International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal

eISSN 3108-026X
International Multidisciplinary Research Journal Reviews (IMRJR)
Volume 2, Issue 11, November 2025
DOI 10.17148/IMRJR.2025.021107

A Comprehensive Study on Cryptographic Approaches for Securing Data in Cloud Storage

Dr. B. Fathima Mary

Assistant Professor, Department of Commerce CA, St.Joseph's College(Autonomous), Tiruchirappalli, India

Abstract: Cloud computing is entirely dependent on the internet. Cloud service providers (CSPs) such as Google, Amazon, Salesforce, Microsoft and others store and manage client data in their data centers. Maintaining and keeping an eye on the outsourced data is the responsibility of CSP. Data leakages insecure interfaces resource sharing data availability and inside attacks are just a few of the security problems and threats that can arise from having little control over the data. Security availability performance lack of standards higher usage costs and difficulty integrating with on-premise IT resources are the initial problems. Because they are unaware of where their data will be stored whether it will be available when they need it and whether it will be processed by others a large number of clients do not fully rely on the cloud environment. Cloud security is a significant issue that needs to be taken seriously because cloud users are more concerned with their data. Data security is a major cloud concern. Confidentiality integrity and availability are some of the factors that can help achieve data security. The study also looks at how hybrid frameworks and steganography can enhance authentication and secrecy in cloud environments. In order to improve the security of data while it is at rest a number of algorithms have been investigated.

Keywords: Cloud computing, Cloud Service Provider, Cryptography, Security.

I. INTRODUCTION

Cloud computing is expanding quickly, which has led to greater concerns regarding security issues. The security of data within cloud infrastructure presents a difficult challenge for researchers. Therefore, when developing security algorithms, it is crucial to focus on several factors: the time required for encryption and decryption, the method by which unique cipher text is generated from plain text, and the number of steps involved in transforming plain text into cipher text. The three main parameters used to ensure data security are confidentiality, integrity, and availability. This research focuses on confidentiality as a means to protect data stored in the cloud. Many researchers have worked on improving data security by addressing confidentiality and integrity. Confidentiality can be ensured by allowing only authorized users to access the data[1]. To prevent unauthorized access, data must be either encrypted or masked. Encryption is achieved through cryptographic techniques. This study explains the concept of cryptography, reviews existing work related to cloud security, compares various current techniques, and discusses ongoing challenges and potential areas for future research.

II. OVERVIEW OF CRYPTOGRAPHY

Cryptography is both an art and a scientific field that focuses on methods for securely storing and transmitting information over the internet, especially when there are third parties involved. Information can be encoded in a way that only authorized individuals can understand it, making it accessible only to those intended. Cryptography is divided into two main types: symmetric and asymmetric key cryptography. The original message that is sent or stored is referred to as plaintext, while the transformed version after applying encryption is known as ciphertext. The process of converting plaintext into ciphertext is called encryption. Decryption is the opposite process, which converts ciphertext back into plaintext. Encryption involves using a specific algorithm along with a key to transform the input data into a format that is not easily readable. In cryptographic systems, the use of encryption and decryption keys is fundamental [2].

II. RELATED WORKS

Goswami et al. [3] proposed a mechanism to improve the data security in the cloud environment. This technique used matrices along with public key cryptography, which is divided into two parts. The first part of this technique deals with the shuffling of data, key generation, and key agreement.

Arockiam et al. [4] introduced a symmetric encryption algorithm aimed at securing data in cloud environments. They constructed a square matrix based on the number of characters in the plaintext. This matrix was then divided into three separate matrices: the upper matrix, the diagonal matrix, and the lower matrix. Each of these matrices was encrypted using distinct keys, and the resulting encrypted matrices formed the cipher text. This method is specifically designed for encrypting non-numerical data.

Zhonghan et al. [5] proposed a method called Hadoop Distributed File System (HDFS) to protect data from unauthorized access. HDFS divides the data into blocks of fixed size. This approach uses symmetric encryption, specifically the Advanced Encryption Standard (AES) algorithm, to both encrypt and decrypt the data blocks. Sanjoli et al. [6] developed an architecture aimed at improving the security of data that is stored at rest. Their design incorporates the Challenge-Handshake Authentication Protocol (CHAP) for verifying user identity and the Rijndael Encryption Algorithm, which is a type of iterated block cipher, for securing the data.

