ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

An Efficient Scheme of Crypto System with Steganography for Cloud Security Environment

Shouket Ahmad Kouchay

King Saud University

ABSTRACT: The cryptography algorithm with high security and low performance is not satisfactory. The efficiency and Data security is the still concern in cloud computing. Efficient and effective techniques are vital for high-level data security in cloud computing. This paper introduces a technique of cryptography algorithm modified Two fish with steganography to protect data integrity, confidentiality and security in cloud computing. To secure the key information, LSB/DTC steganography method is being used. Key information contains the part of the file being encrypted by the modified Two fish algorithm and key. Data encryption keys are inserted into a cover image using the LSB technique. Stego image (image hidden form) is sent to a valid receiver with the Key. Only the valid receiver can access the data with the key. The proposed technique reveals better, efficient performance results with minimum delay in encryption and decryption process.

KEYWORDS: Steganography, Cloud computing, encryption, decryption, Cryptosystem

I. INTRODUCTION

Cloud Computing has captured a significant part of the virtual world with its productivity and effectiveness. The primary motive anyone chooses cloud computing is to limit the use of resources and lower down the cost. But security and efficiency is the main concern for everyone. The primary motive anyone chooses cloud computing is to limit the use of resources and lower down the cost. Despite being so resourceful, cloud networking has plentiful security issues. One of which is the invasion of the client's private resources by Denial of Service [1].

A most common way to secure a client's resources is using algorithms that fall under cryptography (the craft of solving codes). The term cloud computing came from "on-demand computing" where data is shared over the internet. As cloud computing is based on open network environment security issues arise now and then, mostly concerned with privacy and trust [2]. Thus, it makes important for us to do this research and apply new techniques to prevent security problems. Flooding attacks cause both direct and indirect denial of service (DoS). Usually, when a cloud finds a lot of requests for a particular server, it accounts for additional computing power to that service to handle all the requests. This is the general idea of cloud computing. However, in the real situation, this would provide an advantage to the "hacker". After that, the hacker only needs to focus on his flooding attack on a single server so that he can gain access to cloud account services. This is service is known as direct ' Denial of Service' because the hacker focuses on a particular service to get it down. [3].

Benefits Of Cloud Computing

Cloud computing is not only beneficial for everyday users but also for large originations, as it is capable of sharing large data in different forms. This makes sharing very riskier and makes trusting the client almost impossible.
Cloud Computing has plentiful benefits, some of them are; [4].

- **Low Costs:** Due to less consumption of physical resources, companies can cut their capital intakes and utilize it on operational activities for significant growth.

- **Flexibility:** IT Firms can initiate with the little arrangement and expand as per the requirements.

- **Reliability:** Cloud is more reliable and requires less maintenance, which gives an extra boost to the business.

- **Mobile Accessible:** Cloud services can be accessed from anywhere via smartphone which makes it more convenient and portable.

The cryptographic algorithms such as Symmetric, Asymmetric and Combination key algorithms are used for data encryption and its keys will make the secure cloud network and maintain data privacy. Encryption is the process in which one can encode a message or data into an unreadable format so intruder is not able to read it. The user has plain text when it is encoded into an unreadable format using one of the encryption technique called ciphertext. After received by the correct receiver, he can decrypt it into the original plain text. The purpose of encryption is to attain data confidentiality. [5]

Each of the encryption techniques has its own strong and weak points. To apply a suitable cryptography algorithm to an application, we should knowthe performance, strength, and weakness of the algorithms. While reviewing a scheme we listed the algorithms and techniques used in that scheme and the merit and demerit of that scheme are also specified Symmetric key cryptography algorithms are AES,DES,3DES, IDEA ,BRA, and blowfish. The main issue is to deliver the key to the receiver into a multi-user application. These algorithms require a low delay for data encode decode but provides low security. The public key cryptography algorithm is RSA and ECC algorithm. Public and private keys are manipulated into public-key cryptography algorithms. These algorithms accomplished high-level security but increase delay for data encode and decode.

In [6], the selected encryption algorithms namely DES, AES, and BLOWFISH were used for performance evaluation. Blowfish consumes less memory compared with AES and DES. However, AES showed poor performance results compared to other algorithms.

