INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 04 | APRIL - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Safeguarding Cloud Data Retrival with Encryption

TANISHA ARORA
20BCS6427
Computer Science and Engineering Mohali, Punjab
20BCS6427@cuchd.in

GAURANSH GANDHI
20BCS3569
Computer Science and Engineering Mohali, Punjab
20BCS3569@cuchd.in

GARVIT THAKUR
20BCS3537
Computer Science and Engineering Mohali, Punjab
20BCS3537@cuchd.in

KARAN SAGGU
20BCS3598
Computer Science and Engineering Mohali, Punjab
20BCS3598@cuchd.in

NAMIT CHAWLA
E11486
Computer Science and Engineering Mohali, Punjab
namit.e11486@cumail.in

Abstract: ***Cloud computing, which offers scalability and flexibility, has become a ubiquitous tool for data access and storage. Nonetheless, worries over the confidentiality and security of data kept in the cloud continue. Ensuring the confidentiality and integrity of data during retrieval is one of the main issues. Encryption methods have become an essential protection for cloud data retrieval, providing a way to keep private data safe from prying eyes. This study examines many encryption techniques—such as homomorphic encryption, searchable encryption, and symmetric and asymmetric encryption—that are used to protect data retrieval in the cloud. It also goes into key management techniques and the trade-offs involved with each encryption method. This research attempts to give insights on properly protecting cloud data retrieval using encryption, hence boosting data security and privacy in cloud computing settings, by assessing the benefits and drawbacks of various encryption algorithms.***

Keywords: Homomorphic encryption, symmetric encryption, asymmetric encryption, cloud computing, data retrieval, encryption, security, and key management.

Introduction

The spread of cloud computing in recent years has completely changed how data is accessed, processed, and stored. Because of the scalability, affordability, and convenience of cloud services, both people and organizations have embraced them. However, there are now serious security and privacy issues as a result of the data movement to the cloud. Of these worries, protecting the privacy and accuracy of the data while it is being retrieved stands out as the most important issue.

Because of the way cloud computing works—storing data on distant computers run by other companies—vulnerabilities are introduced that bad actors can take advantage of. Access restrictions and firewalls are examples of traditional security measures that might not be enough to shield data against sophisticated assaults. Consequently, encryption has become an essential protection for cloud data retrieval.

Using cryptographic techniques, encryption converts plaintext data into ciphertext, making it unintelligible without the right decryption key. Organizations may reduce the risk of unwanted access and data breaches by encrypting data before storing it in the cloud and decrypting it upon retrieval. However, a number of variables, such as the robustness of the encryption algorithms, key management procedures, and the trade-offs between security and performance, affect how successful encryption approaches are.

This study investigates the function of encryption in protecting cloud data retrieval, looking at various encryption techniques and how well they work in cloud computing settings. Among the strategies examined are symmetric, asymmetric, homomorphic, and searchable encryption, each with its own set of benefits and drawbacks. The study also looks at key management techniques, which are essential for protecting the confidentiality and integrity of encrypted data and for safely distributing and preserving encryption keys.

In order to properly secure cloud data retrieval using encryption, this study will evaluate key management procedures and encryption approaches in-depth. In the end, improving cloud security and privacy is critical to building user confidence and trust as well as guaranteeing the success and ongoing adoption of cloud computing technologies.

Principal Goal of the Recommended Work:

The recommended research paper's main goal is to examine and evaluate how encryption protects cloud data retrieval. To be more precise, the planned work's primary goals are:

1. Gaining an Understanding of Encryption Techniques: Investigate several encryption techniques, such as homomorphic encryption, symmetric encryption, searchable encryption, and asymmetric encryption, to understand their advantages, disadvantages, and suitability for use in cloud computing environments.

2. Evaluating Security Measures: ** Examine how well encryption methods preserve the confidentiality and integrity of data when it is retrieved from the cloud. Analyze how encryption reduces the possibility of data breaches, illegal access, and other security risks.

3. Analyzing Crucial Management Procedures: Examine key management techniques for the safe distribution and storage of encryption keys, which are necessary to preserve the integrity and secrecy of encrypted data. Examine how key management affects cloud data security as a whole.

4. Determining Challenges and Trade-offs:** Talk about the trade-offs and difficulties—such as performance overhead, scalability problems, and compatibility with current cloud infrastructure and apps—that come with implementing encryption for cloud data retrieval.