Rajkishore et al. [7] introduced a Vedic tool called Sri Ramshalakha. This is a square matrix composed of akshar, which are characters taken from nine verses. The encryption method used to create Sri RamShalaka is based solely on the transposition principle. Manas et al. [8] developed a Spiral Matrix Based Bit Orientation Technique (SMBBOT), which is a symmetric encryption method. In this technique, the plain text is treated as a sequence of bits and divided into smaller, manageable blocks. The square matrix is then rotated clockwise, and the bits are read column by column to form the cipher text.

Prakash et al. [9] developed an efficient method for encrypting sensitive data using a block cipher. In this approach, the data is split into fixed-size blocks, and each block is processed individually. The characters within each block are converted into their binary form and stored in a circular array. To enhance security, the circular array is then rotated using a circular array shifter. This circular array plays a crucial role in both the encryption and decryption processes.

Enhancement of data storage security in the cloud using steganography was developed by Mrinal Kanti Sarkar et al. [10]. The entire file is divided into three parts, and the data in each part is stored within corresponding images. The number of images required depends on the size of the data files. The way the file is divided is based on the size of the images and the content of the file. The method involves storing each character in the last bit of consecutive 8 pixels. These images are then stored in the cloud data center, and without proper identification, no one can access or view the original data content.

Padmanaban et al. [11] developed a security framework that integrates different cryptographic methods aimed at preserving security. They introduced a two-step authentication process, which includes a password authentication mechanism and the generation of digital fingerprints as part of their approach.

Vanaja et al. [12] introduced a symmetric encryption algorithm aimed at addressing security and privacy challenges in cloud storage environments to ensure the confidentiality of data stored in the cloud. The process begins by converting plain text into its corresponding ASCII values, after which a modulus operation is applied. A binary search tree is then constructed based on these values, utilizing pre-order and in-order traversal techniques. For encryption, distinct keys are employed at various levels of the tree. Ultimately, the ASCII values are transformed back into character form, which constitutes the encrypted message or ciphertext. This encrypted data is then stored in the cloud, thereby safeguarding it against unauthorized access. In a separate study, Komal S. Landge et al. [13] developed a hybrid secure storage framework for cloud computing, enabling organizations to store their data securely within a public cloud environment. In this framework, the data owner is responsible for encryption, while cloud users carry out the decryption process. The Rijndael algorithm, a widely recognized symmetric key encryption standard, is utilized for encrypting the data.

Sarika [14] proposed a method that employs a two-tier security approach, combining the Vigenere cipher algorithm and the Reverse circle cipher algorithm, along with a symmetric key multi-rotational technique. The Vigenere cipher is a basic polyalphabetic variant of the shift cipher, where the ciphertext is generated through modular addition. This algorithm also incorporates circular substitution combined with reversal transposition. A key benefit of this system is its ability to generate random keys. The authors integrated these two techniques to enhance the confidentiality of the data.

Swapnil V.Khedkar et al. [15] suggested a partitioning for the data storage. According to this technique, data is to be partitioned and stored on several data centres. RSA algorithm is used for encryption. Partitioning function plays a main role in this work. Larger files are divided into smaller parts to store the data effectively.

Sagar Tirodkar et al.[16] developed a 3-Dimensional approach aimed at enhancing the security of cloud data. This method employs a data classification algorithm that categorizes data based on three fundamental aspects: Confidentiality, Integrity, and Availability. The approach makes use of three sets, each containing eight images. In order to proceed, it is required to choose one image from each set. Each image is assigned a unique identifier, which is stored in a database for the purpose of authentication. When a user wishes to access their data, these three sets are presented once more as part of the authentication process. Additionally, the arrangement of images within each set is continually randomized to further minimize the risk of a brute force attack.