The RSA algorithm [6] is a typical asymmetric encryption algorithm, which is widely used not only for user data encryption but also as a digital signature. However, considering that the encryption and decryption efficiency of the algorithm is low, it is not suitable for the encryption of large amounts of data.
In [7] the author introduced a modified approach for Blowfish Algorithm

The Two fish algorithm approach is the replacement of the Blowfish algorithm based on AES framework standards. It is pre-calculated and has more speed than AES. The main length can be 128 bits, 192 bits, also 256 bits. No feeble keys exist in Twofish encryption. It is also extremely adaptable in the model which can easily be put to usage as a portion of an extensive variety of applications while working at a protuberant speed.Twofish has, 128-bit plain-text (divided into four parts of 32-bit each) is given for the input whitening where it is XOR-ed with four keys then function g PHT which are explained under the heading Twofish functions and modules. Twofish cryptographic architecture is shown in figure 1.[8].

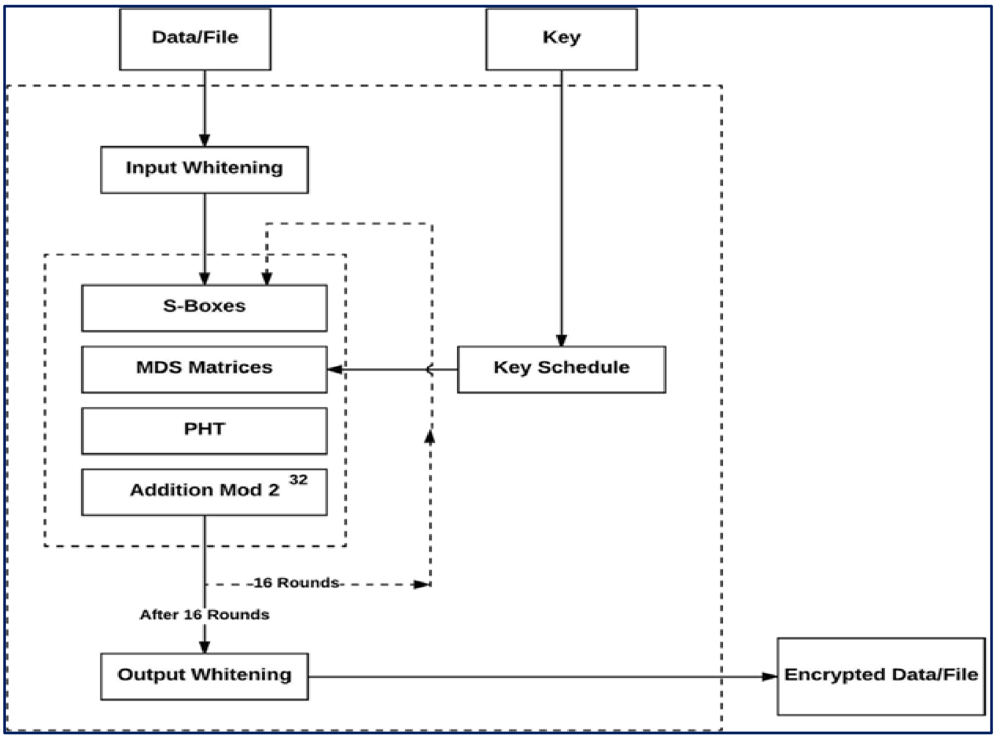

Figure1. Twofish cryptographic architecture

Twofish additionally depends on the Feistel structure. Having developed Blowfish, Bruce Schneier created developments to his cipher that therefore result in Twofish that may be a symmetric cipher, with a block size of 128 bits and a key of any length upto 256 bits. The plain text is broken into 2 32-bit words and fed into the F-boxes. The 2 words are additionally broken down into four bytes among these F-boxes and sent through S-boxes, every smitten by totally different keys. The four output bytes are combined into a 32-bit word using the Maximum Distance dissociable (MDS) matrix. The Pseudo Hadamard transform (PHT) is employed to mix the two 32-bit words. this can be then XOR-ed with the opposite half. Certain 1- bit rotation operations also are performed before and once the XOR operation. after this cipher over the Blowfish cipher is seen in [8].

There are different security risks in cloud computing like Poor Cloud security, Denial of service, Lock-in effect, Downtime. The other security risks like Resource exhaustion, Confidentiality and the Integrity of the data in the cloud result in the financial, economic and reputational losses and can make an organization inoperable. So there is an important need to study cloud computing security issues and find methods to minimize these risks and their impact.

