# DATA SECURITY MANAGEMENT IN CLOUD COMPUTING

Dr. Reshma Banu[1], Apoorva.R[2], Madhushree.P. K[3], Sahana. N.P[4], Sushmitha.N[5]

Professor, Department of Computer Science and Engineering 1

B.E Students, Department of Computer Science and Engineering2,3,4,5

Vidya Vikas Institute of Engineering and Technology, Mysore, India

## ABSTRACT:

Cloud Computing is a collection of various internet services like servers, storage, databases, networking, software, analytics and intelligence and by employing Cryptographic algorithms in cloud computing the user can store and access data in a secure and protective way so that no third part can access and make changes to the user's data. Cryptography handles protection of critical data where the data is no longer under the control of user. In this paper we use AES algorithm to assure that the data is ciphered and is kept safeguarded. This would counteract undesirable interruption into individual information and absence of institutionalization, for example one specialist co-op may have start to finish encryption while others don't. This paper deals with the use of AES algorithm in PaaS cloud computing service. By using AES algorithm, the strength of the security is high (90%) when cd to other security services (RSA, DES and hash functions).

Keywords:AES, DES, 3DES, PaaS

## OVERVIEW:

Cryptography is the method and study of mathematically manipulating data so that it can be stored and transmitted securely. The act of manipulating the above-mentioned data is called encryption, and the manipulated data is called encrypted. Encrypted data goes through a process called as decryption, before its original form is revealed. In case the encryption method is logical, then the following encrypted data will not be decrypted in a given amount of time by anyone who does not have a secret token, called an encryption key. Cryptography is the method of converting or encoding of a simple text or data into some unreadable form so that, that data can be read only by an authorized user. This method prevents the mishandling of the data by any foreign or unauthorized user. It provides privacy and security of the data. There are three types of cryptographic techniques that are used to encode data. Cryptography is additionally utilized in distributed computing to verify the online information.

Distributed computing is a procedure of conveying on the web transmission and capacity of information benefits in which assets are recovered from the Internet through electronic devices and applications, instead of an immediate association with a server. Instead of keeping records on an exclusive hard drive or nearby stockpiling gadget, cloud-based storage enables a client to spare information to a remote database. Distributed computing is anything but a solitary bit of technology rather, it's a framework, principally included three administrations: foundation

as an administration (IaaS), programming as an administration (SaaS) and stage as an administration (PaaS

The users can now freely transfer, store or access data online without any fear of their data being hacked by any other user. The introduction of keys such as public and private keys further increases the security of text or data

In the cloud the data is not under anyone's control and so that data is vulnerable to hacking and being accessed by an unauthorized user. In such a case, Cryptography in cloud computing ensures reliability and integrity of online storage and transmission of data.
This paper deals with some efficient functions and methodologies to ensure the data is ciphered and is kept protected.

## Cloud Security with Cryptography:

### 1. Introduction to data security in cloud computing using cryptography

Cloud computing has revolutionized the way businesses and individuals store, process, and access data. It offers the flexibility and scalability to meet the demands of modern computing, but it also introduces new challenges, especially when it comes to data security. As data is stored on remote servers owned by cloud service providers, there is a need to ensure the confidentiality, integrity, and availability of this data. Cryptography plays a crucial role in achieving these goals by providing various techniques to protect sensitive information in the cloud.

### 2. Understanding Cloud Computing:

Cloud computing refers to the delivery of computing resources, such as storage, processing power, applications, and services, over the internet. Cloud service providers maintain data centers and offer these resources to users on a pay-as-you-go basis. This model eliminates the need for local infrastructure and provides users with the flexibility to scale their resources based on demand.

## RELATED WORK:

In the recent years, a lot of research has been performed on how the cryptographic techniques have been used in the area of cloud computing.

In one of the papers [1], the creator explains the significance of security in distributed computing and how encryption can shield correspondences and put away data from unapproved get to. The idea utilized is the procedure of content information that are scrambled in type of figure content to shield information from unapproved get to. The central theme of this examination paper is to grow how secure is the one's data set on cloud and what are the different security issues one should be stressed over when making usage of the cloud. They have utilized the calculation in portraying the way toward coordinating AES into cloud's information security.

