# SECURING CLOUD DATA USING BLOWFISH ALGORITHM COMBINED WITH TEXT STEGANOGRAPHY

**ISHAQ MUHAMMED; MUHAMMAD ALIYU; ILIYA MUSA ADAMU; AMATULLAH YAHAYA ALIYU; ABDULKADIR MAIGARI TURAKI; & SUNUSI ABDULHAMID DANTATA**
*Federal Polytechnic Bauchi, Computer Science Department*

## Abstract

*Cloud computing has emerged as a computing paradigm and has gotten much attention in the last years known to handle systems with large-scale services sharing between vast numbers of users. It provides enormous storage for data and computing power to users over the Internet. There are many issues with the high growth of data. Data security is one of the most important issues in cloud computing. There are many algorithms and implementation for data security each having its own merit and demerit. These algorithms provided various encryption methods. In this Paper, we propose a combination of these algorithms to provide a high level of security to cloud data, Blowfish Symmetric Algorithm as Cryptography combined with Text Steganography as a cover medium considering that both have proven to have good performance and less data redundant in literature.*

***Keywords**: Cloud Computing, Symmetric Algorithm, Cryptography, Text Steganography.*

## Introduction

Cloud computing is a ubiquitous paradigm where everything offered to the cloud client is treated as service and it is regarded as a utility computing model which offers the wide range of services to the users on-demand bases in a distributed fashion, due to its versatility, agility both medium and large-scale emerging and developing technologies are adopting the cloud (Kumari et al., 2017). There are three services provided by cloud computing that are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Garrison et al., 2015). The basic examples of cloud computing which are used by general people in daily life are Facebook, YouTube, Dropbox, and Gmail etc. It offers scalability, flexibility, agility, and simplicity that's why its use is rapidly increasing in the enterprises (Srivastava & Khan, 2018). Cloud computing offers lots of benefits and features. It offer scalability in that applications that run within the cloud are normally highly scalable. An applicant can manually add or remove resources or application can be configured to scale automatically. Virtualization is to use hardware or software to create the observation of something. Must server have their own CPU that is capable of running a specific operating system (OS), such as Windows, Linux, or Mac OS. By using special software, server can be shown as it has multiple CPUs and are running the same or different operating systems and the server CPU switches its processing power frequently among the various operating systems (Puthal et al., 2015).

As the use of cloud computing becomes widespread, security of the outsourced user data becomes an important research topic (Kumari et al., 2017). The parameters that are taken into consideration for data security are Confidentiality, Integrity, and Availability. Can we trust some third party and share our private data with them or does our data remain confidential over cloud? (Confidentiality), Does the data that we have stored on cloud would be available whenever we required it i.e. Availability, and Integrity which entails that the data outsourcing party must give guarantee to the user that the data that they have stored on cloud would not be modified or altered by any unauthorized user. Many techniques have been adopted by researchers to secure their data in the cloud among such techniques are cryptography and steganography (Abdulkarim & Souley, 2017).

**Cryptography** is widely used to secure data in cloud computing. It is classified into Symmetric (private-key) and Asymmetric (public key) keys encryption. Examples of Symmetric algorithms are DES, 3DES, AES, Blowfish and DSA (Digital Signature Algorithm), Elliptic Curve, Diffie-Hellman (key exchange) and RSA are examples of Asymmetric algorithms (Yassein et al., 2018). But Blowfish is strongest and fastest in data processing and storing compare to other algorithms. In Symmetric key, encryption uses only one key for encrypting and decrypting data between the sender and the receiver, called secret key. On the other hand, Asymmetric key encryption uses public keys for encryption and different key for decryption that is also called private key.

**Steganography** is the art of concealing a message in a cover without leaving a remarkable track on the original message (Sharma, 2013). Steganography is a technique to hide information from the observer to establish an invisible communication (AL-Ani et al., 2010). This steganography system consists of a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a large opportunity in such a way that someone can't know the presence of the hidden message and thus they can't access the original message. According to (Nath & Nath, 2011) four (4) different types of steganography exits. Text, Image, Audio and Video Steganography.