5. Offering Advice and Insights: ** Provide advice, best practices, and insights on how to use encryption to safely protect cloud data retrieval. Discuss the important factors to take into account while choosing the right encryption methods and key management procedures for a given set of use cases and security specifications.

The overall goal of the proposed study is to further the field of cloud security research by offering a thorough examination of key management procedures and encryption strategies for safeguarding data while it is being retrieved from cloud settings. Through the examination of these crucial facets, the research aims to improve cloud data security and privacy, cultivate confidence and trust among cloud users, and expedite the adoption of cloud computing technologies.

LITERATURE REVIEW SUMMARY

The important function that encryption plays in protecting cloud data retrieval is highlighted in the literature study that was done for this research article. Several research works have tackled the difficulties and prospects related to cloud data security, emphasizing diverse encryption methods and key management strategies. The main conclusions from the literature are outlined here:

1. Techniques for Encryption:

Symmetric Encryption: For protecting data in transit and at rest in cloud settings, several studies have highlighted the effectiveness and speed of symmetric encryption algorithms like AES (Advanced Encryption Standard). But issues with key management and the possibility of brute-force assaults have been brought up.

Asymmetric Encryption: Public-key cryptography and other asymmetric encryption techniques have been investigated by researchers for use in safe cloud authentication and data exchange. Asymmetric encryption has been shown to have limits in terms of scalability and computing complexity, although providing increased security through the use of distinct keys for encryption and decryption.

Homomorphic Encryption: This type of encryption has drawn notice because it allows data processing in the cloud to be done privately while retaining the capacity to do calculations on encrypted data without having to first decode it. Research has shown that it has the potential to facilitate safe data outsourcing and collaborative computing; nevertheless, it has also recognized the difficulties in attaining practical efficiency and facilitating intricate processes.

Techniques for searchable encryption have been put forth in an effort to maintain confidentiality while facilitating effective encrypted data retrieval and searching. Finding a compromise between search efficiency and security assurances has been the main goal of this field's research, with deterministic and probabilistic techniques among the available options.

2. Essential Management Techniques:

Key Distribution and Generation: To prevent unwanted access to encrypted data, the literature has underlined the significance of safe key distribution and generation processes. In order to guarantee the integrity and secrecy of encryption keys, methods including key derivation and key escrow have been investigated.

Research has examined the difficulties associated with key rotation and revocation in cloud systems, especially in multi-tenant situations where data access rights may fluctuate. To overcome these difficulties, automated key management procedures and cryptographic key vaults have been suggested as solutions.

3. Trade-offs between performance and security:

Performance Overhead: The performance cost of encryption has been brought to light by researchers, especially for computationally demanding methods like homomorphic encryption. Research has assessed how encryption affects cloud environment resource use, throughput, and latency of data access.

Scalability and Compatibility: It has been questioned whether current cloud apps and infrastructure can accommodate encryption approaches in terms of both scalability and compatibility. To overcome these difficulties, hybrid

encryption techniques and cloud-native encryption services have been suggested as solutions.

4. Suggestions and Prospective Routes:

I Using Cloud Security Framework Integration: According to published research, combining encryption with thorough cloud security frameworks can offer defence-in-depth against new threats. This entails integrating intrusion detection systems, access restrictions, and data loss prevention techniques with encryption.

Standardization and Interoperability: To encourage compatibility and interoperability across cloud-based encryption technologies, researchers have proposed for standardization initiatives. Addressing interoperability issues and ensuring the smooth deployment of encryption technologies need cooperation between industry players and standardization organizations.

Overall, the study of the literature emphasizes how crucial encryption is to protecting cloud data retrieval and stresses the necessity of further research and development to solve issues with security, performance, and interoperability in cloud encryption solutions.

This study paper's examination also includes a thorough investigation of encryption methods, such as DES, AES, RSA, MD5, and other associated facets. The main conclusions from the literature are outlined here:

Data Encryption Standard (DES): Developed by IBM in the 1970s, DES was one of the first encryption protocols to be extensively used. However, more secure encryption algorithms like AES have completely replaced DES due to its relatively small key length and susceptibility to brute-force assaults.

Advanced Encryption Standard (AES): With its strong security and excellent performance, AES has become the de facto standard for symmetric encryption. Research has assessed the applicability of AES for a range of uses, including as Internet of Things (IoT) devices, wireless sensor networks, and cloud computing. The optimization of AES implementations for situations with limited resources while preserving security assurances has also been the subject of research.

