it to the commercial cloud. Cloud customer is the owner of the data that is supposed to be transmitted to the cloud. A key is required for encrypting the image. As stated in the previous sections, Blowfish is an appropriate algorithm for image encryption in the cloud environment. However, it will achieve maximum performance when the key does not differ recurrently. Usually, the encryption key given to the Blowfish algorithm is stored in FLASH PROM or EEPROM of the user's terminal for further use. Hence, an invader would be able to steal the keys from the memory, then he/she could generate the key without any difficulty. In order to resolve this issue, we have incorporated some enhancements in the Blowfish algorithm to secure the image from being disclosed to the unauthorized user. For this purpose, we use TDES to encrypt the key given to the Blowfish algorithm.

The proposed system consists of three components: the data owner, the cloud data center, and authorized users. The data owner first generates a secret key for the Blowfish algorithm using the TDES algorithm. Then, each image in his/her database is encrypted by Blowfish by applying a secret key obtained from TDES. The encrypted images are sent to a cloud server for secure storage and accessed whenever the user requests it. Besides, all authorized users can receive secret keys from the data owner via a secure communication protocol (e.g., HTTPS). Subsequently, the authorized user can decrypt the image by applying the secret key. Encrypted images would be mined by the unauthorized users but the key remains unidentified to the invader (*i.e.*, unauthorized user). It is noteworthy that the key distribution is a separate issue and out of the scope of this article.

The proposed hybrid algorithm is implemented for protecting images in two steps: 1) we generate a secret key for the Blowfish algorithm using TDES by giving a plaintext and a key as input; 2) the ciphertext from TDES (*i.e.*, a secret key for blowfish) is used by Blowfish algorithm for encrypting the user images. **Figure 1** shows the block diagram of the proposed system.

Triple data encryption standard is a symmetric-key block cipher. It uses the Data Encryption Standard (DES) algorithm thrice for all in key generation, encryption, and decryption processes. DES is one of the most primitive block ciphers proposed by IBM in the year 1970 and subsequently approved by the National Bureau of Standards [24] [25]. It accepts 64 bits (8 pixels at a time) as an input block and performs Initial Permutation (IP). The result obtained from this initial permutation is then split into two sub-blocks (Li, Ri). These sub-blocks after performing 16 rounds of operations with diverse keys (48 bits) are finally permuted to achieve final encrypted text.

The function block in DES is an integration of Expansion permutation (32 - 48 bits), XORing function followed by substitution (48 - 32 bits), and final direct

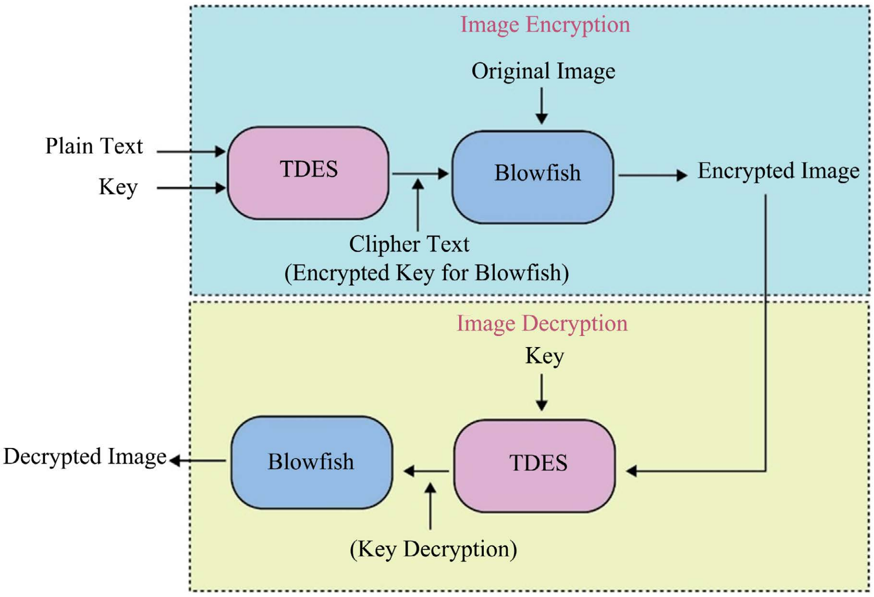

Figure 1. Block diagram representation of the proposed system.

permutation box. The original key size is 64 bits, out of which 8 bits are used for parity checks. The remaining 56 bits are obtained by applying permuted choice 1 (PC1). This block of data (56 bits) is then split into two sections and rotated several times to get 56 bits keys (16 sub keys). From these 56 bits sub keys, 16 keys (48 bits keys) are obtained by applying permuted choice 2 (PC2). Decryption follows the same procedure as encryption does, but with the order of sub keys is reversed.