Steganography is a technique which hides the secret data into envelope. The presence of data is not visible to all users. Only legal user knows about the data. Text steganography technique is used to provide high level data security. Secret data of user hide into text cover file. After adding text into text cover file it looks like normal text file. If text-file found by an illegal user than also cannot get sensitive data. If an illegitimate user tries to recover original data than a large amount of time is essential. [9] DES algorithm is used for text encode and decode. The advantage of the text steganography technique is to provide security to text. Minimum space is essential for text steganography as compare to image steganography. [9] Three bit LSB technique used for image steganography is suggested to Sensitive data of the user to hide into the cover image. Theauthor has implemented high throughput architecture for the cryptography algorithm.AES is symmetric-key cryptography algorithm. It supports three types of keys. For 128 bit key require 10

rounds, 192-bit key require 12 rounds and 256-bit key require 14 rounds. In improved AES algorithm encryption and decryption, time is reduced. [10], [11].
In this paper, we have discussed related workin section II.The proposed Scheme in section III, results and discussion are presented in section IV and finally conclude in section V.

II. RELATED WORK

The idea behind cloud computing is to provide innovative data sharing services over the network changing the way we used to share data resources before. Many enterprises want the minimal cost and effective benefits of cloud computing, without losing control and security. The security that is generally applied at the network border tends to disappear in cloud built computing, where networks without robust firewalls are connected by many types of cloud consumers with private and public data hubs [12]. The capability of Twofish algorithm in low power source consumption and efficient execution time performance is revealed in researches [13]

The authors describe the process of AES and RSA in their encryption and decryption. They thinkthe hybrid algorithm improved the speed of RSA encryption and decryption, and also solves the keymanagement problem in the AES algorithm [5].Fang presented an overview about the AES algorithm, and then the significance of the security in the cloud storage system, they proposed an approach for the security mechanism of users' files when uploading and downloading using AES algorithm. [14] In Cloud Storage any organization’s or individual’s data is stored in and accessible from multiple distributed andconnected resources that comprise a cloud. To provide secure communication over distributed and connected resources,the encryption algorithm [14] plays a vital role. It is a fundamental tool for protecting the data.

The comparative study by Faung shows different encryption algorithms kind; Asymmetric and symmetric, block cipher and stream cipher. These EA are AES, IDEA, DES, RC4, and RSA. At the conclusion, he found from the experimental results, that RSA has least performance efficiency as compared to DES, AES, IDEA and RC4 algorithm. Also, conclude that the performance of RC4 algorithm is best as compared to all other algorithms discussed in this paper. [14] The author [15] introduces the combination of RSA and improved blowfish algorithm for encryption and decryption of cloud data. Although the combination is robust and secure it affects overall the encryption speed. Thuswe propose a better hybrid of updated RSA and Twofish algorithm to overcome the encryption delay and security issues in the previous technique.

Existing methods like DES and RSA algorithms experimented by authors [16] for cloud storage security is with only single level encryption and decryption. This type of encryption can be breached with ease. Several techniques have been proposed by various researchers like DSA and RSA and AES and RSA. But DES is extremely susceptible to attacks, Weak keys is also a big issue and is exposed to brute force attack. [17].Various studies have emphasized the security of and threats for cloud storage and cloud computing in general: [18], [19], [20], [21], and [22]. However, all these studies do not focus on publicly available IaaS-based cloud storage. The cloud storage has specific properties and potential to be modeled.

Generally, cloud computing users don’t have full control over the available assets in the cloud and data exposure risk is always there. Various researches have been conducted to address the common as well as rare security issues that arise constantly in cloud computing and also to present effective techniques to prevent such problems in the future. [23].The author [24]proposed Blowfish, a new secret-key block cipher. Also, this paper discussed the requirements for a standard encryption algorithm. While it may not be possible to satisfy all requirements with a single algorithm, it may be possible to satisfy them with a family of algorithms based on the same cryptographic principles.

