ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 6 || June– 2019 ||
International Journal of Computational Engineering Research (IJCER)

Distributed Data Security Enhancement in Public Cloud Storage and Hosting Using Data Obfuscation & Steganography

Momin Uddin[1], Dr. Shashank Singh[2]

[1]M.Tech Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, UP, India
[2]Assistant Professor, Department of Computer Science & Engineering, Integral University, Lucknow, UP, India

ABSTRACT
The data is not considered to be very secure at the cloud because it can be retrieved or extracted easily using some tools or algorithms. In this paper we aim to improve the confidentiality, integrity, and security of the information amassed on cloud by exploiting the conception of cryptography as well as steganographic techniques which make data obfuscated. We use distributed algorithm by exercising Steganography technique and distributing the file and its reference into two parts at different locations.

Keywords: *Cloud Security, Steganography, Cryptography, Data obfuscation*

Date of Submission: 11-06-2019 Date of acceptance:28-06-2019

I. INTRODUCTION

Distributed computing alludes to the utilization of figuring assets, those being equipment and additionally programming) that dwell on a remote machine and are transmitted to the end client as an administration over a system, with the most common model being the web. By definition, a user bestows his information to a remote administration, which has constrained to no impact.

When it originally showed up as a term and an idea, a ton of commentators expelled it similar to the most recent tech prevailing fashion. The Cloud has consummated cutting costs for undertakings and assisting customers center around their center business as opposed to being dispirited by IT predicaments. Consequently, it appears that it is staying put for the quick future.

1.1. Cloud security

Disseminated computing safety is a swiftly developing administration that gives a hefty number of indistinguishable functionalities from conservative IT sanctuary. This integrates protecting basic data from larceny, information spillage, and annulment.

One of the advantages of cloud administrations is that you can work at scale and still stay secure. It is like how one at present supervises protection, nevertheless, at this point, one has improved approaches for conveying safekeeping arrangements that address novel regions of apprehension. Cloud safekeeping does not change the methodology on the most dexterous method to supervise safekeeping from averting to an investigator and curative activities [1].

1.2. Steganography

Steganography is the study of entrenching and trouncing messages in a medium called a cover text. Steganography is associated with cryptography. It was utilized by the prehistoric Greeks to conceal information about troop activities by tattooing the information on someone's skull and then letting the individual grow out their hair. Simply put, steganography is as aged as grime.

The fundamental initiative behind cryptography is that anyone can maintain a message a furtive by encoding it so that no one can interpret it. If a high-quality cryptographic cipher is applied, it is probable that no one, not even a government entity, will be able to interpret it. Figure 1 depicts this conception of steganography.

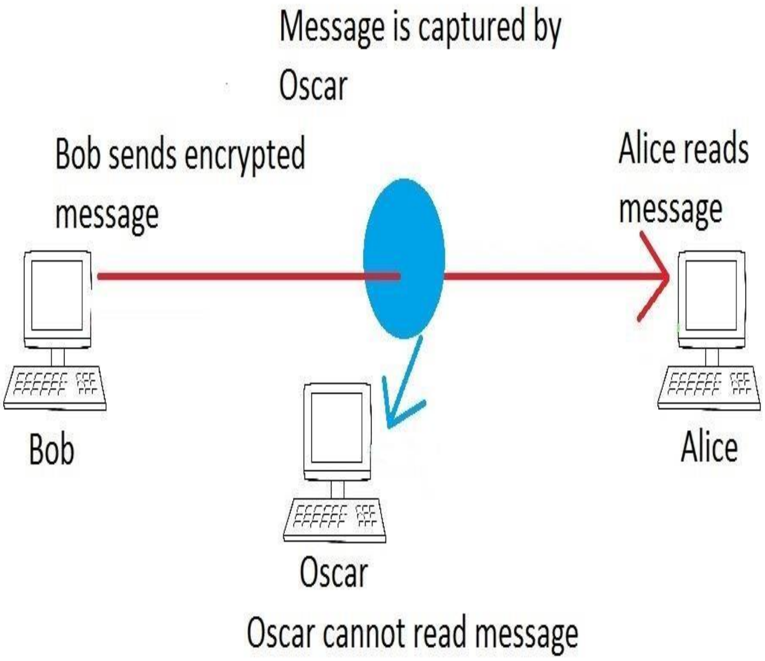
Message is captured by Oscar
Bob sends encrypted message
Alice reads message
Bob
Alice
Oscar
Oscar cannot read message

Figure 1.1: Conception of Steganography

The straightforward truth is that an encrypted message does not bear a resemblance to anything else but an encrypted message.