TDES employs three 56-bit keys for image encryption and decryption [26]. The method of selection of these keys is called the keying option (KO). The TDES offers three keying options as given below:

- KO 1: All three keys are independent of each other. It is the most consistent keying option and is not susceptible to any recognized real-world attacks.
- KO 2: Key 1 and Key 2 are independent, while Key 3 is similar to Key1. It is resilient against meet-in-the-middle attacks but is susceptible to attacks such as chosen plaintext. It is also called 2DES.
- KO 3: All three keys are identical. It the weakest keying option.

Irrespective of the KO, the encryption process of TDES employs Key 1 for encryption Key 2 for decryption, and Key 3 for encryption again. Correspondingly, the decryption processes employ the respective keys to decrypt, encrypt, and decrypt the data. The ciphertext obtained from the TDES is used as a key in Blowfish to encrypt the user image.

Blowfish is also a symmetric-key block cipher algorithm. Its key element is a Feistel register, iterating 16 times [27]. The length of the block is the same as used in the DES algorithm (64 bits). Nevertheless, contrasting DES, it employs a variable key size of 32 - 448 bits. These sub-blocks send through 16 rounds of operation using S box, adder, and bitwise XOR operations of the Feistel network.

The output of each round is an input to the next round. To end, the right and left sub-blocks are XORed with the key values (P-array generator 17 and 18) and concatenated to get the resultant cipher text.

Blowfish algorithm employs comparatively large keys. P-array consists of 18 keys (32-bits each) and four S boxes, each with 256 entries initialized to random values. The next step is to XOR P-array with the key bits, for instance, P1 XOR (first 32 bits of the key), P2 XOR (second 32 bits of the key). In this fashion, all zero strings are encrypted. This resultant output is now P1 and P2. This P1 and P2 are not encrypted with the modified sub keys to get P3 and P4. The process is repeated to get all keys. In spite of having an intricate initialization, there is effective encryption of the given image. The encrypted images are analyzed visually to find if any information can be extracted by looking at the encrypted images.

5. Result and Discussion

The proposed image encryption system is realized using JAVA language in NetBeans IDE 8.2 environment. We used java safety and java crypto packages to conduct experimentation. These packages offer security features including authentication and authorization, key generation, encryption, decryption, and key management infrastructure features. The input images of various sizes employed in this work are between 8 KB to 144 MB. The encrypted image is saved as a file, which in turn is input for decryption. Both image encryption and decryption processes are analyzed and evaluated based on performance metrics such as cloud storage time, encryption time, decryption time, and encryption throughput.

- Total processing time: The total time to store and retrieve the image in the cloud platform.
- Encryption Time: It is the time taken by the server to encrypt any image.
- Decryption time: It is the time taken by the server to decrypt the encrypted image.
- Encryption throughput: It is the ratio of the size of the input file (MB) to encryption time (seconds). It indicates the speed of encryption. As the throughput value is increased, the power consumption of this encryption technique is decreased.

A comparative study with conventional image encryption methods such as DES [28], AES [29], TDES [28], and Blowfish [29] algorithms will demonstrate the effectiveness and robustness of our proposed hybrid TDES—Blowfish method in terms of performance metrics (**Figure 2**).

Table 1 shows the time of cloud storage in second for various sizes of jpg images with around upload rate 2.2 Mb/s and download rate 7.3 Mb/s. **Figure 3** demonstrate the performance of cryptographic algorithms in terms of time required to upload the image to the cloud (*i.e.*, processing time) for different image size. Results show the superiority of our hybrid TDES-Blowfish algorithm over other algorithms in terms of the processing time.

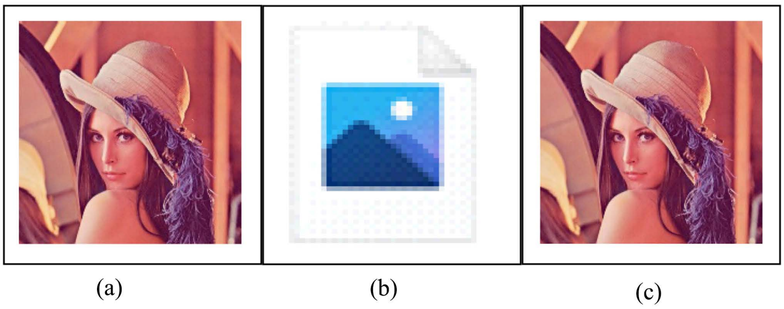

Figure 2. Image encryption/decryption using hybrid TDES—Blowfish algorithm. (a) Original image; (b) Encrypted image; (c) Decrypted image.