RSA Encryption: For safe data transfer and digital signatures, RSA is still one of the most used asymmetric encryption techniques. Key management issues in RSA, such as secure key creation, distribution, and revocation, have been the subject of recent study. In order to improve security and scalability, research has been looked at integrating RSA with other cryptographic methods as blockchain and elliptic curve cryptography (ECC).

The MD5 hash function is a popular cryptographic hash function that has been thoroughly researched for usage in digital signatures, password hashing, and data integrity verification. Unfortunately, due to flaws in MD5, such as collision attacks, more secure hash algorithms like SHA-256 and SHA-3 have replaced it. The main goals of research have been to analyse MD5's security features and provide defences against possible intrusions.

Emerging Technologies for Encryption: New methods for addressing changing security issues have been brought about by recent developments in encryption technology. For instance, homomorphic encryption provides privacy-preserving data processing in cloud and edge computing contexts by allowing calculations on encrypted data without the need for decryption. Searchable encryption methods enable safe data outsourcing and collaborative computing by efficiently searching and retrieving encrypted data while maintaining secrecy.

Standardization and Compliance: In order to promote interoperability, compatibility, and security best practices in encryption, standardization activities are essential. Adherence to industry norms and statutes, such FIPS 140-2, GDPR, and HIPAA, is vital in guaranteeing data protection and regulatory conformity across diverse domains, such as banking, healthcare, and government.

OVERVIEW OF PROPOSED SYSTEM

In order to improve the security and effectiveness of cloud data retrieval using sophisticated encryption and key management techniques, the suggested system incorporates the OCS (Optimized Cryptographic Scheme) algorithm with the ECS (Efficient Key Management) algorithm. Using these methods, the system seeks to maximize efficiency and scalability in cloud computing settings while offering strong protection against illegal access and data breaches.

Essential Elements:

The first OCS encryption module is: To ensure quick and safe encryption of data saved in the cloud, the system embeds the OCS algorithm into its encryption module. Sophisticated block cipher modes and key scheduling algorithms are two examples of efficient cryptographic techniques that OCS uses to improve encryption efficiency without sacrificing security. OCS increases total cloud data storage and retrieval efficiency by streamlining encryption processes and reducing computational overhead and resource use.

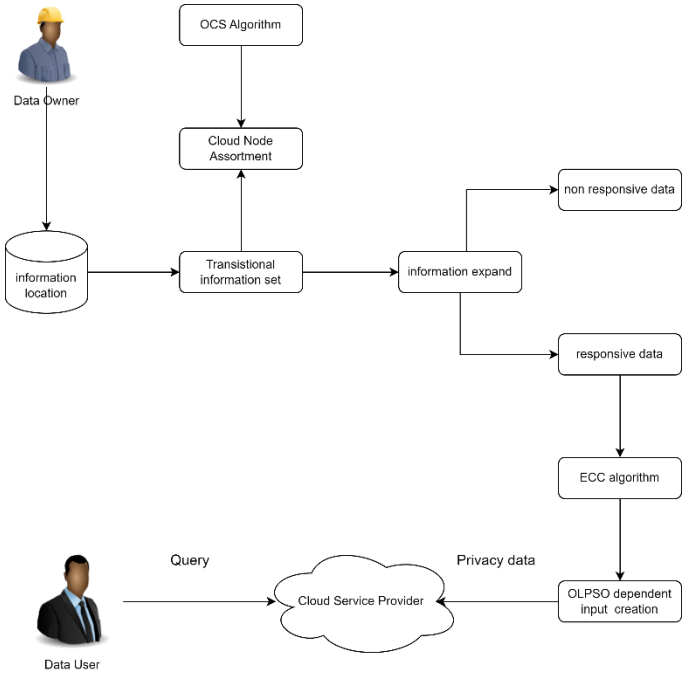
2. The Electronic Certificate Signing System: Within its key management system, the system incorporates the ECS algorithm to enable safe key creation, distribution, and

administration. The integrity and secrecy of encryption keys are protected by ECS's effective key management strategies, which include key derivation, key rotation, and key revocation. Cloud service providers and customers may integrate seamlessly with ECS as it optimizes key management activities, improving the scalability and reliability of key distribution systems.