In one of the other papers [2] the creator talks about the investigation of information in the cloud and perspectives identified with it concerning security. Accessibility of information in

the cloud is gainful for some applications however it presents hazards by presenting information to applications which may as of now have security escape clauses in them. So likewise, use of virtualization for circulated processing may danger data when a guest OS is continued running over a hypervisor without knowing the faithful nature of the guest OS which may have a security stipulation in it.

One of alternate [3] papers in which the creator analyzes the utilization of ECC in compelled situations where security is the fundamental issue and talks about the premise of its security, investigates its execution and ultimately, overviews the utilization of ECC applications available today is described. The idea depicted is the utilization of FIFO to actualize RR booking and utilizing scientific change to irreversibly scramble data.
In another paper [[4] the creator proposes and executes a calculation which would encode the records transferred on such online distributed storage benefits and would decode the document once it has been downloaded utilizing the keys that were produced amid encryption

In paper [5] published discusses about the symmetric block cipher that can be used as a substitute for DES. The blowfish algorithm has been used and the benefits of blowfish algorithm in domestic and exportable use has been discussed.

In the paper [6] the makers deal with the issue of security of data in the midst of data transmission. The essential worry to fear about this paper is the encryption of data so mystery and security can be successfully cultivated. The estimation used here is Rijndael Encryption Algorithm close by EAP-CHAP.

This paper [7] presents a tradition or set of bearings that uses the organizations of an outcast analyst or checker not only to affirm and approve the reliability of data set away at remote servers yet what's more in recuperating and recouping the data as fast as time allows in immaculate structure.

In another paper [8] the focus is upon the looking over and perception of cloud security issues by proposing crypto counts and amazing measures so as to ensure the data security in cloud. Close by this, we will outline increasingly about some security parts of cryptography by showing some insurance issues of current conveyed figuring condition

# SYSTEM DESIGN:

## 1. System Introduction

Cryptography is characterized as making composed or created codes that enable information to be stayed quiet. Cryptography changes over information into a non-lucid arrangement for an unapproved user (who doesn’t have unscrambling key), enabling it to be transmitted without read or gotten to by unapproved elements and interpreting it once more into a clear organization, thusly giving secure correspondence within the sight of noxious outsiders.

## 2. Various Cryptographic Algorithms

**1) Symmetric-Key Algorithm:** Symmetric utilizations single key, which works for encryption just as unscrambling. It guarantees confirmation and approval. The key is kept as mystery. It works with rapid in encryption. Symmetric-key calculations are partitioned into two kinds: Block figure type and Stream figure type. In bock figure input is taken as a square of plaintext of fixed size contingent upon the sort of symmetric encryption calculation, key of fixed size is connected on to square of plain content and after that the yield figure square of a similar size as the square of plaintext is acquired.

**2) Asymmetric-Key Algorithm:** This calculation is known as open key cryptography and utilizations open and private keys to scramble or unscramble information. The keys referenced is essentially a gathering of extensive numbers that have been combined together however are unidentical (unbalanced). Open key in the pair can be imparted to everybody while the other key in the pair is known as the private key is stayed discreet.

**3) RSA Algorithm:** The calculation was developed by three researchers named Ron Rivest, Adi Shamir, and Len Adleman and hence, it is named as RSA cryptographic calculation. It is Asymmetric encryption Type calculation it implies that open key is disseminated to for encryption and private key is utilized to unscrambling. The key size is 1024 bits. In the RSA measured exponential is utilized for encryption and unscrambling. It utilizes two examples x and y where x is open key and y is private key. Messages hidden with the utilization of open key can be decoded just by utilizing the private key. This private key it is then given to the customer for check of client utilizing the server's known open key.

**4) AES Algorithm:** AES represents Advanced Encryption Standard. It goes under symmetric-key calculation. It is the most utilized and proficient Symmetric-key calculation among others. It was distributed by the National Institute of Standards and Technology (NIST). It is worked on bytes as opposed to bits; it treats 128bits of plaintext hinder as 16bytes. These 16bytes is prepared as a 4-4 framework. The greater part of the computers currently incorporate equipment AES bolster making it quick. Besides, it is the More secure than DES and Most embraced symmetric encryption calculation.