To improve data confidentiality, Arockiam et al. [17] have proposed a security framework. This framework aims to protect against both external and internal threats by introducing a data confidentiality framework known as AROMO. In order to store data in cloud storage, it is necessary to synthesize the data type. According to this framework, non-numeric data are encrypted, while numeric data are obfuscated. The AROcrypt technique is employed to encrypt non-numerical data, and the MONcrypt technique is used to obfuscate numerical data. In this process, the key is generated randomly.

Joyita Goswami et al. [18] proposed a symmetric key cryptography method that uses a doubly even order magic square of size 4n. In this approach, the plain text is transformed into binary format. The binary data is then split into blocks of a fixed size. A session key is created for each of these blocks to perform encryption. The bits are retrieved from the magic square matrix in a row-wise manner to form the encrypted block, and the final encrypted output, known as the cipher text, is produced from each of these encrypted blocks.

Alla et al. [19] introduced an Embedded Zerotree Wavelet zig-zag scanning order (EZWZBS) method to protect data within a network. The algorithm is based on the principles of block ciphers. The data is first converted into ASCII values and then transformed into binary form. The data is divided into blocks of a manageable size, specifically $(2*n)^2$. The binary bits of each block are extracted starting from the most significant bit (MSB) to the least significant bit (LSB), and they are arranged into a corresponding matrix using the EZW zig-zag scanning pattern. The bits are then read diagonally from the matrix and concatenated into a string cipher.

Monikandan et al.[20] introduced a confidentiality-focused obfuscation method called MONcrypt. The original text values are organized into a numerical array. A mathematical operation, specifically the power function, is applied to the plain text. The pow() function is used to calculate the square root (ST) of the plain text. The ST value is then rotated (RT) a number of times determined by the key. The key K is increased by one for each subsequent digit in the ST. The RT value is divided by 256 to obtain the remainder, which is referred to as the Modulus (MT) value. In the end, the obfuscated text is produced by converting the MT value into its corresponding ASCII character code.

Amandeep Kaur [21] introduced a new system design that relies on Diffie Hellman and pattern-based security methods. In the first step of the process, users can authenticate themselves using a username and password. This architecture also includes a pattern-based password approach. The Diffie Hellman algorithm is used to secure the data. Ayman and colleagues [22] suggested a framework aimed at improving data security. They utilized a Diffie Hellman key based on the Elliptic Curve Cryptography Algorithm. This method helps in creating a shared secret key between the sender and the receiver. This shared key enhances the integrity and authenticity of messages, supports non-repudiation, and ensures the confidentiality of the data.

Izevbizua et al. [23] introduced a method to enhance data security by integrating the Serpent cryptographic algorithm with distributed steganography, which is an established technique. Distributed steganography builds upon the traditional steganography model, aiming to refine and improve the principles of hiding information. Serpent is a symmetric key block cipher that operates with a block size of 128 bits and supports key sizes of 128, 192, or 256 bits. The data is encrypted using the Serpent algorithm and the resulting encrypted data is then distributed across various images for storage.

Ramalingam Sugumar et al.[24] created a symmetric encryption algorithm (SEA) to protect data that is stored in public cloud environments. The process starts by counting the number of values in the original text and then converting these values into their corresponding ASCII codes. A square matrix is formed, and the ASCII values are placed within the matrix in a left-to-right manner. Next, the algorithm retrieves the rows that are at even positions and the rows that are at odd positions from the matrix. A key value is added to these selected values, and the resulting ASCII values are used to form the encrypted output, which is referred to as the cipher text.

Fortine Mata et al.[25] developed a model aimed at ensuring data security within cloud environments. The authors integrated both the AES and Blowfish encryption algorithms to secure the data. Salim and others [26] suggested a method to enhance cloud security. Their approach combines identity-based cryptography with Elliptic Curve Cryptography. Hamad Naeem and team [27] introduced a technique to boost data security. In this technique, data is encrypted using a pseudorandom stream of bits generated by a pseudo-random algorithm. The encrypted data is then split into individual bits and embedded into the color pattern of an image's pixels through the least significant bit method.

A partitioning method was introduced by Sandesh G Pawar et al. [28] to improve data security in data storage. In this approach, data is divided into equal parts and each part is encrypted individually. The encrypted data is then stored across different cloud servers. The AES encryption algorithm is used for this purpose. This method also helps to minimize the storage space required. Aysan Shiralizadeh et al. [29] proposed another solution to enhance security in cloud computing. They integrated the AES and RSA algorithms to provide better data protection.