The cryptography scrambles a message so that if it is intercepted, it cannot be understood to unauthorized users but it may draw doubt. Steganography camouflages a message to hide its existence and secret message hidden in a cover image cannot be suspected. [25].The secret message is hiding into the cover object and generates the stego object using an embedding algorithm and may use a stego key. This stego object is sent to the other party where the secret message is simply extracted from the stego object using an extracting algorithm [25][26]

The following ideas must be considered when creating a steganography method [27]

a. **Capacity**: It is the maximum number of secret messages bits that can be embedded in the cover without losing the quality of cover.

b. **Security**: It is one of the most significant evaluation standards in steganography. A good steganographic method should be proof of steg analysis attacks.

c. **Imperceptibility**: It refers to the transparency and quality of an image. After hiding a secret message into the cover image, transparency and quality are degraded into a stego image compared with a cover image. Therefore, the stego image should seema like to the original image.

In [28], the authors increased cloud storage security using steganography, encryption, decryption techniques, compression, and splitting technique to overcome the limitations of traditional data protection algorithm. Once the data have been authenticated, they are concealed using image steganography to ensure smooth transfer without drawing the attention of intruders.

In [29], after exploring the security problem in cloud computing, the authors propose an efficient stenographic strategy to support the data security atrest. In this technique, the first and last bits of the image are extracted from odd pixel values of an image file. This image covers the message to be hidden using the steganographic method, to produce an image similar to the original.

III. PROPOSED SCHEME

This new scheme increases security by using a modified Twofish algorithm and steganography. The encryption process converts the original data intocipher data with the help of a modified Two fish algorithm. If time and memory is the main issue in cloud security, Twoshishalgorithm is the best suitable algorithm. The LSB steganography technique is being used to hide key information into a cover image using java language. Key information contains the part of the file being encrypted by the modified Twofish algorithm and key. Data encryption keys are inserted into the cover image using the LSB technique. Stego image is sent to a valid receiver with the Key.The receiver can then decrypt the image with the key to access the data. LSB technique is widely used for hiding data and has high payload capacity, but it is simple to encode. DCT technique can also be used but it is more complex and has a lower payload, although provides higher security than LSB technique [30].The Architecture of the proposed technique is shown in figure 2.

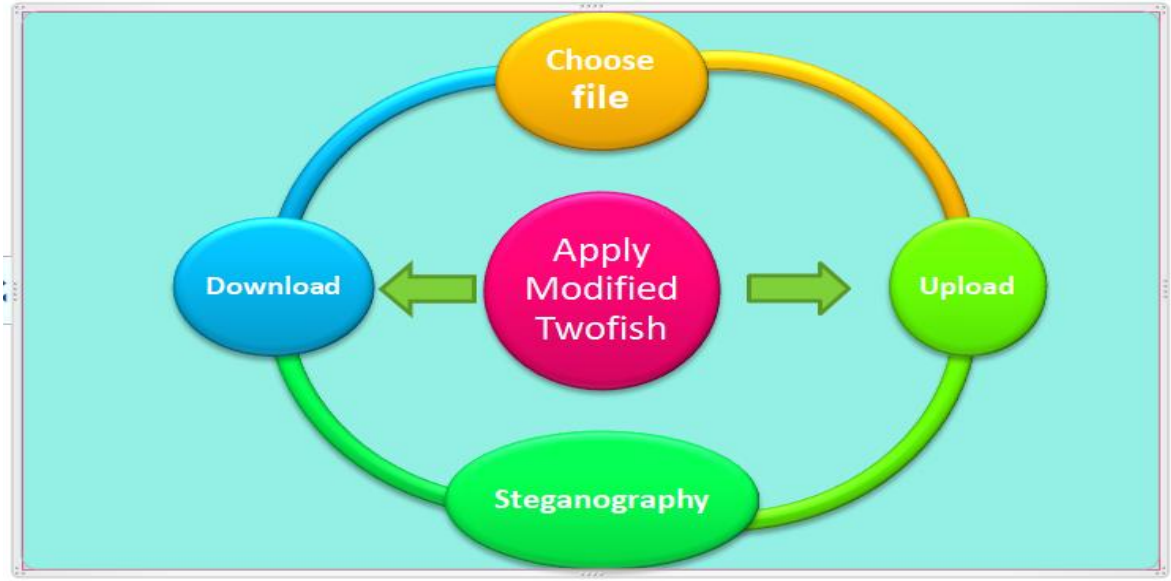

Figure-2 Architecture of the proposed technique

The proposed scheme demonstrated the least amount of time for encryption and decryption processes. The decryption procedure of Twofish can be done in the same way as the encryption procedure by reversing the order of the sub-keys, which is one of the advantages of Feistel networks.

