A Secure Communication With One Time Pad Encryption And Steganography Method In Cloud

Lalit Kumar[1], Sanjeev Kumar Mandal[2], Srinivasan S[3], Omkar Singh[4], Sabari Giri Murugan[5]

[1]Assistant Professor, Department of Computer Science & Information Technology, Jain University, Bengaluru Karnataka, India
[2]Assistant Professor, Department of Computer Science & Information Technology, Jain University, Bengaluru Karnataka, India
[3]Assistant Professor, Department of Computer Science & Information Technology, Jain University, Bengaluru Karnataka, India
[4]Assistant Professor, Department of Computer Science, Bareilly College, Bareilly UP
[5]Assistant Professor, Department of Computer Science & Information Technology, Jain University, Bengaluru Karnataka, India
[1]k.lalit@jainuniveristy.ac.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Cloud computing is a framework for suitable on demand network admittance to a mutual pool of computer resources. Cloud computing is a model for delivering services as per the demand related to information technology over the internet. It is a type of internet-based computing by which client pay for using the services. A client sends a request to the cloud server, server respond to his request and deliver on demand services. The inflamed attack in the cloud surface makes it extra susceptible to prevailing and emerging security threats. Predictable cloud data prevention and security approached have been initiated unable in anticipation of such threats and this distasteful trend has compelled the need of revolutionary approach to cloud data security. Blowfish Encryption and Steganography already had established techniques of data security. This Research work possess an amplify approach to safeguarding data security by combining both of the proven techniques. The united methodology is aimed to leveraging the strength of these two proven techniques to attain a robust mechanism of confirming security in cloud data.

Keywords: Cloud computing, Cryptography, Steganography.

1. Introduction

Cloud computing is a innovative internet based computing technology that has gradually established in past years. [1] The idea behind cloud computing is to empower users or organizations to access computing resources via internet and pay per use model, the same way client pay for electricity, water and related services of daily life. [2] Cloud computing defined a framework for delivering services related to IT on internet according to user requirement. [3] Cloud computing approach affords various benefits to cloud users as well service providers. Adoption of cloud computing has been by security concerns and others challenges like performance service quality and integration. It essential to ensure prevention of cloud data is imperative and it motivated researches in cloud computing communities to develop mechanism to safeguard availability confidentiality and integrity.

An important aspect of data security is quality of services, cloud computing inescapably postures new challenging security threats for a number of reasons which are concentrated on the individuality of cloud computing concept. As we all know that data stored in cloud is in black box process i.e. cloud user does not know that where is data stored and how data can be utilized by third party. [4] The aim of cloud data security is to ensure data is sufficiently secured for its life cycle. Therefore, contending such threats would require more than the outmoded cryptography primitives. This paper suggests an approach using grouping of steganography and blowfish to preserve security of data in the cloud.

A. Cloud Computing Overview

Sidhu and Kinger [5] define, the emerging computing paradigm in information technology is cloud computing (CC) that is an evolving technology exemplar. The aim of cloud computing is share data, service transparently and calculation over data in the network. Meanwhile cloud computing store the data and distributed resources in open environment. The amount of data storage in cloud increases quickly. Usually, there is no regular definition of cloud computing. However, it comprises of a cluster of distributed servers known as masters, providing demanded services to dissimilar user known as client in a network with reliability and scalability of data center. CC has four disposition replicas.

1. Public Cloud

These usually proved services to general public including operation, application and storage of data. Such service may be free or accessible as expense as per use.

2. Private Cloud

Private cloud normally provides services to the single organization. This cloud not accessible by general public i.e. VMware Private Cloud, Microsoft Private Cloud.

3. **Community Cloud**

These collective its arrangement among numerous organizations with shared consent of clients including prerogative and compliance etc.

4. **Hybrid Cloud**

It is the mixture of two or more than two cloud such as public and private or private and unrestricted etc.

B. Cloud Computing Deployment Models

There are usually three service model of cloud: Software as a Services, Platform as a Services and Infrastructure as a Services as shown in Figure-1.