# DATA ENCRYPTION:

AES encryption is the FIPS endorsed cryptographic calculation is utilized to ensure enduring electronic information.

- It is symmetric square figure for encoding and decoding data.

- Encryption part changes over a snippet of data or information into figure content while decoding includes transformation of the figure message back to basic lucid information.

The highlights of AES are –

- Symmetric Key, symmetric square figure • 128-bit information, 128/192/256-piece keys.
- Stronger and quicker than DES and Triple-DES
- Provides full particular and configuration subtleties

AES encryption plays out the majority of its calculations on bytes as opposed to bits. Along these lines, AES treats the 128 bits of a plaintext hinder as 16 bytes. These 16 bytes are orchestrated preparing as a 4x4 network for example in four sections and four lines Unlike in DES, the quantity of rounds in AES is a variable amount and relies upon the length of key.

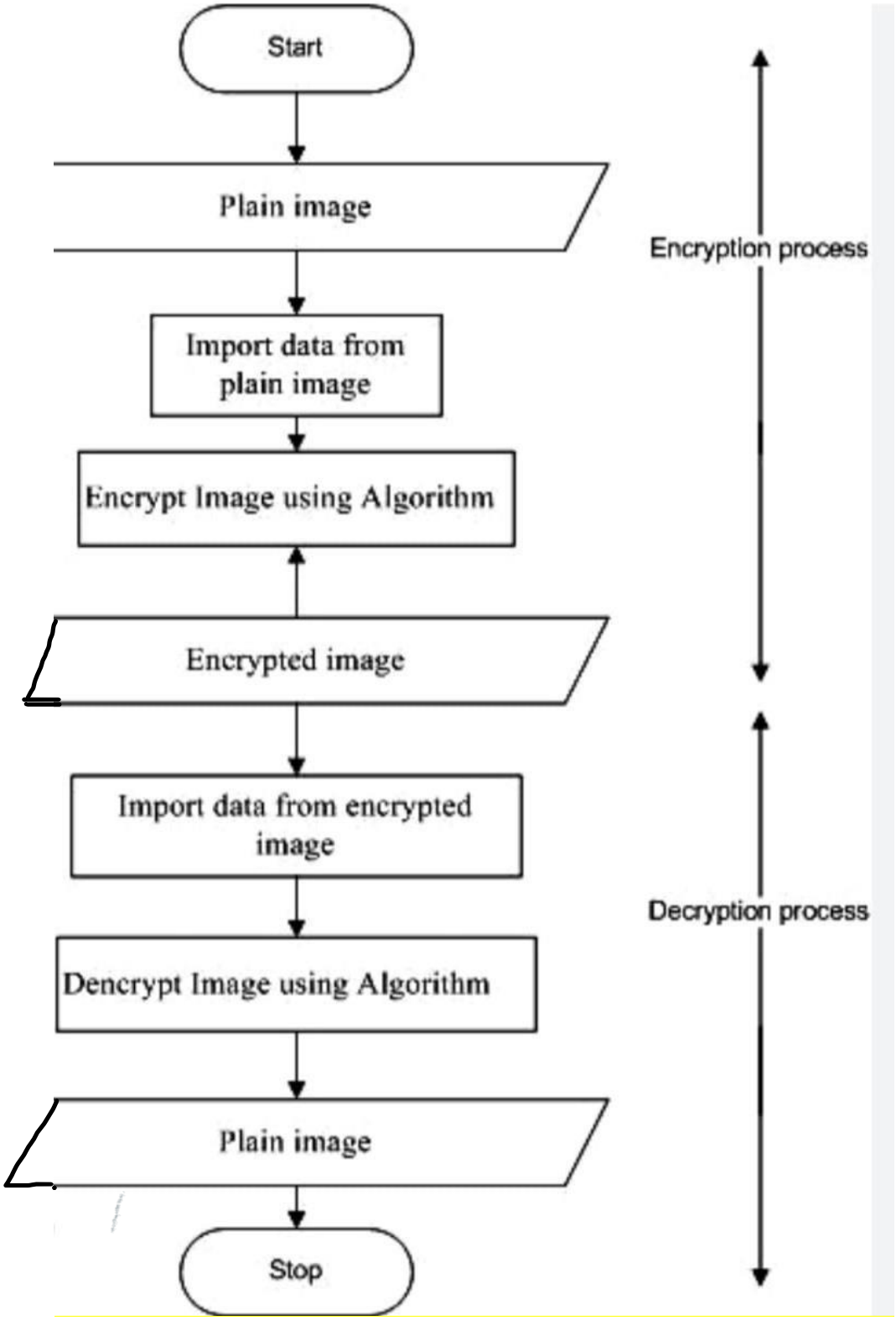
## ENCRYPTION PROCEESS

Here, the process is restricted to mainly the description of a typical round of AES encryption. Each round of encryption comprises of four sub-processes. The first round process is given below as following –

A) Byte Substitution (sub bytes): The 16 input bytes are substituted by looking up a fixed table called the S-box given in the specified design. The resultant product is a matrix of four rows and four columns. Here we have taken 128 as the key size which will have 10 rounds .

B) Shift Rows: Each of the four rows of the 4x4 matrix is shifted one byte row to the left. Any entries that fall off from allocation are re-inserted on the right side. Shift is carried out as follows –

- 1st row isn't shifted to the left but is kept as it is.
- The 2nd row gets shifted 1 (byte) position to the left.
- The 3rd row gets shifted 2 positions (i.e. 2 bytes) to the left.
- The 4th row gets shifted 3 positions (3 bytes) to the left.