1.3. **Cryptography**

Symmetric cryptography, asymmetric cryptography, and hashing are the diverse categorizations of cryptography as revealed in figure 2.

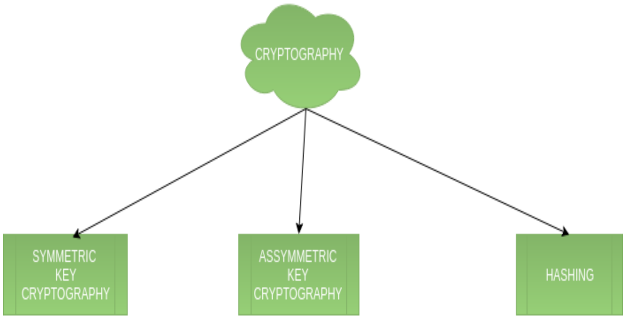

Figure 1.2: Cryptography categorizations

1.3.1. Cryptography with Symmetric key

It engrosses practice of one furtive key for encryption as well as decryption algorithms which assist in protecting the stuffing of the message. The potency of symmetric key cryptography depends upon the number of key bits. In comparison with asymmetric key cryptography, it is quicker. The key circulation hitch is biggest task in this approach as the key has to be conveyed from the dispatcher to the recipient through a protected path[3].

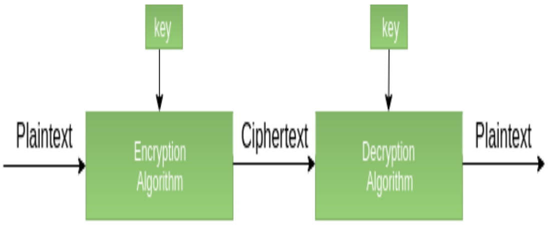

Figure 1.3: Cryptography with Symmetric key

1.3.2. Cryptography with Asymmetric key

This approach is also recognized as public key cryptography since it involves usage of a public key along with a secret key. It resolves the setback of key distribution as both parties use dissimilar keys for encryption/decryption. It is not practicable to utilize for decrypting bulk messages as it is extremely time-consuming as compared to symmetric key cryptography[4].

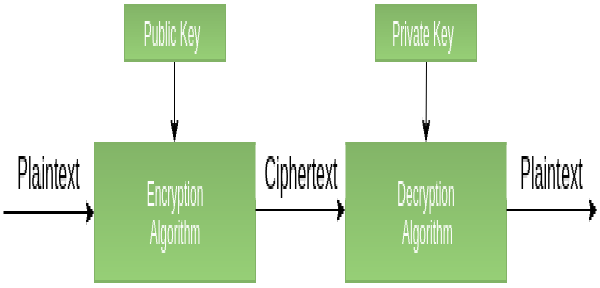

Figure 1.4: Asymmetric key cryptography

II. LITERATURE REVIEW

Xiao et. al. [5] recognized five mainly representative safekeeping and confidentiality attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Commencing with these attributes, they presentd the associations among them, the vulnerabilities that may be subjugated by attackers, the menace models, as well as existing defence strategies in a cloud scenario.

Karun Handa et. al.[6] portrays how to protect data as well as information in a cloud surroundings in time of data sharing or storing by using their proposed cryptography and steganography method. Their proposed approach assists to make a sturdy structure for the safety of data in the cloud computing meadow or web.

Parah, Shabir A. et. al.[7] presented a sky-scraping capacity steganographic method in which secret data is entrenched in Intermediate Significant Bit planes of the cover image. The data to be entrenched is broken down in blocks of comparatively decreasing lengths and each block is entrenched in the cover media under control of a extremely secure key. This work showed gorgeous outcome with respect to imperceptibility and capacity when compared with a few reported techniques in addition to providing ample data safety.