1. Software as a Services (SaaS)

It is the very common model in which cloud suppliers connect and function software in cloud. Most of the applications of cloud support precise client software committed to these application such as Email, Virtual desktop etc.

2. Platform as Services (PaaS)

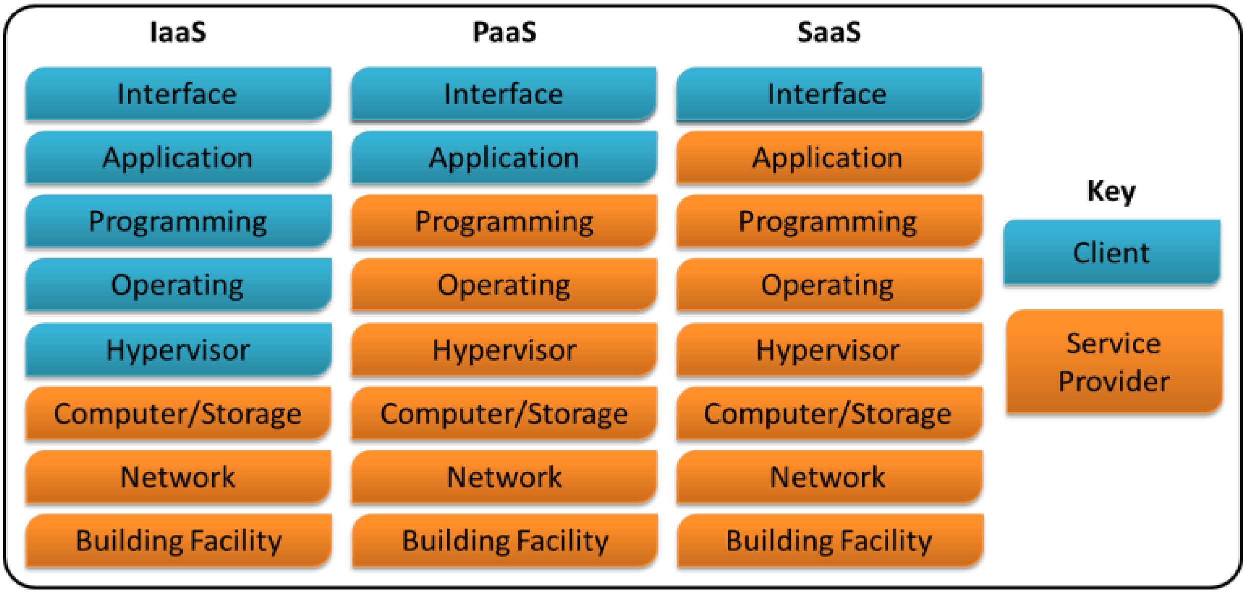
Cloud providers run a computing platform containing execution environment, operation system, programming language, webserver and database etc. Application developer can advance and execute the software on cloud. Some implemented open sources platform as a service providers are Open shift origin, cloud foundry etc.

3. Infrastructure as Services (IaaS)

These cloud providers provide their infrastructure (data base, hardware etc) to the cloud user. Cloud provider offer computer as a virtual machine and resources. Virtual machine runs as guest by a hypervisor such as Kvm or Xen. Iaas also provide images as resources in cloud such as virtual machine library, file based storage, firewalls, block storage, load balancing and much more.

C. Cloud Security Responsibilities

The inflamed attack surface intrinsic in cloud surface makes it problematic to regulate who is predominantly accountable for securing dissimilar software and hardware tools that establish the deployment model. The CS provider tends to place accountability for securing the cloud data on the client but most of the client shoulders security accountability is totally provided by the service provider. The shared accountability between the user and the service providers to define who is responsible for securing data in the cloud totally depends on deployment model. For achieving this aim the cloud Special Interest Group of the Security Council Propagated a matrix of responsibilities [6]. This has been somewhat modified to programming tools given in Fig.1.