- The result achieved is a new 4x4 matrix consisting of the same 16 bytes but shifted to the left with respect to each other. Let the original 4x4 Matrix be N with elements A1 to An.




## GENERAL STEPS IN CRYTOGRAPHY:

1. Choose a Secure Cloud Service Provider: Select a reputable cloud service provider that offers robust security features, encryption options, and compliance with

relevant regulations. Review their security policies and practices to ensure they meet your data security requirements.

2. Data Encryption: Encrypt the data on the client-side before transferring it to the cloud. Use strong encryption algorithms such as AES (Advanced Encryption Standard) to ensure data confidentiality. This way, even if the data is intercepted during transmission, it will be unreadable without the decryption key.

3. Secure Data Transfer: Use secure communication protocols like HTTPS or SFTP for transferring encrypted data to the cloud. These protocols protect data during transit and guard against eavesdropping and man-in-the-middle attacks.

4. Authentication and Access Control: Implement multi-factor authentication (MFA) and role-based access control (RBAC) to ensure only authorized users can access and manage the data stored in the cloud.

5. Use Cryptographic Algorithms on the GUI Platform: If your application uses a graphical user interface (GUI), integrate cryptographic algorithms within the application itself. This can be achieved by leveraging cryptographic libraries and APIs to perform encryption and decryption operations securely.

6. Key Management: Properly manage encryption keys. Store and manage encryption keys separately from the encrypted data to prevent unauthorized access to the keys.

7. Secure Storage: Choose the appropriate storage options provided by the cloud service that offer enhanced security features, like data replication, redundancy, and backups, to ensure data integrity and availability.