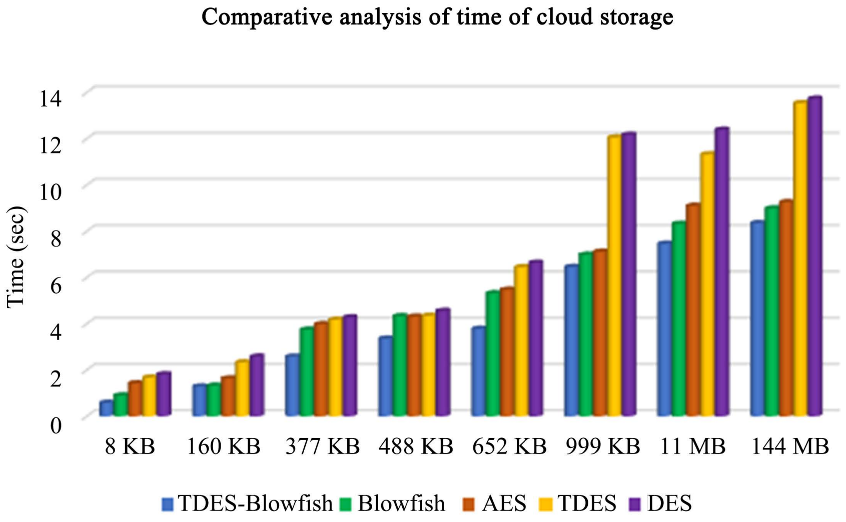

Figure 3. Comparative analysis of time of cloud storage.

Table 1. Comparative analysis of time of cloud storage.

Image Size	Times in Second				
	TDES-Blowfish	Blowfish	AES	TDES	DES
8 KB	1.428	0.587	1.674	0.902	1.815
160 KB	0.587	0.902	1.428	1.674	1.815
377 KB	1.29	1.325	1.642	2.332	2.584
488 KB	2.582	3.744	3.986	4.175	4.281
652 KB	3.363	4.328	4.314	4.347	4.562
999 KB	3.784	5.321	5.476	6.449	6.643
11 MB	6.459	6.988	7.118	12.054	12.17
144 MB	7.464	8.321	9.104	11.325	12.391

From Figure 3, it can be observed that the processing time of the hybrid TDES-Blowfish was much smaller than all other approaches. Consequently, the combination of TDES and Blowfish algorithms provides much more consistent results for securing image than the others. In other words, the hybrid TDES—Blowfish can not only improve the performance of the encryption process but also provide more promising results for cloud storage. The comparative study demonstrates that hybrid TDES-Blowfish is a very competitive approach for cloud image security.

Table 2 and Figure 4 illustrates the encryption time of all approaches for different size of images. It can be found that the performance measures achieved by the hybrid TDES-Blowfish approach are superior to all other approaches. Hence, the results show that the integration of TDES and Blowfish has revealed better results as compared to the original TDES, Blowfish, and all other approaches used in this research work. Moreover, it is worth noting that hybrid TDES—Blowfish exhibits better results as related to AES and DES in almost all of the cases. This demonstrates that the integration of TDES and Blowfish has significantly increased the performance of the image encryption.

Table 3 and Figure 5 illustrates the decryption time of all approaches for different size of images. It can be found that the performance measures achieved by the hybrid TDES-Blowfish approach are superior to all other approaches. Hence, the results show that the integration of TDES and Blowfish has revealed better results as compared to the original TDES, Blowfish, and all other approaches used in this research work. Moreover, it is worth noting that hybrid TDES-Blowfish exhibits better results as related to AES and DES in almost all of the cases. This demonstrates that the integration of TDES and Blowfish has significantly increased the performance of the image decryption.

The encryption throughput gained by each approach is shown in Table 4 and Figure 6. It can be observed that the hybrid TDES-Blowfish encryption technique outdoes all other algorithms in terms of encryption throughput. The main reason behind the superior performance of the proposed technique is that TDES-based encryption can increase the efficiency of the image encryption process.

Table 2. Comparative analysis of encryption time.