IaaS	PaaS	SaaS
🟦 Interface	🟦 Interface	🟦 Interface
🟦 Application	🟦 Application	🟧 Application
🟦 Programming	🟧 Programming	🟧 Programming
🟦 Operating	🟧 Operating	🟧 Operating
🟦 Hypervisor	🟧 Hypervisor	🟧 Hypervisor
🟧 Computer/Storage	🟧 Computer/Storage	🟧 Computer/Storage
🟧 Network	🟧 Network	🟧 Network
🟧 Building Facility	🟧 Building Facility	🟧 Building Facility

Key

🟦 Client

🟧 Service Provider

Fig. 1 Modified Cloud Security Responsibility Matrix

D. ***Cryptography Techniques***

Cryptography techniques can be described as follows:

1. ***Rivest-Shamir-Adleman (RSA)***

RSA is known as finest cryptography algorithms which work on public key altercation, digital signature and encryption of data. It uses variable key size and variable size encryption block. RSA grounded on asymmetric cryptography system based on number theory known as block cipher system [7].

2. ***Data Encryption Standard (DES)***

This algorithm is broadly acknowledged and publically available encryption system advanced by IBM in 1970 but was future espoused by NIST as Federal information Processing Standard 46 [8.There are many method and attacks logged those abuse the weaknesses of DES, which made it little unsecure [9].

3. ***Advanced Encryption Standard (AES)***

AES swap DES in 2001. [10] AES has the ability to support any arrangement of data and key length, as its key length throughout the progression of encryption and decryption, the procedure of AES spirits to 10 circles for 128 bits

key, 12 rounds for 192 bits key and 14 rounds for 256 bits key in order to delever concluded cipher or to regain the original plain text.

4. Blowfish Algorithm

Blowfish is used for preservation of data and encryption using symmetric block cipher process. It uses 32 bits to 448 bits as its variable length key and made it ideal for data prevention.It is an open and non-patented algorithm thus it is freely available for all users [11].

5. TwoFish Encryption

Twofish is used for preservation of data and encryption using symmetric block cipher process. TwoFish awarded one of the finalists among top five algorithms in Advance Encryption Standard contest. Unfortunately it was not selected for standardization. Twofish is the next step of Blowfish algorithm. Twofish uses S-box independently as pre computed key and schedule of respective complex key. Twofish divide entire plain text into two equal parts. It is also used in feistel network like DES. Maximum Distance Separable Matrix is used by Twofish algorithm.

[12, 13] Twofish is somewhat slower than AES for 128bits key but slightly faster for 256bit keys on most of the plateforms.

Table 1: Comparison of Encryption Algorithms

Algorithms	**Proposed By**	**Key Size**	**Bloc k Size**
RSA	Rivest, Shamir & Adelman in 1978	128	64
DES	IBM IN 1975	56	64
AES (RAJINDAL)	Joan Daemen & Vincent Rijmen In 1998	256	128
Blowfish	Bruce Schneier In 1993	32-448 128 by Default	64
TwoFish	Bruce Schneier In 1998	256	128

E. Steganography

Steganography is the technique of hiding data from outside the world. It uses object (Carrier), Message and password to produce stego object. Cover object is a message that is to be sent [7]. Cover object is the data that dispatcher desires to continue it secret and hidden from the outside world. In this model data may be hiding in any image, autio or video [14]. Cryptography is known as secret writing while steganography know as hiding of data [15].There are so many techniques for hiding the data of message in such fashion that the modification done to image is perceptually imperceptible: Steganography methods are: Least Significant Bit (LSB), Covering, Filtering and Transformation.