Zhongma Zhu et. al.[8] proposed a protected data sharing method for vibrant members. Initially, they proposed a secluded method for key sharing without any secluded communication mediums, and the users can securely achieve their private keys from group manager. Then after, their method can attain fine-grained access control, any user in the group can utilize the source in the cloud and rescinded users cannot access the cloud again after they are rescinded. They protected the scheme from collusion assault, which resulted in confidence that rescinded users can never obtain the original data file even if they conspire with the untrusted cloud.

1. MySteg: PROPOSED APPROACH FOR CLOUD SECURITY

We distribute the main message into two parts as follows:

- At hosting site
- At Cloud

At hosting site, we store Images, Audio & Video files which are encrypted using the steganographic method. At Cloud, the references of the Image, Audio & Video files or their keys are stored.lse. So, even if someone got the key or reference from the cloud then he cannot get the information as the other half to dncrypt a file is present somewhere else. The system architecture, block diagram and process diagram of proposed method is illustrated in figure 1, figure 2 and figure 3 respectively.

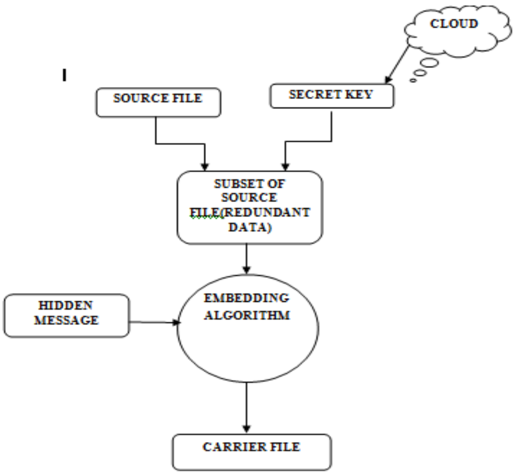

Figure 3.1: System architecture of proposed method

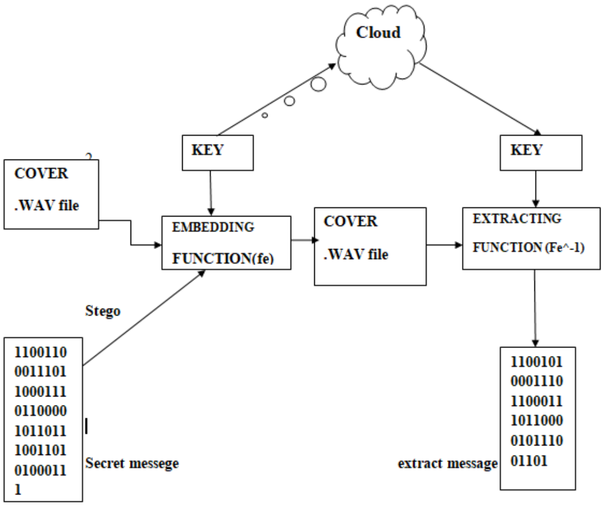

Figure 3.2: Block diagram of proposed method

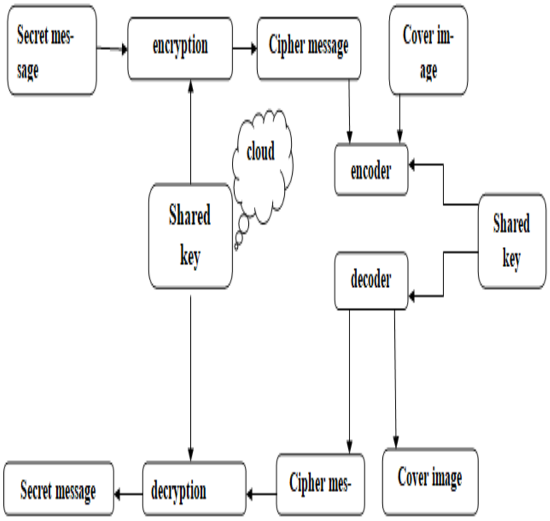

Figure 3.3: Process diagram of proposed method

3.1 Algorithm

Encode ()

```
1.   to-bit-generator(msg)
2.   for  c.each  msg
```

```
 0←ord(c)
For   i=1  to  8
Binary (0)
endfor
Enfor
```