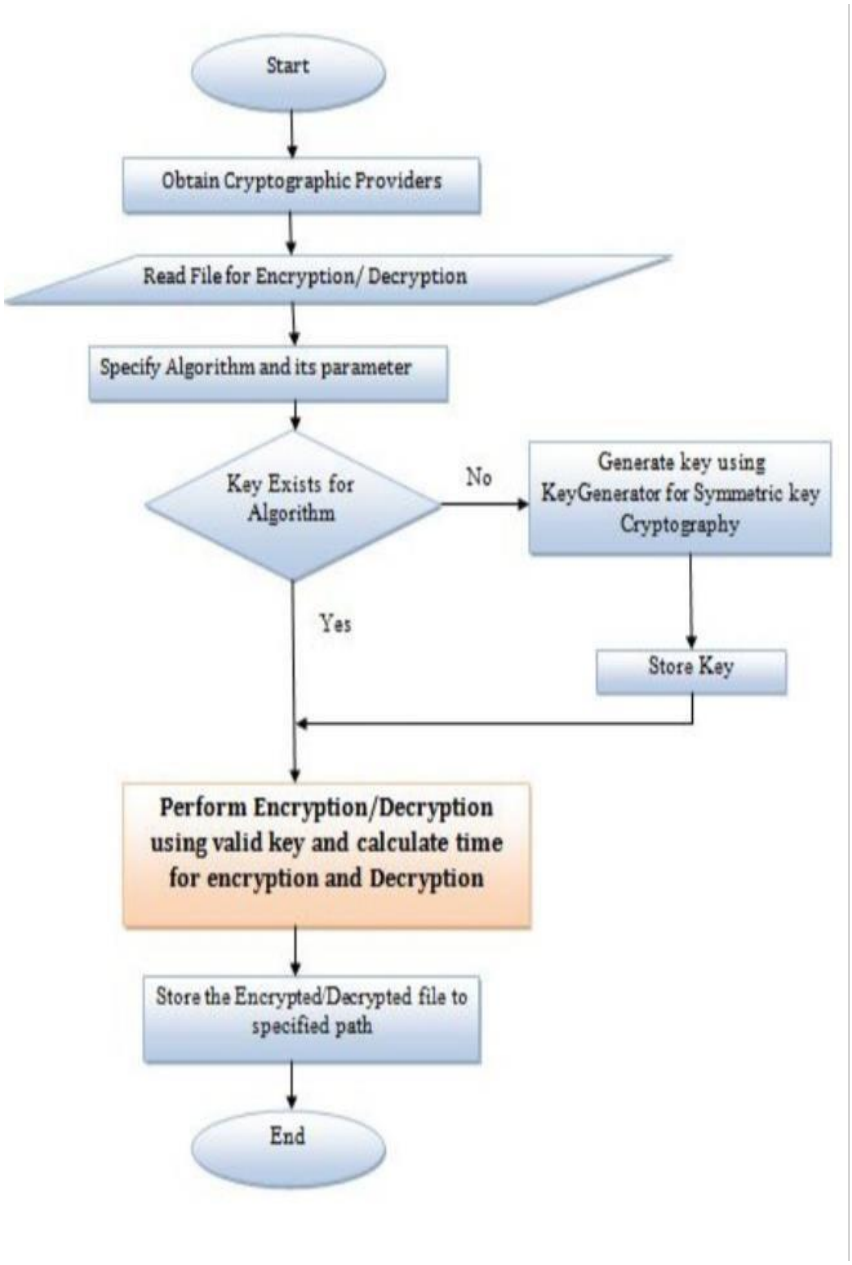
8. Regular Data Backups: Implement a regular backup strategy to maintain multiple copies of your encrypted data in case of accidental deletion, data corruption, or other incidents.

9. Data Lifecycle Management: Define data retention and deletion policies to manage data lifecycle effectively. This helps to minimize the risk of storing unnecessary data in the cloud.
10. Periodic Security Audits: Conduct periodic security audits of your cloud infrastructure and applications to identify and address potential vulnerabilities.

11. Employee Training: Train employees on best security practices, including the proper handling of encryption keys and data access controls.

12. Continuous Monitoring: Implement a monitoring and logging system to detect any unusual activities or security breaches within your cloud environment.

By following these steps, you can enhance the security of your data while transferring it to the cloud and ensure that cryptographic algorithms are applied effectively within your GUI platform. Remember that data security is an ongoing process, and regular updates and improvements are necessary to stay ahead of evolving security threats in the cloud computing landscape.




SYMMETRIC KEY CRYPTOGRAPHY FLOWCHART

## CRYPTOGRAPHY LIMITATIONS:

While cryptography is an essential component of data security in cloud computing, it has its limitations. Some of the key limitations include:

1. Key Management: Cryptographic systems rely on encryption keys to secure data. However, managing encryption keys can be challenging in a cloud environment, especially when dealing with a large number of keys and multiple cloud service providers. If encryption keys are not properly managed and stored securely, it could lead to unauthorized access to sensitive data.

2. Data Breaches: While cryptography can protect data from unauthorized access, it does not prevent data breaches altogether. If an attacker gains access to the encryption keys or exploits vulnerabilities in the cryptographic algorithms, they may still be able to decrypt the data and gain unauthorized access.

3. Performance Impact: Encryption and decryption processes can introduce a performance overhead. In cloud computing, where data is frequently accessed and processed, the computational cost of cryptography can be significant. This may lead to slower processing times and increased latency.