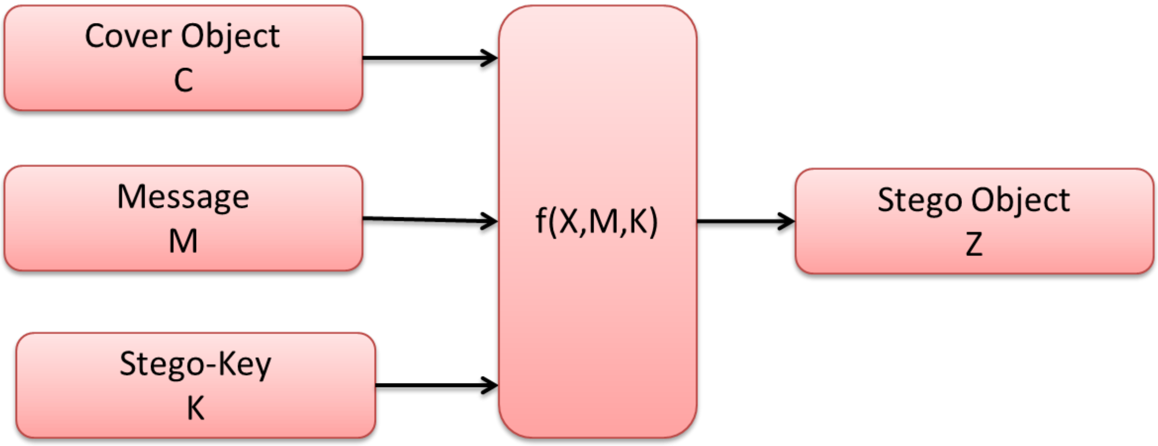


Fig. 2 Model of Steganography

2. Related work

Steganography and Cryptography have a common objective to ensure the protection of data by hiding and secrecy respectively. These techniques widely used in previous researches and also tested and approved to protect sensitive data. Cryptography and Steganography share common objectives of ensuring adequate protection of data. In literature survey there are many approaches to secure data in the cloud.

Gurjeevan Singh et. al [17] discusses Cryptography algorithms play an effective and key role in data protection. They provide evaluation of cryptography algorithm such as AES, DES, Blowfish RC 6. They conducted a comparison among these encryption algorithm and they found that blowfish is the winner algorithm. In the final result blowfish has best performance than others shared encryption algorithm.

Ranjeet Masram et al.[18] states that electronic data which is most confidential is circulated in the network for achieving faster communication. Cryptographic algorithms uses cipher text for providing confidentiality and security of data against malicious or attacks. However security is an important factor and some other factors also can affect the performance and selection of encryption algorithms during the implementation of such cryptography cipher for different application. They analysis and comparison of encryption algorithm RC4, AES, Blowfish, RC2, DES, 3DES.

Garima and Naveen [3] states that the key feature of steganography over cryptography is secret data not get attention to itself as message can be concealed under the image, audio or video files. They describe that steganography is the best data hiding methodology when cryptography is not acceptable. Yuri et al, [19] explained and represented the framework of cloud centered infrastructure service provisioning. They also suggested an architecture that facilitate cloud services such as integration and interoperability for inter cloud environment.

Selvn et al. [20][21] conversed some issue of data storing and data security in the cloud. They concluded some steps after implementing: 1) displacement strategies for new data, 2) service level agreement between service provider and client and verification of service quality. Sharon et al. for further inters cloud security infrastructure development. Rajiv et al. [23] projected a method, which is the amalgamation of identity based encryption (IBE) and facilitated RSA methodology for ensuring secure cloud environment.

Table 2: Comparison of Encryption Algorithms

Proposed Approach	**Merits**	**Demerits**
EMK[1]	Significant data associated, provides sufficient storage and sharing.	Required effective training and education for applying strategy.
AES[3]	Improves pixel assortment of image, detection information of multifarious	Need more security in steganography compress shrink.
ADK[4]	Generate master secret key, verified original data, finger print authentication exist	Enhances data index and space complexity.
HMR[5]	Balances network load, aware network category, designed for specific applications	Need high metrics cost
EMG[6]	Provides cloud storage services, enables digital physiological system.	Sometimes information is not confidential.
ACE[7]	Satisfy security standards, enables access control encryption	Issue of verifiability in cipher text.
ECC[8]	Improves processor and memory usage, reduces power consumption	Whole communication is not secure.
3DES[10]	Improves cost performance trade off, best fit in many crucial applications	Security strength is not much complex.
Blowfish [11]	Improves encryption time and throughput	Authentic mechanism is limited only few applications.