Raghu et al. [30] introduced a parallel method for encrypting and decrypting data to improve security in cloud environments. In their system, data is split into smaller parts of equal size, referred to as chunks, using a subdivision algorithm. Each chunk is assigned to a separate thread and processed as input. The encryption of each chunk occurs simultaneously, resulting in encrypted outputs known as cipher texts. Swapna V. Tikore et al. [31] developed a method to enhance data integrity and confidentiality in cloud storage. This method incorporates the RSA algorithm along with a hash function. Varsha Yaduvanshi et al. [32] conducted a review on various data security issues within a cloud environment. Vishal R. Pancholi and others [33] recommend the AES algorithm for securing data stored in cloud computing environments.

Arul Oli et al. [34] proposed a confidentiality technique for stored data in a public cloud storage environment. The proposed encryption technique is designed to protect non-numerical data stored in the cloud. This technique is based on a symmetric cryptographic system. It involves manipulating the plaintext data using a square matrix. The data processing occurs in three distinct stages. Initially, the data is split based on whether the columns are even or odd in the matrix. Then, the keys K1 and K2 are applied alternately to the data. The data is placed inside a square matrix in a column-wise manner and is read out in a row-wise fashion.

Marwa E. Saleh and colleagues [35] introduced a hybrid approach for data security that integrates cryptography and steganography. In this method, the Advanced Encryption Standard (AES) algorithm is employed to encrypt the confidential message. Once encrypted, the message is concealed within an image. Alok Ranjan et al. [36] developed a technique aimed at securing data stored in the cloud. They used the AES algorithm to encode the data and applied a hash function to the Least Significant Bit (LSB) of the cover image before embedding the encrypted message into it. G. Yogeswari et al. [37] presented an innovative method to improve cloud storage security by combining cryptographic techniques with steganography. Their approach uses the AES algorithm for data encryption and the LSB substitution method to hide the data within an image.

George et al. [38] introduced the Enhanced RSA (ERSA) method, which modifies the Standard RSA algorithm by incorporating two additional prime numbers. This modification aims to improve both the speed and security of the RSA algorithm by utilizing two random numbers during the key generation process. The proposed approach demonstrates better performance in terms of encryption and decryption time compared to the traditional RSA algorithm.

Deepika et al. [39] integrated cryptography with steganography to strengthen data security in cloud environments. They employed an image sequencing password for authentication purposes, allowing only legitimate users to access the system if they provide the correct sequence of images. To safeguard data from potential attackers, the data is concealed within images. Additionally, a randomized and anonymized privacy-preserving technique is utilized in this method to ensure data confidentiality.

Ekta Agrawal et al. [40] introduced a symmetric encryption method that uses cryptography for securing data. In this method, a random number serves as the initial key, which is placed before the original text. The original text is then converted into a decimal number using ASCII encoding. This decimal number is divided by four, and the result is converted back into an ASCII code. The final encrypted text is created by combining this result with the remainder from the division. Table 2.1 presents an analysis of the algorithms used to improve data storage security by applying different techniques.

Table 2.1. Analysis on Security Enhancement in Public Cloud Storage

S.No	Algorithms	Symmetric	Asymmetric	Obfuscation	Steganography	Issues
1	Public Key Cryptography using Matrices [3]	---	Yes	---	---	Increases the time required for encrypting and decrypting data.
2	Hybrid Symmetric Encryption [4]	Yes	---	---	---	Cipher text is the combination of ASCII values.
3	HDFS [5]	Yes	---	---	---	Existing Algorithm AES is used