Encryption and decryption time impacts the performance of the system. Its time must be less making the system fast and responsive. The pattern is reversed of the same algorithms in a decrypted form when the user downloads a file from a cloud network, making it as secure as possible. The technique is intended to make the Cloud secure and fast.
The data has to go through several processes such as encryption, embedding, extracting and decryption process to enhance security in the cloud environment.

The flow diagram of the proposed systemis elucidated in figure-3

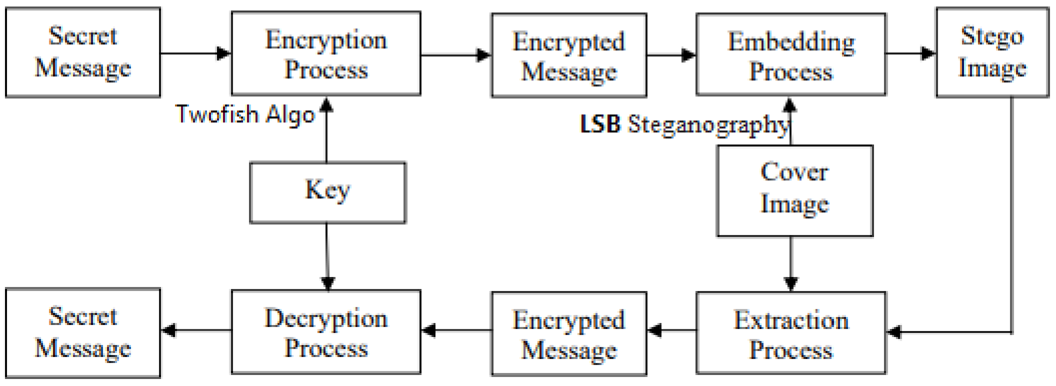

Figure-3- Flow diagram of proposed system

DOI: 10.15680/IJIRCCE.2018. 0610048

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

IV. RESULTS AND DISCUSSION

The proposed system of modified Twofish Encryption with steganography is one of an effective and efficient method to protect cloud data storage. Twofish algorithm ispre-calculated and has more speed than AES. There are total of 16-rounds in Twofish algorithm. Some building blocks of Twofish algorithms are: [13]
S-Box: Twofish Algorithm builds up to 4 key reliant 8*8 bit blocks using a secure key authorization. In Twofish, each S-box consists of three 8-by-8-bit fixed permutations for 128-bit and four for 192-bit, chosen from a set of two possible permutations, q0, and q1.

MDS: Maximum Distance Separable guarantees that there several non-zero bytes acting as a dispersion in Twofish apparatus. MDS is a maximum separable matrix. It is a matrix ofbytes that multiplies a vector of four bytes. Multiplications arecarried out in the Galois Field GF(28) with the primitive polynomial x8 + x6 + x5 + x3 + 1. Each byte is converted into apolynomial in which each power p of x is present only if the p-th bit is 1. A multiplication in GF amounts to a multiplication of polynomials followed by a division by the primitive is a reversible transformation of a bit string that provides cryptographic diffusion.

PHT:PHTPseudo Hadamarad Transform utilizes a simple yet active fickle effect. PHT is a reversible transformation of a bit string that provides cryptographic diffusion. transform consists of two additions. SAFER Algorithm uses PHTs extensively for diffusion for the first time. Twofish uses a 32-bit PHT.

Q-Permutation: The Q-Permutation is at the core of the design of Twofish. Thepermutations q0 and q1 are fixed permutations on 8-bitvalues.These permutation functions are the main componentsof the S-boxes [5].

TWOFISH FUNCTIONS

Function F: TheFeistel function F is a key-dependent permutation on 64bit values. It takes three arguments, two input words P0, andP1, and the round number r used to select the appropriate subkeys. R0 is passed through the g function, which yields T0.R1 is rotated left by 8 bits and then passed through the gfunction to yield T1 [14]

4.2 FunctionG: The function g forms the heart of Twofish. The input word Xis split into four bytes. Each byte is run through its own key-dependentS-box. In Twofish algorithm, for encryption, firstly, a 128-bit input plaintext P is divided into four parts of 32-bit each, say P0, P1, P2, P3 and XORed with four 32-bit sub-keys, K0, K1, K2 . 2, then sixteen rounds of iteration and then the four outputs are Xor-ed with four more keys K4, K5, K6, K6.