4. Lack of Standardization: The lack of standardized cryptographic algorithms and implementations across different cloud service providers can create compatibility issues and potential security vulnerabilities.

5. Side-Channel Attacks: Cryptographic systems can be susceptible to side-channel attacks, where attackers exploit information leaked during the encryption/decryption process (e.g., power consumption, timing data) to gain insights into the encryption key or decrypted data.

6. User Errors: Even with strong cryptographic measures in place, data can still be at risk due to human errors. For example, if users mishandle encryption keys, use weak passwords, or accidentally expose sensitive data, the data's security can be compromised.

7. Cloud Provider Vulnerabilities: Cloud service providers are responsible for managing the underlying infrastructure, and they may become targets of cyberattacks. If a cloud provider's infrastructure is compromised, it could potentially expose encrypted data or encryption keys.

8. Regulatory Compliance: Depending on the nature of the data and the industry regulations, encryption alone may not be sufficient to meet certain compliance requirements. Additional security measures may be necessary to comply with specific data protection laws.

9. Quantum Computing Threats: While this is more of a futuristic concern, the emergence of powerful quantum computers could potentially break some of the existing cryptographic algorithms, rendering current encryption methods ineffective.

To mitigate these limitations, organizations need to adopt a comprehensive security approach that includes not only strong encryption techniques but also robust key management, access controls, secure coding practices, and regular security audits. It's essential to stay informed about the latest developments in cryptography and security best practices to adapt to evolving threats.

## CONCLUSION:

Data security in cloud computing is of utmost importance due to the increasing reliance on cloud services and the growing volume of sensitive information being stored and processed in the cloud. As organizations continue to adopt cloud solutions for their operational needs, safeguarding data becomes a shared responsibility between cloud service providers and their customers.

To ensure robust data security in the cloud, organizations must adopt a proactive and multifaceted approach. This approach includes implementing strong encryption protocols, enforcing stringent access controls, and employing robust authentication mechanisms. Regular monitoring, logging, and auditing of activities within the cloud environment are vital to detect and respond to potential security incidents promptly.

Furthermore, data segmentation based on sensitivity levels, along with continuous updates and patching, will bolster the overall security posture. Backup and disaster recovery plans are essential components of a comprehensive security strategy, providing the ability to recover data in the event of data loss or breaches.

Organizations should carefully evaluate cloud service providers, ensuring they meet stringent security standards and comply with relevant regulations to safeguard against potential vulnerabilities. Employee training and awareness programs are also crucial in preventing human errors that could lead to security breaches.

## REFERENCES:

[1] ShaffiBansal “Analyzing working of AES and DES algorithm in cloud security”, International journal of research studies in computer science and engineering (IJRSCSE), Volume 4, Issue 3, 2017.

[2] Sajjan R.S and Vishwajit Damblikar "Survey paper on data security in cloud computing", International journal of Computer Sciences and engineering, volume 4, special issue 4, June 2016.

[3] Wendy Chou, "Elliptic Curve Cryptography and its Applications to Mobile Devices", University of Maryland, College Park.

[4] Prerna, Parul Agarwal, "Cryptography Based Security for Cloud Computing System", Volume 8, No. 5, May-June 2017 International Journal of Advanced Research in Computer Science.

[5] Rishav Chatterjee, Sharmistha Roy, "Cryptography in cloud computing: A basic approach to ensure security in cloud", International journal of Engineering Science and Computing, May 2017.

[6] Sanjoli Singla, Jasmeet Singh," Cloud computing security using encryption technique", IJARCET, vol.2, ISSUE 7.

[7] Anjali Arora, "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers", International Journal of Computer Science and Information Technology & Security, 2012.

[8] Bhaskar SM, Ahson SI, "Information Security A Practical Approach", Narosa Publishing House, India, 2008.

[9] Gupta B, Agrawal DP, Yamaguchi S, "Handbook of research on modern cryptographic solutions for computer and cyber security", IGI Global, 2016.

[10] Yogesh M, Rohit K V, Mahipal S , Rajeev K, "Secure Cyber Network to Sharing Information through Cryptography & Stenography". EngTechnol Open Acc. 2019; 2(5): 555598