4	CHAP [6]	Yes	---	---	---	Existing Algorithm Rijndael is used
5	SMBBOT [8]	Yes	---	---	---	Increases the time taken for cipher text generation
6	Symmetric Crptography [12]	Yes	---	---	---	Cipher text will be in the combination of ASCII values
7	3-D approach [16]	---	---	---	---	Additional time needed for authentication
8	Symmetric Encryption Algorithm (SEA)[24]	Yes	---	---	---	Cipher text will be in the combination of ASCII values
9	Hybrid Technique [33]	Yes	Yes	---	---	Increases the time taken for set of keys generation
10	AO_Enc CT Technique [34]	Yes	---	---	---	Supports only non-numerical data
11	Hybrid Technique [35]	Yes	---	---	Yes	Increases the total time of cryptosystem as well as communication time and cost
12	Hybrid Technique [37]	Yes	---	---	Yes	Cipher text is also in image format and hence can be identified easily
13	Enhanced RSA [38]	---	Yes	---	---	Need additional time to generate the key
14	ARARO Framework [ARU 16]	Yes	---	Yes	---	Cipher text will be in the combination of ASCII values

IV. CONCLUSION

Cloud provides accessible, open, and diverse services to the world. However, as this new cloud technology continues to grow, it also introduces new risks and threats. Despite the variety of structures and the expansion of cloud services, the perception of cloud computing has not been fully visualized. Cloud users store their data in cloud storage, and they do not need to worry about space limitations, purchasing new storage devices, or managing their data. They simply need to access their data anytime and anywhere, as long as they have an internet connection. One of the major drawbacks of cloud computing is its significant security risks. This chapter discusses the purpose of the research and the security issues associated with the cloud. Throughout this study, various aspects of security problems have been analyzed. A literature review shows that most researchers have focused their work on data security, and it is encouraged to propose new algorithms. Therefore, the cloud storage environment needs to enhance cryptography and obfuscation techniques to ensure data security.

REFERENCES

[1] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I., “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility” ,*Elsevier Science Publishers*, 25, 599–616, 2009.

[2] Buyya R, Vecchiola C, S. ThamaraiSelvi, Mastering Cloud Computing Foundations and Applications Programming, *Elsevier*, pp. 1–469,2013.

[3] BirendraGoswami, Dr.S.N.Singh, “Enhancing Security in Cloud computing using Public Key Cryptography with Matrices”, *International Journal of Engineering Research and* Applications, Vol.2, pp.339-344,2012.

[4] Dr. L. Arockiam, S. Monikandan,” A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage”, *International Journal of Engineering Research & Technology*, Vol.3, pp.1053-1058, 2014.

[5] Zhonghan Cheng, Hao Huang,” Design and Implementation of Data Encryptionin Cloud based on HDFS”, *International Workshop on Cloud Computing and Information Security*, pp.274-277,2013.

[6] SanjoliSingla, Jasmeet Singh,” Cloud Data Security using Authentication and Encryption Technique",*International Journal of Advanced Research in Computer Engineering and Technology*,Vol.2,pp.2232-2235,2013.

[7] RajkishorePrasad,”SriRamshalaka: A Vedic Method of Text Encryption and Decryption”, *Indian Journal of Computer Science and Engineering*, Vol.4, pp.225-234, 2013.

[8] Manas Paul, Jyotsna Kumar Mandal,” A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept”, *International Conference on Information Technology, Electronics and Communications*,pp.6-11,2013.

[9] Prakash G L,Dr.ManishPrateek and Dr.Inder Singh,” Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System*”, International Journal Of Engineering And Computer Science*,Vol.3,pp.5216-5223,2014.

[10] MrinalKanti Sarkar, Trijit Chatterjee,” Enhancing Data Storage Security in Cloud Computing Through Steganography”,*International Journal on Network Security*, Vol.5,pp.13-19,2014.

[11] Padmanaban K, PanneerSelvi R, Janani S,” A Novel Symmetric Key Cryptography Algorithm for Improving Privacy of Data in Cloud Servers”, *International Journal of Research in Computer and Communication Technology*, Vol.3,pp.181-185,2014.

[12] Vanaja A,” Efficient Cryptography Technique for Data Security using Binary Tree”, *International Journal of Innovative Research in Computer and Communication Engineering*,Vol.2,pp.67-76,2014.

[13] Ms. Komal S. Landge, Ms. RanjanaShende,” Enhancing Cloud Data Security by using Rijndael Encryption Algorithm”, *International Journal of Science, Engineering and Technology Research*,Vol.3,pp.3427-3430,2014.