Image Size	Times in Second				
	TDES-Blowfish	Blowfish	AES	TDES	DES
8 KB	0.067	0.397	0.659	0.963	1.34
160 KB	0.621	0.789	0.761	1.534	1.563
377 KB	1.422	2.176	2.628	2.678	2.969
488 KB	1.805	2.561	2.586	2.846	2.907
652 KB	2.527	3.092	3.331	3.343	3.976
999 KB	3.993	4.512	5.418	6.756	7.893
11 MB	4.504	5.783	6.331	7.876	7.978
144 MB	5.382	5.852	7.911	9.024	9.486

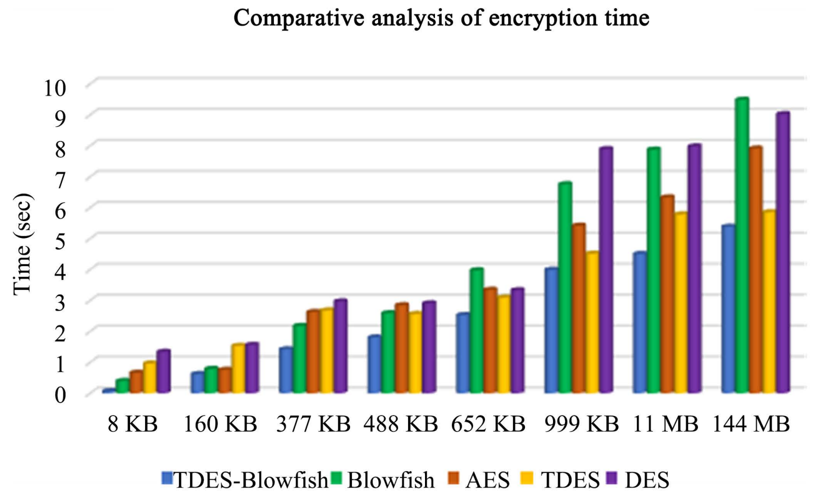

Figure 4. Comparative analysis of encryption time.

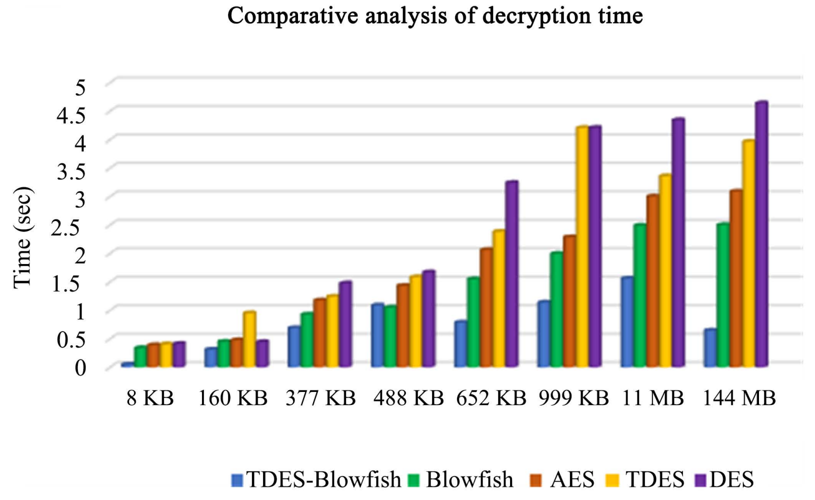

Figure 5. Comparative analysis of decryption time.

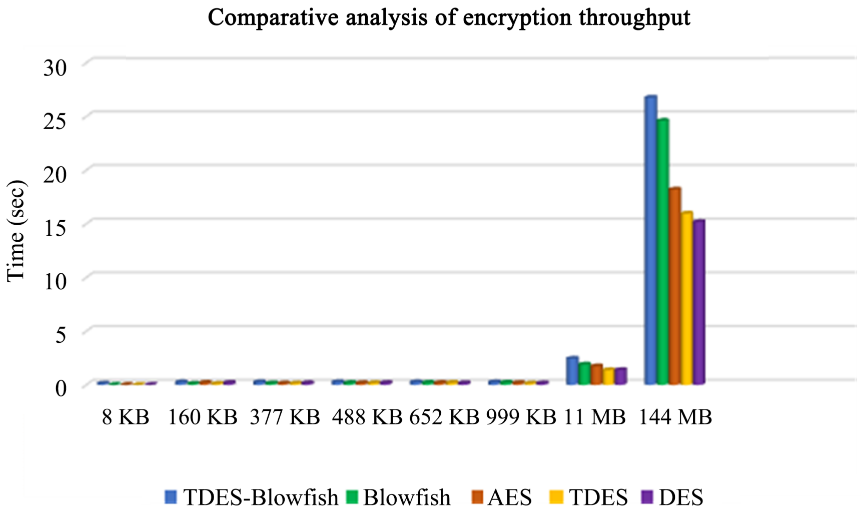

Figure 6. Comparative analysis of encryption throughput.