**Text Steganography**: They have a very small amount of redundant data, therefore they are very often used.

**Audio/Video Steganography**: They are very complex in use.

**Image Steganography**: It is mostly used for hiding process of data. It provides a secure and simple way to transfer the information over the internet. It is categorized in various types:

- Transform Domain: It includes JPEG.
- Spread Spectrum: It includes patch work.
- Image Domain: It includes->LSB and MSB in BMP and LSB and MSB in JPG

## 1. Proposed Work

The main aim of the proposed method is to introduce a more secured communication means by which merging cryptography and steganography techniques will make it more difficult for unauthorized users to retrieve the plaintext of a secret message from a stego-object. The proposed method is divided into two parts. In the first part, the Blowfish algorithm will be used as it is suitable for cryptography as it is the most efficient encryption algorithm in the world (Gowda, 2016), to encrypt the data to give cipher text and the second part, text steganography will be merged with the cipher text to hide the encrypted data in the cipher text as they have less redundant information (Krishnan et al., 2017), where a message being sent is concealed. Therefore, two levels of security have been applied. Based on the evaluation by (Krishnan et al., 2017), Character and String Mapping has being proposed to be used as the steganography method as it requires the least number of cover characters to embed a secret character.

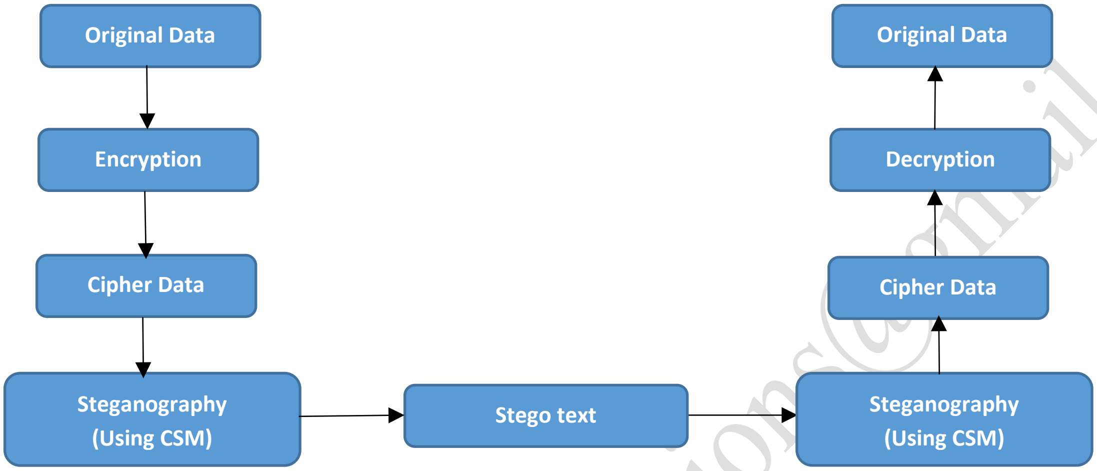

*Figure 1: Architecture of the Proposed System*

### Working Principle of the Proposed System

The system encrypts the plain data (text, image, audio or video) using BLOWFISH Algorithm and give cipher data. Now Steganography is done on this cipher data. This process gives stego text in which cipher data is hidden into stego text. To get original data, first of all steganography process is applied on stego text. From this process, the cipher data will be obtain. Then again BLOWFISH Algorithm is applied on this cipher data to be decrypted to obtain the original data. In our whole proposed work steganography process will be done using Character and String Mapping approach.

### Blowfish Algorithm

Blowfish has a 64-bit block size as shown in figure 2 below and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes(“Academic: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) - Schneier on Security,” 1995). In blowfish algorithm a 64-bit plaintext message is first divided into 32 bits. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

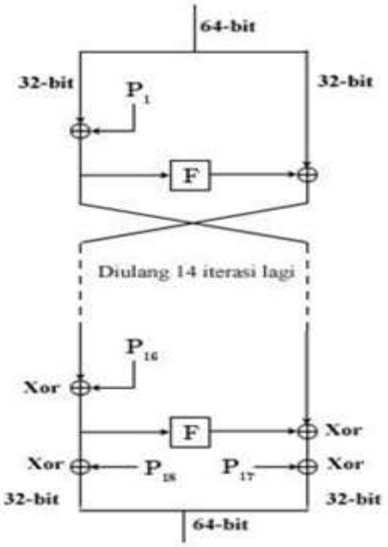

***Figure 2: Blowfish Algorithm***

The F-function as we can see in figure 3 below splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. This is not so obvious because xor is commutative and associative.