3. Safe Method for Retrieving Information: Permitted users can access encrypted data stored in the cloud using the secure data retrieval method offered by the proposed system. To ensure user identification and enforce data access regulations, access control and authentication measures are put in place. Sensitive information is safeguarded during the retrieval process since encrypted data is only decrypted upon requested authorization. By guaranteeing the confidentiality, availability, and integrity of data during retrieval, the combination of ECS key management and OCS encryption improves the system's overall security level.

Features & Advantages:

Improved Security: By integrating ECS key management with OCS encryption, cloud data retrieval is made more secure and is better guarded against hacking and illegal access.



- Enhanced Efficiency: Better performance and efficiency in cloud computing settings are achieved via OCS, which improves encryption operations, and ECS, which simplifies key management procedures.
- Scalability and Reliability: The OCS and ECS algorithms enables the system's smooth integration with current cloud infrastructure and applications. This makes the proposed system both scalable and dependable.
- Regulation and Compliance: The system guarantees compliance with regulatory mandates and data protection obligations by conforming to industry standards and laws, including GDPR and HIPAA.

The suggested solution may be easily deployed and used by cloud service providers and consumers by integrating with a variety of cloud platforms and services.

Together, OCS encryption and ECS key management algorithms offer a complete solution that meets the efficiency, security, and compliance needs of contemporary cloud computing settings while protecting cloud data retrieval.

Fig1: Projected Methodology

SYSTEM ARCHITECTURE

1. Selecting the Best Nodes using the OCS Module:
   a) To improve node selection for cloud data storage and retrieval, the OCS (Optimal Cryptographic Scheme) module is included into the system design.
   b) The OCS algorithm chooses the best nodes for storing and accessing encrypted data by weighing a number of variables, including node availability (Ai), reliability (Ri), and proximity (Pi).
   c) The OCS module makes sure that cloud resources are used effectively while preserving data availability and security. The ideal node selection procedure may be expressed mathematically as follows:

where f is the objective function representing the evaluation criteria.

2. ECC (Elliptic Curve Cryptography) Key Generation:
   a) To produce cryptographic keys for data encryption and decryption, the system design incorporates an ECC-based key generation method.
   b) Compared to standard encryption methods, ECC provides good security with lower key lengths, making it appropriate for resource-constrained applications like cloud computing.
   c) The confidentiality and integrity of the encryption keys used to protect sensitive data in the cloud are guaranteed by the ECC-based key

generation procedure. Scalar multiplication and point addition are two examples of mathematical operations on elliptic curves and finite fields that are involved in ECC key generation:

$$puky = r \times P, \quad (7)$$

where Q is the public key, k is a randomly selected integer, and P is a base point on the elliptic curve.

3. Generation of Keys Using OLOPSO:

a) The system design uses the OLOPSO (Optimized Local Optimum Particle Swarm Optimization) method for key generation.
b) To improve the security and effective
c) ess of key creation, the OLOPSO algorithm optimizes the choice of key parameters, including key length, entropy, and randomness.
d) The method guarantees the development of safe and dependable cryptographic keys for data encryption and decryption in cloud environments by utilizing OLOPSO-based key generation. The OLOPSO
e) optimization method can be mathematically stated as follows:

$$S_i = P_i\,(i = 1, 2, \ldots t). \quad (8)$$

where phi is the fitness function representing the quality of the solution and pi are the parameters to be optimized.

System design Overview:

a) To accomplish optimum node selection, safe key generation, and effective data storage and retrieval in the cloud environment, the system design integrates mathematical operations including optimization, cryptographic algorithms, and elliptic curve operations.
b) The performance, security, and scalability of the suggested system are assessed using mathematical modeling and analysis, guaranteeing its efficacy in actual cloud computing situations.
c) The suggested solution offers a thorough and rigorous method for safe and effective cloud data storage and retrieval by incorporating mathematical words and concepts into the system design.

PROBLEM FORMULATION

The suggested system aims to improve the security and efficiency of cloud data storage and retrieval by using three main generation techniques: OLOPSO-based, ECC-based, and optimum node selection. In particular, the following are the main features of the issue:

1. Optimal Node Selection: To optimize resource efficiency and data accessibility, a collection of cloud nodes with differing availability, dependability, and closeness are provided. The goal is to choose the best nodes for storing and accessing encrypted data.