Some modules have been modified keeping delay as the main constraintAll the modules and functions are interrelated hence, after modifying MDS and PHT function g and function F also got modified. The results show the delay of Twofish algorithm of the 128-bit key [18]

The modules MDS and PHT had been modified and implemented for the modified algorithms. All the modules and functions are interrelated hence, after modifying MDS and PHT function g and function F also got modified. According to the results it is clear that modified 192-bit key twofish algorithm has less delay than 192-bit twofish.[18].

The delay and frequency for encryption, decryption for 192-bit Twofish algorithm and 192-bit modified Twofish algorithm is revealed in Table-1.

DOI: 10.15680/IJIRCCE.2018. 0610048

Algorithm	Factors	Encryption	Decryption
Twofish algorithm *(192-bit)*	*Delay (ns)*	114.905	114.905
	Frequency (MHz)	8.759	8.759
Modified Twofish algorithm *(192-bit)*	*Delay (ns)*	102.819	102.819
	Frequency (MHz)	9.352	9.352

The following figure Illustrates time comparisons between Twofish and Blowfish. The Twofish takes lesser encryption time than Blowfish. The author's [8] experimental results have shown better results for the Twofish algorithm. Figure-4 showsthe encryption speed of the Twofish algorithm is more than Blowfish.

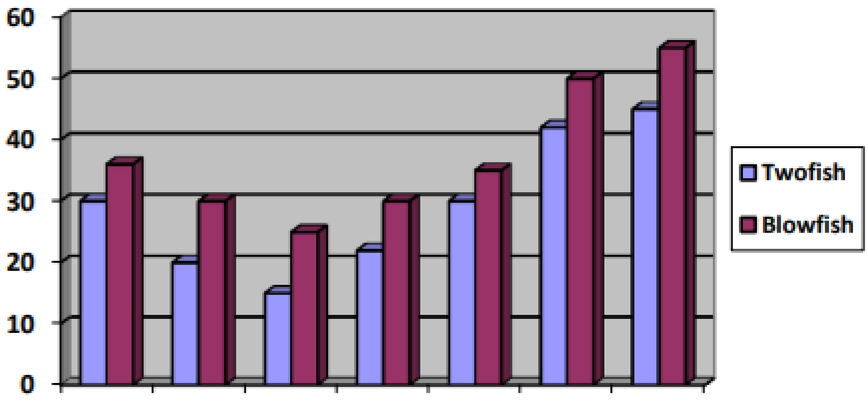

Figure-4 shows the encryption speed of Twofish algorithm is more than Blowfish

The experimental results of the proposed Scheme demonstrate better performance results than existing techniques likeRSA and Bluefish technique [15] in terms of encryption speed. The security and efficient technique is very important in cloud computing adaptability. The proposed technique is secure and efficient with minimum delay in encryption and decryption process.

The proposed technique of modified Twofish algorithm and steganography overcomes the encryption delay and security issues present in old techniques. The modified Twofish algorithm makes the proposed scheme more efficient and the steganography part adds more security and confidentiality of the encrypted data. Thus enhancesthe secret communications which is vital forthe cloud computing environment.

V. CONCLUSIONS

An efficient and secured scheme for improving Cloud Data Security is introduced. Various encryption algorithms and security concerns have been thoroughly reviewed. Each of the security methods has its merits and demerits. The speed, performance, strength, and weakness of the algorithm is vital to apply a suitable cryptography technique. The proposed system of modified Twofish Encryption with steganography is one of the effective and efficient scheme to protect and preserve cloud data storage. The Results analysis of the proposed technique demonstrates better performance results as it is efficient with minimum delay in the encryption and decryption process. The future work would be to extend its implementation for huge sized video files for encryption and decryption.