[14] Sarika U. Kadlag, Rahul L. Paikrao,” Hybrid Cryptosystem for Secure Text File for Cloud”, *International Journal of Advance Research in Computer Science and Management Studies*,Vol.2,pp.419-426,2014.

[15] SwapnilV.Khedkar, A.D.Gawande,” Data Partitioning Technique to Improve Cloud Data Storage Security”, *International Journal of Computer Science and Information Technologies*,Vol.5,pp.3347-3350,2014.

[16] SagarTirodkar, YazadBaldawala, SagarUlane, Ashok Jori,” Improved 3-Dimensional Security in Cloud Computing”, *International Journal of Computer Trends and Technology*,Vol.9,pp.242-247,2014.

[17] L. Arockiam, S. Monikandan, P. D. Sheba K Malarchelvi, Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage, *International Journal of Computer Applications*, 2014, pp.17-21.

[18] JoyitaGoswami, Manas Paul,” A Novel Symmetric Key Cryptography Based on Doubly Even Order Magic Square”, *International Journal on Advanced Computer Theory and Engineering*,Vol.3,pp.16-22,2014.

[19] KalavathiAlla, Sai Jyothi B,” A New-Fangled Symmetric block cipher using Zig-zag Scan Patterns”, *International Journal of Research in Engineering and Technology*, Vol.3, pp.216-223, 2014.

[20] S. Monikandan and L. Arockiam,” Confidentiality Technique to Enhance Security of Data in Public Cloud Storage using Data Obfuscation”, *Indian Journal of Science and Technology*,Vol.8, pp.1-10,2015.

[21] Amandeep Kaur, PawanLuthra,” To Enhance the Reliability and Security in Cloud Environment Using Diffie-Hellman and Image Pattern Password”, *International Journal of Computer Science Engineering and Technology*,Vol.5,pp.13-17,2015.

[22] Ayman Helmy Mohamed, Aliaa A.A. Youssif, Atef Z. Ghalwash,” Cloud Computing Security Framework based on Elliptical Curve”, *International Journal of Computer Applications*,Vol.110,pp.45-51,2015.

[23] Izevbizua, Peter Odion,” Data security in the cloud using Serpent Encryption and Distributed Steganography”, *European Scientific Journal*,Vol.11,pp.347-359,2015.

[24] RamalingamSugumar and SharmilaBanu Sheik Imam,” Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage”, *Indian Journal of Science and Technology*, Vol.8, pp.1-5, 2015.

[25] Fortine Mata, Michael Kimwele, George Okeyo, ”Enhanced Secure Data Storage in Cloud Computing using Hybrid Cryptographic Techniques”, *International Journal of Science and Research*,Vol.6,pp.1702-1708,2015.

[26] Dr. Salim Ali Abbas, Amal Abdul BaqiMaryoosh,” Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography”, *Journal of Computer Engineering*, Vol.17, pp.48-53, 2015.

eISSN 3108-026X
International Multidisciplinary Research Journal Reviews (IMRJR)
Volume 2, Issue 11, November 2025
DOI 10.17148/IMRJR.2025.021107

[27] Hamad Naeem, Jun Sang, Waqar Ali Abro, Adeel Khalid, Muhammad Rashid Naeem, Adeel Akbar Memon, SaadTanvir, ”Message Encryption by Processing Image Using Pseudo Random Key Streams Generation”, *International Journal of Computer Trends and Technology*,Vol.20,pp.78-82,2015.

[28] Sandesh G Pawar,Karan K Kachroo,Rakesh R Mangudkar, Sanket D Ghule,” Cloud Data Storage Security using Data Partitioning Technique”, *Multidisciplinary Journal of Research in Engineering and Technology*,pp.24-30,2015.

[29] AysanShiralizadeh, AbdulrezaHatamlou, Mohammad Masdari,” Presenting a new data security solution in cloud computing”, *Journal of Scientific Research and Development*,Vol.2,pp.30-36,2015.

[30] Raghu, Ravishankar,” Application of Classical Encryption Techniques for Securing Data- A Threaded Approach”, *International Journal on Cybernetics & Informatics*, Vol.4, pp.125-132, 2015.