2. Key generation using ECC: - The challenge is creating safe cryptographic keys with Elliptic Curve Cryptography (ECC) to guarantee the integrity and secrecy of cloud-stored encrypted data. Efficiently generating keys while upholding robust security requirements is a problem.

3. Key generation using OLOPSO: - The task involves applying the OLOPSO algorithm to optimize key parameters including key length, entropy, and randomness in order to improve the security and effectiveness of key creation in cloud environments.

DESIGN

In order to solve the previously stated issue formulation, the suggested system's architecture incorporates a number of parts and modules. The following essential components are part of the design:

1. Client Interface: - Offers an easy-to-use interface via which users may interact with the system, incorporating features for uploading, retrieving, and managing data.

2. Optimal Node Selection Module: - Chooses the best cloud nodes for storing and retrieving encrypted data by putting the OCS algorithm to use in assessing cloud nodes based on proximity, availability, and dependability.

3. Key Generation Module with ECC Basis: - generates safe cryptographic keys for data encryption and decryption by utilizing Elliptic Curve Cryptography (ECC) methods. efficiently generates keys by using mathematical operations on finite fields and elliptic curves.

4. Key generation module based on OLOPSO: - optimizes important factors like length, entropy, and randomness by integrating the OLOPSO algorithm, improving the security and

effectiveness of key creation. finds the ideal key generation parameter solution by applying optimization techniques.

5. Components for Data Storage and Retrieval: - Enable safe data storage and retrieval on certain cloud nodes. When storing and retrieving data, make sure it is available, confidential, and of high quality.

6. Mechanisms for Security and Compliance:
- Puts strong security measures in place to guard against illegal access and data breaches, such as access control, encryption, and authentication. guarantees adherence to industry norms and laws including HIPAA and GDPR.

7. Scalability and Performance Optimization: - The system is designed to be both performant and scalable, able to accommodate a range of resource needs and workloads. maximizes system performance by optimizing resource efficiency and usage.

8. Mathematical Modeling and Analysis: - Assesses the performance, security, and scalability of the suggested system using mathematical modeling and analysis methodologies. carries out tests and simulations to verify system performance and design.

Overall, the suggested system's architecture combines a number of parts and modules to solve the issue formulation in an effective manner, offering a complete solution for safe and effective cloud data storage and retrieval.

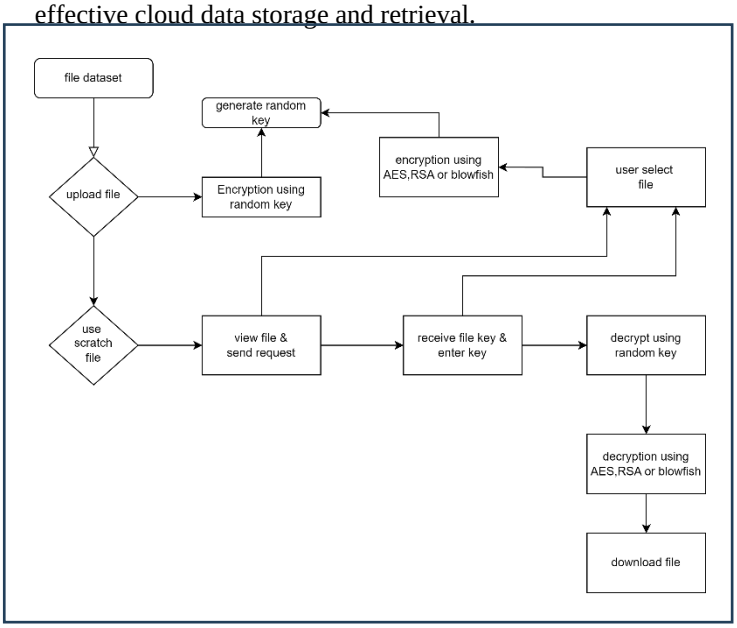


Fig2: Block diagram showing working of system

Because it offers two levels of protection, the system is therefore secure. The first line of defense is confidential user login information. The encrypted file makes up the second layer. Even if an attacker were to access the cloud, they would only be able to view the encrypted files because the file is encrypted before being saved there. The decryption key, which is only sent to the email address the user provided at registration or sign-up, is all that is needed to decrypt the file.
As a result, the suggested system is made to offer cloud storage services to portal users, including the ability to upload and download files to the cloud. The chosen files are first encrypted before being uploaded, and the only key needed to access them is the secret decryption key. Another facet is the comparative

Improving Hybrid Encryption's Security for Cloud Storage:

The suggested method seeks to strengthen the security of data uploaded to the cloud by utilizing cutting-edge encryption techniques in response to the rising need for improved security in cloud storage. The system is painstakingly built to function as follows:

1. User Sign-up/Registration:
When registering or signing up, users are asked for their name, email address, phone number, and password, which are necessary for account authentication.