CTR[12]	Secures network cards, suitability in symmetric block	High time complexity.
MSE[13]	Maximizes embedded capacity, improves image steganography	LSBs do not perform well.
A[14]	Designed a framework for steganography	Adversary cannot distinguish
PSNR[15]	Improves cover objet and stego-object, provides secure communication	Spatial and frequency domain are much complex.
A[16]	Improves data link encryption	Need to improve data system and process
STRIDE[21]	Identify potential threats, and provides traceability	Need extra power and resources
CDS[23]	Audit variable size and block in public cloud	Enhances computational overhead.

Proposed approach

In day-to-day life internet is very important for everyone all almost all the work is done with the help of the internet, like online payment, shopping, browsing, data storing, etc.., there are many attacks are possible when we are using the internet, like Man-in-middle attack, mathematical attack, timing attack, etc., therefore keeping Confidential information in Cloud or online database is not secure. To overcome this, in the proposed method cryptography and stenography technique have been used to hide the confidential information for further communication.

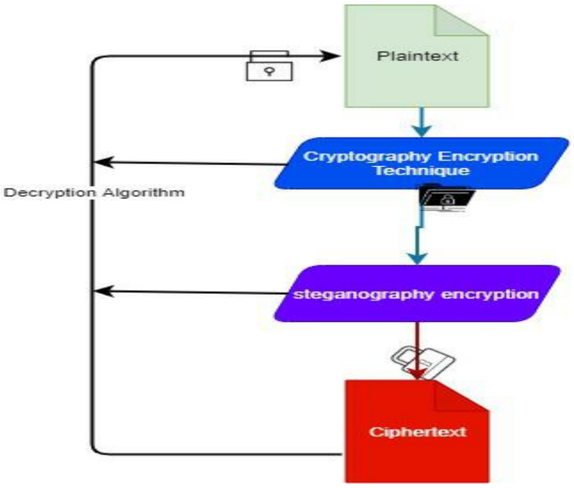


Fig 3: Encryption Process in Proposed Model

A. Implementation

First Encryption: Cryptography Method Let consider the word "CONOFO" as confidential information and is converted into a numeric value representation