Table 3. Comparative analysis of decryption time.

Image Size	Times in Second				
	TDES-BLOWFISH	BLOWFISH	AES	TDES	DES
8 KB	0.050	0.339	0.391	0.405	0.415
160 KB	0.313	0.451	0.478	0.951	0.446
377 KB	0.690	0.928	1.177	1.242	1.478
488 KB	1.089	1.052	1.433	1.585	1.671
652 KB	0.788	1.548	2.064	2.383	3.242
999 KB	1.140	1.996	2.286	4.207	4.208
11 MB	1.560	2.490	3.001	3.359	4.343
144 MB	0.648	2.502	3.089	3.965	4.642

Table 4. Comparative analysis of encryption through put.

Image Size	Times in Second				
	TDES-BLOWFISH	BLOWFISH	AES	TDES	DES
8 KB	0.012	0.120	0.008	0.020	0.006
160 KB	0.120	0.008	0.012	0.006	0.02
377 KB	0.258	0.104	0.210	0.102	0.203
488 KB	0.265	0.141	0.143	0.127	0.173
652 KB	0.270	0.191	0.171	0.168	0.189
999 KB	0.258	0.211	0.195	0.196	0.164
11 MB	0.250	0.221	0.184	0.127	0.148
144 MB	2.442	1.902	1.737	1.379	1.397

6. Conclusion

Cloud computing is gaining increasing popularity due to its rich functionality for resource-constrained devices. At the same time, it brings more security issues to solve. In this work, we develop a method for enhancing the security of images on the cloud by means of hybrid cryptography algorithms. The proposed technique presents the idea of protecting images in two straightforward steps. In the first step, we generate a chipper text (*i.e.*, secret key) using Triple Data Encryption Standard (TDES) by giving a plaintext and a key as input. In the second step, the encrypted text obtained from TDES is given to the Blowfish algorithm for encrypting the user images. The encrypted image is then uploaded to the database of the cloud server and can be retrieved whenever the user requests it. Both image encryption and decryption processes are analyzed and evaluated based on the performance metrics such as cloud storage time, encryption time, decryption time, and encryption throughput. A comparative study with conventional image encryption methods will demonstrate the effectiveness and robustness of our proposed method.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Greenwald, G. and MacAskill, E. (2013) NSA Prism Program Taps into User Data of Apple, Google and Others. *Guardian*, **7**, 1-43.

[2] Covert, A. (2012) Google Drive, iCloud, Dropbox and More Compared: What's the Best Cloud Option? http://gizmodo.com/5904739

[3] Kardashian, K. (2014) Apple Admits Celebrity Accounts Hacked But Denies i Cloud Breach. https://www.ft.com/content/916d7d24-327e-11e4-93c6-00144feabdc0

[4] Madhu, B., Holi, G. and Murthy, S.K. (2016) An Overview of Image Security Techniques. *International Journal of Computer Applications*, **154**, 37-46. https://doi.org/10.5120/ijca2016911834

[5] Maraghy, M.E., Hesham, S. and Ghany, M.A.A.E. (2013) Real-time Efficient FPGA Implementation of AES Algorithm. 2013 *IEEE International SOC Conference* (*SOCC*), Erlangen, 4-6 September 2013, 203-208.

[6] Valmik, N.K. and Kshirsagar, V.K. (2014) Blowfish Algorithm. *IOSR Journal of Computer Engineering*, **16**, 80-83. https://doi.org/10.9790/0661-162108083

[7] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N. (1998) TwoFish: A 128-Bit Block Cipher. NIST AES Proposal, Minneapolis.

[8] Chnag, C.C., Hwang, M.S. and Chen, T.S. (2001) A New Encryption Algorithm for Image Cryptosystems. *Journal of Systems and Software*, **58**, 83-91. https://doi.org/10.1016/S0164-1212(01)00029-2

[9] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/S021812749800098X

[10] Guan, Z.H., Huang, F.J. and Guan, W.J. (2005) Chaos-Based Image Encryption Algorithm. *Physics Letters A*, **346**, 153-157. https://doi.org/10.1016/j.physleta.2005.08.006

[11] Meyers, R.K. and Desoky, A.H. (2008) An Implementation of the Blowfish Cryptosystem. 2008 *IEEE International Symposium on Signal Processing and Information Technology*, Sarajevo, 16-19 December 2008, 346-351. https://doi.org/10.1109/ISSPIT.2008.4775664

[12] Varsha, D., Wadhwa, A. and Gupta, S. (2015) Study of Security Issues in Cloud Computing. *International Journal of Computer Science and Mobile Computing*, **4**, 230-234.