Decode ()

```
Hidden_message←to-bit-generator(open(file))
img=cv2.(imread(original.png,cvz. IMREAD_GRAXSCALE)
aes message ← aes encryption(hidden_message)
for h ← len(img)
for w in len(img{0})
img [h][w]←(img[h][w] &--1)|next(aes message)
cvz.imwrite("output.png",img)
```

AES ENCRYPTION (MSG)

1. Substitution bytes (substitution)
2. 3- Boxes in bytes to byte substitution of block
3. Shift rows (simple permutation)
4. Mix columns (substitutions)
5. Uses finites field arithmetic on gf(2^8)
6. Add round key (substitution)
7. Simple bitwise xor of current block with portion of ex-panded key.
8. This is only the stage that uses the key
9. Store key on the cloud
10. Stop.

DECRYPTION ALGORITHM

Retrieve key from the cloud.

1. Decryption make use of keys in reverse order just as with DES
2. Decryption algorithm is not the identical as encryption algorithm –unlike DES
3. The 4 stage utilize in the rounds consist of three substitution And permutation
4. Inverse shift rows(simple permutation)
5. Inverse substitution bytes (substitution)
6. Add round key (substitution)
7. Inverse mix columns (sustituion)
8. 10th round involve 3 stages as in encryption.

Encryption and decryption methods are illustrated in figure 4 and figure 5 respectively.

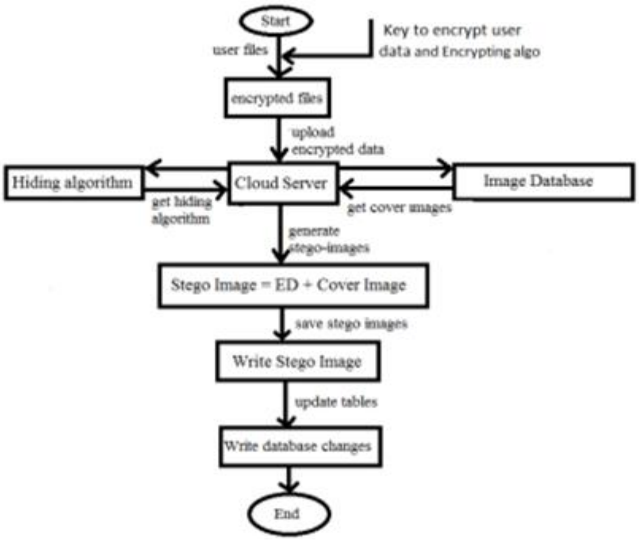

Figure 3.4: Encryption process used proposed method

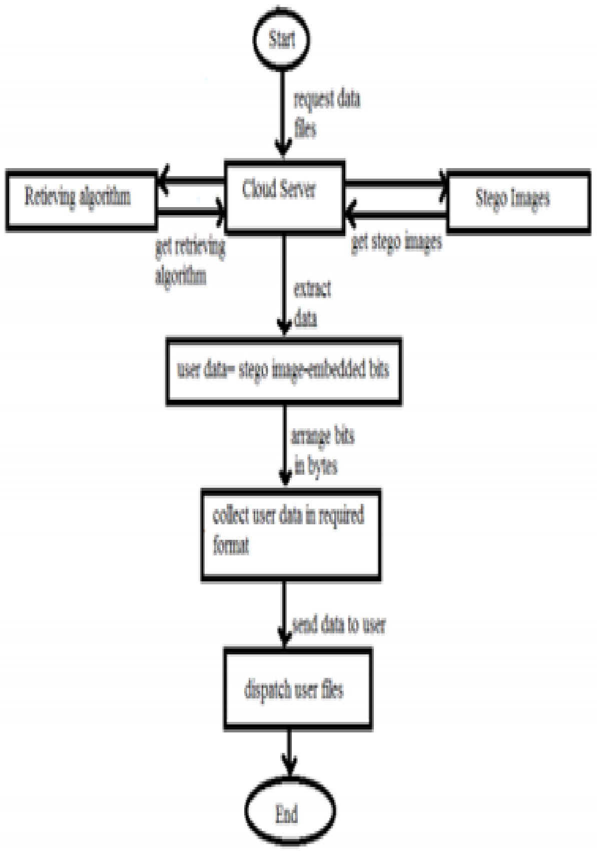

Figure 3.5: Decryption process used proposed method

III. EXPERIMENTAL EVALUATION

We implemented the proposed approach in python and compared the accuracy of my approach with existing approaches such as Optimum Pixel Adjustment Process (OPAP)[9], Stream of 1's and 0's[11], Pixel value differencing (PVD1 and PVD2)[10]. We compared my work in terms of time complexity, in which my algorithm i.e. MySteg is having better time complexity than OPAP[9], Stream of 1's and 0's[11], PVD1, PVD2[10]. It has less time complexity as shown in figure 6.