Plaintext	C O N O F
Numeric Value	3 15 14 15 6

Key	C R Y P T
Numeric Value	3 18 25 16 20

Encryption is done with the help of,

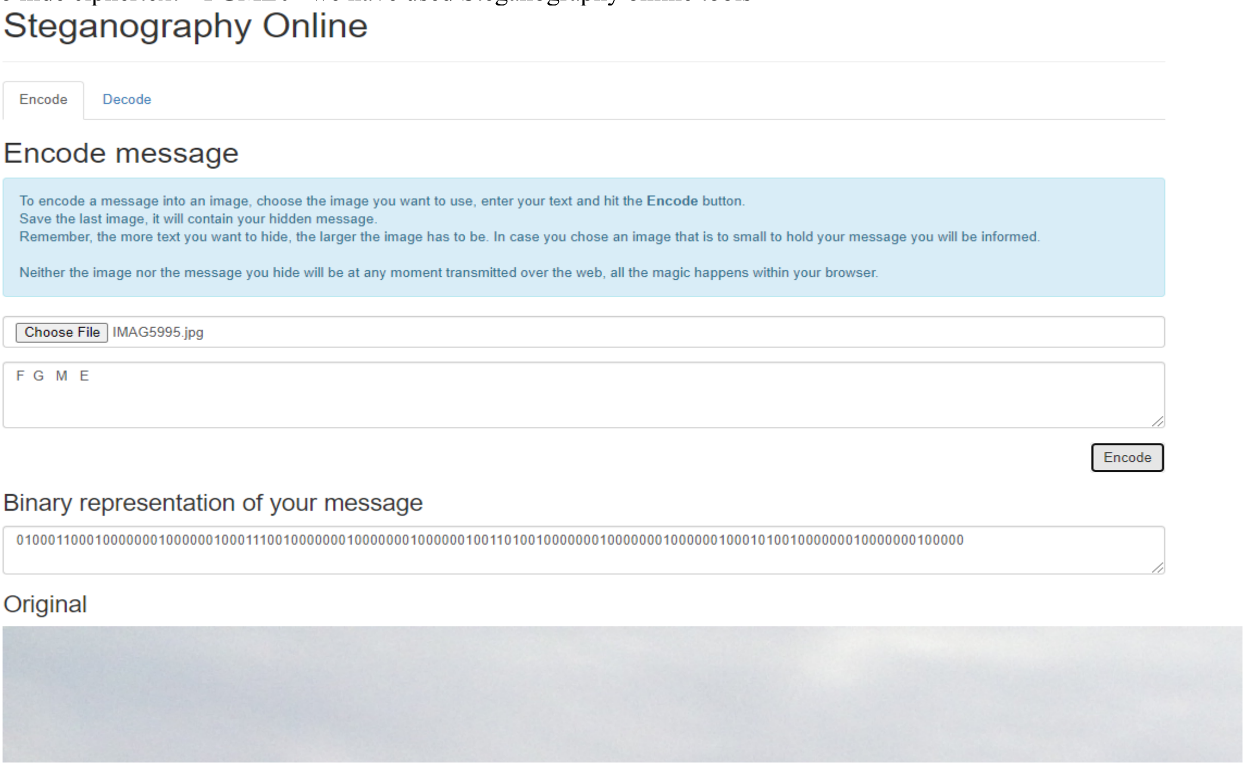
$$P_i + K_i \bmod 26 = C_i$$

C + C = 3 + 3 = 6 mod 26 = 6
O + R = 15 + 18 = 33 mod 26 = 7
N + Y = 14 + 25 = 39 mod 26 = 13
O + P = 15 + 16 = 31 mod 26 = 5
F + T = 6 + 20 = 26 mod 26 = 0

After performing the first encryption Ciphertext is:

Ciphertext	6 7 13 5 0
Alphabetic representation	F G M E 0

Second Encryption: Steganography Method
To hide ciphertext " FGME0" we have used Steganography online tools



Steganography Online

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.
Save the last image, it will contain your hidden message.
Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is to small to hold your message you will be informed.

Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

IMAG5995.jpg

F G M E

Binary representation of your message

```
0100011000100000000100000010001110010000000010000000100000010011010010000000010000000100000010001010010000000010000000100000
```

Original

Fig 4: Encryption Using Stenography

Finally Ciphertext us hidden behind this image

Fig 5: Encrypted with Stenography

Upon receiving an image to obtain Plaintext decryption is performed in a reversed way

3. Conclusion

This paper deliberated the cloud computing concept and its possible security risks based. Various prevailing mechanisms for data security in the cloud were also evaluated and then a unified methodology for safeguarding data integrity and confidentiality was anticipated. The proposed approach is a combination of two tested and proven techniques: cryptography and steganography, to achieve a unified data security mechanism. The awareness of spreading this proposed method by uniting a cryptography algorithm with steganography would extant absolute crushed for future research. This is because holomorphic cryptography is endowed with the potential to support computations on encrypted data without the need for prior decryption of such data. This would significantly improve the confidentiality of both data-at-rest and data-in-transit within the cloud environment.

References

A. IbrahimArpaci,(2017) “Antecedents and consequences of cloud computing adoption in education to achieve knowledge management”, Computers in Human Behavior, vol. 70, pp. 382-390.

B. S. Garima, and S. Naveen (2018), “Triple Security of Data in Cloud Computing”, International Journal of Computer Science and Information Technologies, Vol. 5, No. 4, pp. 5825-5827.

C. Pratiksha Sethia , V. Kapoor, (2016) “A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography”, International Conference on Computational Science, pp. 61-66,

D. S. Shanthi , R.Jagadeesh et. al., (2018) “Efficient secure system of data in cloud using steganography based cryptosystem with FSN”, Elsevier Materials Today: Proceedings, vol , pp. 1967–1973,

E. E. Jafarnejad, G.A.Masoud and R.N.Qader, (2017) “Load-balancing algorithms in cloud computing: A survey”, Journal of Network and Computer Applications, vol. 88, pp. 50-71,.