[13] Bothe, S., Jadhao, R.M. and Shinde, S. (2012) Cloud Computing-Based Image Processing Applications for Agro Informatics Using 'Self-Learning System' Approach. https://api.semanticscholar.org/CorpusID:173982965

[14] Wang, P., Wang, J., Chen, Y. and Ni, G. (2013) Rapid Processing of Remote Sensing Images Based on Cloud Computing. *Future Generation Computer Systems*, **29**, 1963-1968. https://doi.org/10.1016/j.future.2013.05.002

[15] Trusted Computing Group (TCG)'s White Paper (2010) Cloud Computing and Security—A Natural Match. http://www.trustedcomputinggroup.org

[16] Zhang, Q. and Ding, Q. (2015) Digital Image Encryption Based on Advanced Encryption Standard (AES). 2015 *Fifth International Conference on Instrumentation and Measurement*, *Computer*, *Communication and Control* (*IMCCC*), Qinhuangdao, 18-20 September 2015, 1218-1221. https://doi.org/10.1109/IMCCC.2015.261

[17] Singh, P. and Singh, K. (2013) Image Encryption and Decryption Using Blowfish Algorithm in MATLAB. *International Journal of Scientific & Engineering Research*, **4**, 150-154.

[18] Nadeem, A. and Javed, M.Y. (2005) A Performance Comparison of Data Encryption Algorithms. 2005 *International Conference on Information and Communication Technologies*, Karachi, 27-28 August 2005, 84-89. https://doi.org/10.1109/ICICT.2005.1598556

[19] Zefreh, E.Z., Rajaee, R. and Farivary, M. (2011) Image Security System Using Recursive Cellular Automata Substitution and Its Parallelization. 2011 *CSI International Symposium on Computer Science and Software Engineering* (*CSSE*), Tehran, 15-16 June 2011, 77-86.

[20] Wang, S., Nassar, M., Atallah, M. and Malluhi, Q. (2013) Secure and Private Outsourcing of Shape-Based Feature Extraction. In: Qing, S., Zhou, J. and Liu, D., Eds., *ICICS* 2013: *Information and Communications Security*, Springer, Cham, 90-99. https://doi.org/10.1007/978-3-319-02726-5_7

[21] Rathi, R., Choudhary, M. and Chandra, B. (2012) An Application of Face Recognition System Using Image Processing and Neural Networks. *Journal of Computer Science and Information Technology*, **3**, 45-49.

[22] Xia, Z., Ma, X., Shen, Z., Sun, X., Xiong, N.N. and Jeon, B. (2018) Secure Image LBP Feature Extraction in Cloud-Based Smart Campus. *IEEE Access*, **6**, 30392-30401. https://doi.org/10.1109/ACCESS.2018.2845456

[23] Bhattacharyya, D., Ranjan, R., Alisherov, F. and Choi, M. (2009) Biometric Authentication: A Review. *International Journal of u-Service*, *Science and Technology*, **2**, 13-28.

[24] Matthews, R. (1989) On the Derivation of a "Chaotic" Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[25] Mousa, A. and Hamad, A. (2006) Evaluation of the RC4 Algorithm for Data Encryption. *International Journal of Computer Science & Applications*, **3**, 44-56. http://www.tmrfindia.org/ijcsa/v3i24.pdf

[26] Barker, W.C. and Barker, E. (2012) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. National Institute of Standards and Technology, Gaithersburg.

[27] Schneier, B. (1994) The Blowfish Encryption Algorithm. *Dr. Dobb's Journal*, **19**, 38-40. http://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216

[28] Priyadarshini, P., Prashant, N., Narayan, D.G. and Meena, S.M. (2016) A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, **78**, 617-624. https://doi.org/10.1016/j.procs.2016.02.108

[29] Zhang, Y., Li, X.Q. and Hou, W.G. (2017) A Fast Image Encryption Scheme Based on AES. 2017 2*nd International Conference on Image*, *Vision and Computing*, Chengdu, 2-4 June 2017, 624-628. https://doi.org/10.1109/ICIVC.2017.7984631