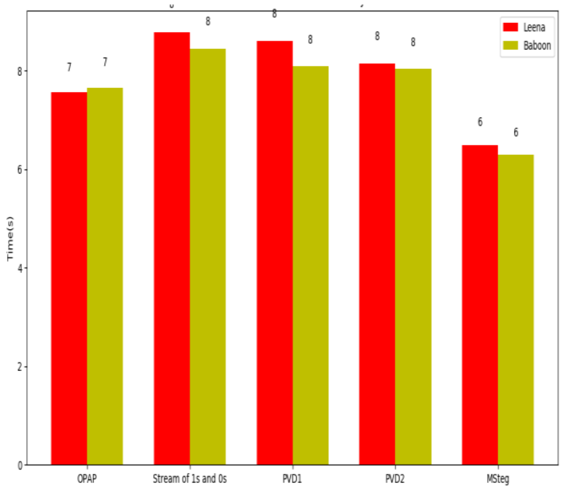

Figure 6: Comparative analysis of proposed approach (MySteg)

IV. CONCLUSION

Security is the greatest concern with regards to distributed computing. By utilizing a remote cloud-based foundation, an organization basically gives away private information and data, things that may be delicate and classified. It is then up to the cloud specialist organization to oversee, ensure and hold them, along these lines the supplier's dependability is extremely basic. By our novel approach data is hidden in any images or audio or video and its secured from the hackers. Using our algorithm to different types of data can be sent in a single unit. Data transferring in more reliable using our novel approach. Data is more secured by providing two different locations for storing the data by using this approach.

REFERENCES

[1]. Kalaiprasath, R., Elankavi, R. and Udayakumar, D.R., Cloud. Security and Compliance-A Semantic Approach in End to End Security. International Journal Of Mechanical Engineering And Technology (Ijmet), 8(5), pp.987-994, 2017.

[2]. Menon, N., A survey on image steganography, IEEE International Conference on Technological Advancements in Power and Energy (TAP),pp. 1-5, 2017.

[3]. Chandra, Sourabh, Bidisha Mandal, Sk Safikul Alam, and Siddhartha Bhattacharyya. "Content based double encryption algorithm using symmetric key cryptography." Procedia Computer Science 57, pp 1228-1234, 2015.

[4]. Yassein, Muneer Bani, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. "Comprehensive study of symmetric key and asymmetric key encryption algorithms." In 2017 international conference on engineering and technology (ICET), pp. 1-7. IEEE, 2017.

[5]. Xiao, Z. and Xiao, Y., Security and privacy in cloud computing. IEEE communications surveys & tutorials, 15(2), pp.843-859, 2012.

[6]. Handa, K. and Singh, U., 2015. Data security in cloud computing using encryption and steganography. International Journal of Computer Science and Mobile Computing, 4(5), pp.786-791.

[7]. Parah, Shabir A., Javaid A. Sheikh, and G. M. Bhat. "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique." In 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET), pp. 192-197. IEEE, 2012.

[8]. Zhu, Z. and Jiang, A secure anti-collusion data sharing scheme for dynamic groups in the cloud. IEEE Transactions on parallel and distributed systems, 27(1), pp.40-50, R., 2015.

[9]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) 469– 474, 2004.

[10]. M.Padmaa Dr.Y.Venkataramani.‖ ZIG-ZAG PVD - A Nontraditional Approach. International Journal of Computer Applications 5(7),pp 5–10, 2010.

[11]. N. Wu and M. Hwang, "Data hiding: current status and key issues," International Journal of Network Security, vol4, No.1, pp. 1-9, Jan. 2007.

Momin Uddin"Distributed Data Security Enhancement in Public Cloud Storage and Hosting Using Data Obfuscation & Steganography" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 6, 2019, pp 11-17