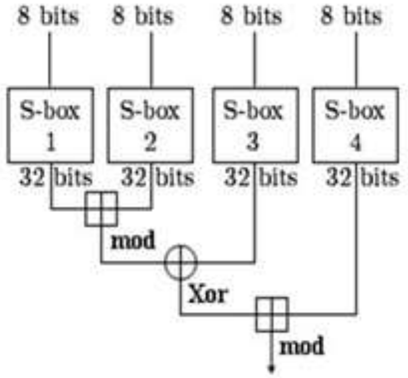

***Figure 3: Work of F-function in Blowfish***

## Character and String Mapping Approach

This method alters a font attribute, called the *character spacing*, in the cover document to embed the secret. It generates a list of 28 strings, each of length 7, using the 26 English alphabets, dot and space characters. All the 26 alphabets of English, dot and space characters are mapped to these generated 28 strings. To embed a secret character, the string that is mapped to the respective character is identified. The cover document is then scanned, serially, for the occurrence of any character in the identified string. The position of the occurred cover character, in the identified string, decides its character spacing. Since a single secret character can be embedded in any of the 7 characters of the identified string, this technique automatically handles the limitation of the non-uniform occurrence of characters in an English text.

## Simulation Tools

The proposed system will be implemented using java programming as language and Net Beans IDE 8.0.2 as the programing environment. A HP lap-top System with Core i (TM) i5-4200U, 2.30GHz CPU and 8GB RAM as hardware requirement will be used as well.

## Conclusion and Future Work

This work proposed a technique to protect user data in the cloud using Blowfish Algorithm as cryptography by encrypting the data from unauthorized users and then concealing it using Text steganography in order to achieve a secure communication in the cloud. After the work has been achieved successfully, a performance analysis will be conducted in the future with other systems designed using a combination of cryptography and steganography techniques.

## References

Abdulkarim, A. I., & Souley, B. (2017). *An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography*. *8*(7), 1512–1517.

Academic: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) - Schneier on Security. (1995). *Dr. Dobb's Journal, April 1994*, *v.19*(n. 4), 38–40. https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html

AL-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., & Alanazi, H. O. (2010). *Overview: Main Fundamentals for Steganography*. *June 2014*. http://arxiv.org/abs/1003.4086

Garrison, G., Wakefield, R. L., & Kim, S. (2015). The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. *International Journal of Information Management*, *35*(4), 377–393. https://doi.org/10.1016/j.ijinfomgt.2015.03.001

Gowda, S. N. (2016). Using Blowfish encryption to enhance security feature of an image. *Proceedings of the 6th International Conference on Information Communication and Management, ICICM 2016*, *200*, 126–129. https://doi.org/10.1109/INFOCOMAN.2016.7784228

Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017). An overview of text steganography. *2017 4th International Conference on Signal Processing, Communication and Networking, ICSCN 2017*, 0–5. https://doi.org/10.1109/ICSCN.2017.8085643

Kumari, M. S., Pathak, P., & Madan, M. I. (2017). Techniques for Securing the Data in Cloud Computing. *International Research Journal of Engineering and Technology(IRJET)*, *4*(5), 742–745. https://www.irjet.net/archives/V4/i5/IRJET-V4I5146.pdf

Nath, J., & Nath, A. (2011). Advanced Steganography Algorithm using Encrypted secret message. *International Journal of Advanced Computer Science and Applications*, *2*(3). https://doi.org/10.14569/ijacsa.2011.020304

Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015). Cloud computing features, issues, and challenges: A big picture. *Proceedings - 1st International Conference on Computational Intelligence and Networks, CINE 2015*, *Cine*, 116–123. https://doi.org/10.1109/CINE.2015.31

Sharma, H. (2013). Secure Image Hiding Algorithm using Cryptography and Steganography. *IOSR Journal of Computer Engineering*, *13*(5), 01–06. https://doi.org/10.9790/0661-1350106

Srivastava, P., & Khan, R. (2018). A Review Paper on Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(6), 17. https://doi.org/10.23956/ijarcsse.v8i6.711

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2018). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, *2018-Janua*, 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215