F. ShiuHung-Jra,LinBor-Sing et. al., (2017) “Preserving privacy of online digital physiological signals using blind and reversible steganography”, Computer Methods and Programs in Biomedicine, vol. 151, pp. 159-170.

G. HuigeWanga, KefeiChen et.al, (2018) “Access control encryption with efficient verifiable sanitized decryption”, Information Sciences vol. 465, pp. 72-85.

H. Natassya B.F.SilvaaDaniel F.Pigatto et. al., , (2016) “Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer”, Journal of Network and Computer Applications, vol. 60, pp. 130-143.

I. A. K. Sidhu, and S. Kinger, (2018) “Analysis of Load Balancing Techniques in Cloud Computing”, International Journal of Computers & Technology, Vol.4, No. 2, pp. 737-741.

J. Priyadarshini,PatilaPrashant,Narayankar et. al., 2016 “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish”, Procedia Computer Science, vol. 78, pp. 617-624.

K. Manju Suresh and Neema M.b, (2016), “Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things”, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016), vol. 25, 248-255.

L. David Smekal, Jan Hajny, Zdenek Martinasek, (2018) “Comparative Analysis of Different Implementation of Encryption Algorithm on FPGA Network Card, IFAC Conference Elsevier, vol. 51-6, pp. 312-317.

M. Xin Zhou and Xiaofei Tang, (2017) "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121.

N. Mamta Jaina , Saroj Kumar Lenka and Sunil Kumar Vasistha, (2016), “Adaptive circular queue image steganography with RSA cryptosystem”, Recent Trends in Engineering and Martial Science, vol. 8, pp.417-420.

O. MaciejLiśkiewicz, RüdigerReischuk and UlrichWölfel, (2017) “Security levels in steganography – Insecurity does not imply detectability”, Theoretical Computer Science, vol. 692, pp. 25-45.

P. P.Malathi and T.Gireesh kumar, (2016) “Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains”, 6th International Conference On Advances In Computing & Communications, vol. 93, pp. 878-885.

Q. SalmanIqbala, LaihaMat Kiah et.al., (2016) “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service”, Journal of Network and Computer Applications, vol. 74, pp. 98-120.

R. Akashdeep Bhardwaj, GVB Subrahmanyam et. al., (2016) “Security Algorithms for Cloud Computing”, International Conference on Computational Modeling and Security, Elsevier, vol. 85, pp. 535-542.

S. Gabriel G.Castañé, Huanhuan Xiong et.al., (2018) “An ontology for heterogeneous resources management interoperability and HPC in the cloud”, Future Generation Computer Systems vol. 88, pp. 373-384.

T. Qin Liu, Guojun Wang et. al., (2017) “Achieving reliable and secure services in cloud computing environments”, Computers & Electrical Engineering, vol. 59, pp. 153-164.

U. Jin B.Hong, Armstrong Nhlabatsi et.al., (2018) “Systematic identification of threats in the cloud: A Survey”, Computer Networks, vol. 150, pp. 46-69.

V. John O’Loughlin, Lee Gillam et. al., (2018), “A performance brokerage for heterogeneous clouds”, Future Generation Computer Systems, vol. 87, pp. 831-845.

W. Yong Yu, Liang Xue et.al, (2016), “Cloud data integrity checking with an identity-based auditing mechanism from RSA”, Future Generation Computer Systems, vol. 62, pp. 85-91.

X. Sanjeev Kumar Manda. (2018) "A Secure Cryptosystem by using Euler Totient Function and Modified RSA.” IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10, pp. 01-07.

Y. Sanjeev Kumar Mandal, A. R. Deepti, Lalit Kumar, and M. N. Nachappa, (2020), “An Improvised Caesar Cipher Technique for Enhancing Data Security, International Journal of Advanced Research in Engineering and Technology 11(11), pp. 1304-1313.