[31] Swapna V. Tikore, K.Deshmukh Pradeep ,B. Dhainje Prakash ,” Ensuring the Data Integrity and Confidentiality in Cloud Storage Using Hash Function and TPA”, *International Journal on Recent and Innovation Trends in Computing and Communication*,Vol.3,pp.2736-2740,2015.

[32] VarshaYaduvanshi, Manish Rai, MohitGangwar,” A Review On Data Security in Cloud Environment”, *International Journal Of Engineering And Computer Science*,Vol.5,pp.19574-19579,2016.

[33] Vishal R. Pancholi, Dr. Bhadresh P. Patel,” Enhancement of Cloud Computing Security with Secure Data Storage using AES”, *International Journal for Innovative Research in Science & Technology*,Vol.2,pp.18-21,2016.

[34] S.ArulOli, Dr.L.Arockiam,” Enhanced Obfuscation Technique for Data Confidentiality in Public Cloud Storage”, *MATEC Web of Conferences*, 40,2016,pp.1-5.

[35] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara,”Data Security using Cryptography and Steganography techniques”, *International Journal of Advanced Computer Science and Applications*,Vol.7,2016.

[36] AlokRanjan, Mansi Bhonsle,” Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography”, *International Journal of Engineering Research*, Vol.5,2016.

[37] G.Yogeswari, P.Eswaran, “Enhancing Data Security for Cloud Environment based on AES Algorithm and Steganography Technique”, *International Journal of Advanced Research Trends in Engineering and Technology*,Vol.3, 2016.

[38] Dr. D.I. George Amalarethinam, H. M. Leena,” Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud”, *World Congress on Computing and Communication Technologies*,2016.

[39] Deepika,” Enhancement of Data Security for Cloud Environment Using Cryptography and Steganography Technique”, *International Journal of Innovative Research in Computer and Communication Engineering* , Vol.5,pp.225-230,2017.

[40] Ekta Agrawal,” A New and More Authentic Cryptographic Based Approach for Securing Short Message”, *International Journal of Advanced Research in Computer Science*, Vol.8, pp.917-921, 2017.

[41] Dr.D.I.George Amalarethinam, B.FathimaMary, DMUCE- A Confidentiality Enabled Technique To Improve Cloud User Security, *International Journal of Applied Engineering Research*,pp.34103,34108,2015.

[42].Dr.D.I.George Amalarethinam, B.FathimaMary, eDSSuMRT- Ensured Data Security Strategy using Matrix Random Traversal In Cloud Storage Environment, *International Journal of Applied Engineering Research*,pp.272-279,2015.

[43].Dr.D.I.George Amalarethinam, B.FathimaMary, Data Security Enhancement in Public Cloud Storage, *Journal of Computing and Intelligent Systems*, pp.1-5,2017.

[44].Dr.D.I.George Amalarethinam, B.FathimaMary, Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography, *IEEE Explore*,pp.181-184,2016.

[45].Dr.D.I.George Amalarethinam, B.FathimaMary, Security Enhancement for Public Cloud Storage with Minimum Cost, *International Journal of Pure and Applied Mathematics*, pp.1-9,2018.

[46].D.I.George Amalarethinam, B.FathimaMary, Comparative Analysis of Obfuscation Techniques in Public Cloud, *American International Journal of Research in Science, Technology, Engineering & Mathematics*,pp.309-312,2019.

[47]Dr.D.I.George Amalarethinam, B.FathimaMary, Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation, *International journal of control theory and application*,pp.1-11,2016.

[48].Dr.D.I.George Amalarethinam, B.FathimaMary, *Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography*, IEEE Explore,pp.181-184,2016.

[49].B.Fathima Mary, Dr.D.I George Amalarethinam, Data security enhancement in public cloud storage using data obfuscation and steganography, *world congress on computing and communication technologies (WCCCT)*,pp.181-184,2016.

[50]Dr. B. Fathima Mary, Data Security Enhancement In Cloud Using Magic Square Obfuscation,*International Multidisciplinary Research Journal Reviews (IMRJR)*,vol.2, pp.66-70,2025.