REFERENCES

[1]. Malik, A., & Om, H. (2018). Cloud computing and internet of things integration: Architecture, applications, issues, and challenges. In Sustainable cloud and energy services (pp. 1-24). Springer, Cham.
[2]. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International journal of Computer Science and Information Technology Vol2 (3), 242-249 2012.
[3]. Wu, B., Chen, J., Wu, J. and Cardei, M. (2007) A survey of attacks and countermeasures in mobile ad hoc networks. Signals and Communication Technology, Part II, 103-135.
[4]Randeep Kaur ,SupriyaKinger, "Analysis of Security Algorithms in Cloud Computing", Volume 3, Issue 3, March 2014
[5] Bhise, A. S., &Phursule, R. N. (2017). Developing secure cloud storage system by integrating trust and cryptographic algorithms with role based access control. International Journal of Computer Applications, 168(10).
[6] Ramesh, A.; Suruliandi, A., "Performance analysis of encryption algorithms for Information Security," International Conference on Circuits, Power and Computing Technologies, vol., no. 2, pp.840-844, 20-21 March 2013
[7] Agrawal, M. & Mishra, P. (2012). A Modified Approach for c Cryptography Based on Blowfish Algorithm. International Journal of Engineering and Advanced Technology, 1(6), 79-83.
[8] Deepali D. Rane, "Superiority of Twofish over Blowfish", International Journal of scientific research and management, vol. 4, no. 11, pp. 4744-4746, 2016.
[9] Abu Marjan, Palash Uddin, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography",IEEE, IFOST,pages 14-17, October 2014.
[10]Rasmi, A., &Mohanapriya, M. (2017). An Extensiv Survey of Data Hiding Techniquesǁ. European Journal of Applied Sciences, 9(3), 133-139.
[11] Solichin, A., & Ramadhan, E. W. (2017, October). Enhancing data security using DES-based cryptography and DCT-based steganography. In 2017 3rd International Conference on Science in Information Technology (ICSITech) (pp. 618-621). IEEE.
[12]. Effective Ways of Secure, Private and Trusted Cloud Computing by Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta and ManojDiwakar ; CSE & IT, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, 173215,India
[13] Gehlot, P., Biradar, S. R., & Singh, B. P. "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL". International Journal of Computer Applications, 70(13). (2013)
[14] Fang, Z., Sun, Y., Sun, Y., & Yang, J. (2013, July). The Reseach of AES algorithm and application in cloud storage system. In 2nd InternationalConference on Science and Social Research (ICSSR 2013). Atlantis Press.
[15] Shouket Ahmad, "Robust Cryptographic Technique for Improving Data Security in cloud computing.International Journal of Innovative Research inScience,Engineering and Technology May(2017).
[16]. RashmiNigoti, ManojJhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013
[17]. LimorElbaz&Hagai Bar-El, "Strength Assessment of Encryption Algorithms", October 2000, website: http://www.discretix.com/PDF/Strength%20Assessment%20of%20Encryption%20Algorithms.pdf
[18] Cloud Security Alliance,"Security Guidance for Critical Areas of Focus in Cloud Computing" V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.-2011
[19]Shouket Ahmad K, Data Protection in Cloud Computing-vulnerabilities, challenges and Solution. Int Journal of Computer Trends and Technology V34(4):179-185, April 2016. ISSN:2231-2803.
[20] European Network and Information Security Agency,"Cloud Security Guide for SMEs" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloudcomputing/security-for-smes/cloud-security-guide-for-smes. -2013
[21] Open Security Architecture (2015). SP-011: Cloud Computing Pattern.http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloudcomputing.
[22] National Institute of Standards and Technology ,"NIST Guidelines on Security and Privacy in Public Cloud Computing".-2011 http://www.nist.gov/manuscript-publicationsearch. cfm?pub_id=909494
[23] Cloud Security Alliance ,"Security Guidance for Critical Areas of Focus in Cloud Computing" V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.-2011
[24]B.Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204
[25]Johnson, N. F., Duric, Z., &Jajodia, S. (2001). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures (Vol. 1). Springer Science & Business Media.

[26]Ali, A. A., &Saad, A. H. S. (2013). Image steganography technique by using Braille method of blind people (LSBraille). International Journal of Image Processing (IJIP), 7(1), 81-89.
[27] Hashim, M., Rahim, M., Shafry, M., &Alwan, A. A. (2018). A review and open issues of multifarious image steganography techniques in spatial domain. Journal of Theoretical & Applied Information Technology, 96(4)
[28] Rani, K., &Sagar, R. K. (2017). Enhanced data storage security in cloud environment using encryption, compression and splitting technique. Paper presented at the Telecommunication and Networks (TEL-NET), 2017 2nd International Conference on.
[29] Suneetha, D., & Kumar, R. K. (2017). A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography. Advances in Computational Sciences and Technology, 10(9), 2737-2744
[30]Ardiansyah, G., Sari, C. A., &Rachmawanto, E. H. (2017, November). Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm. In 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE) (pp. 249-254). IEEE.