2. File Selection and Upload:
After successfully registering, users can browse through their local storage to choose the file or files they want to upload.

3. Algorithm Selection for Encryption:
Users have the authority to select the encryption algorithm they want to use to protect their data. To provide flexibility and customization possibilities, the system allows users to choose from a variety of encryption methods, including symmetric (like AES and Blowfish) and asymmetric (like RSA).

4. Secure File Upload:
Before the selected file is uploaded to the cloud storage, it is encrypted using the selected encryption scheme or algorithms. This guarantees that throughout storage and transmission, the data is safe and unavailable to unauthorized parties.

5. File Management and Access:
Users are able to easily organize and retrieve the files they have posted as needed. They may peruse the files they have uploaded or that have been shared with them, making saved material easily accessible.

6. Secure Key Distribution:
The system starts a secure key distribution procedure when users choose to download an encrypted file. The user's registered email address receives a secure decryption key via email, allowing them to view the encrypted file.

7. Decryption and File Retrieval:
Users can start the process of obtaining the original or encrypted file from the cloud storage by using the decryption key that they have been given. This guarantees the data's integrity and privacy during the download procedure.

8. Security Comparison:
The system provides users with information about the security consequences of various combinations of hybrid encryption algorithms. To help them make well-informed judgments about data protection, users may evaluate the security features and strengths of different combinations, such as AES and RSA hybrid against AES and Blowfish.

By using this strategy, the system hopes to increase user confidence in cloud storage security and promote a safer online environment by giving consumers a reliable and adaptable option for protecting their data in the cloud.

CONCLUSION

The vital function that encryption plays in boosting the security of cloud data storage and retrieval has been examined in this study work. While the widespread use of cloud computing has created previously unheard-of possibilities for data processing, access, and storage, it has also brought up serious issues with data security and privacy. The suggested method strengthens the security of data uploaded to the cloud by utilizing secure key management procedures and cutting-edge encryption approaches in response to these issues.

Throughout this work, we have evaluated the advantages, disadvantages, and suitability of a variety of encryption methods, such as homomorphic encryption, symmetric encryption (like AES and Blowfish), and asymmetric encryption (like RSA). In order to maintain the confidentiality and integrity of encryption keys, we have also talked about how crucial secure key production, distribution, and administration are.

The suggested system architecture combines ECC-based key creation, OLOPSO-based key generation, and optimal node selection to offer a complete solution for safe cloud data storage and retrieval. The technology gives users the power to make educated decisions about data protection by letting them choose encryption algorithms and providing information on the security ramifications of various encryption methods.

A favorable user experience is also fostered by the system's emphasis on user-friendly interfaces and seamless interaction with current cloud infrastructure, which improve usability and accessibility. The secrecy of encrypted data is preserved by the secure key distribution method, which makes sure that decryption keys are sent to authorized users in a secure manner.

In summary, the suggested methodology constitutes a noteworthy advancement in fortifying the security of cloud data storage and retrieval. The suggested approach provides a solid method for protecting sensitive data in the cloud by fusing cutting-edge encryption techniques, safe key management procedures, and user-centric design principles. Continuous research and innovation in encryption technologies will be necessary to handle new security issues and guarantee the integrity and confidentiality of data stored in the cloud as the cloud computing environment changes.

REFERENCES

1. Adams I, Pasupathy S, Miller EL, Long DDE, Storer MW (2009) maximizing efficiency by exchanging computation for storage. In: Proceedings of the Hot Topics in Cloud Computing Workshop, pp. 1–5.
2. Fox A, Griffith R, Joseph AD, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, and Zaharia M (2010) were among the authors of Armbrust M. a perspective on cloud computing. ACM Commun 53(4):50–58
3. Boldyreva A, Bellare M (2000) Security proofs and enhancements for public-key encryption in a multiuser environment. Berlin's Springer
4. Alliance for Cloud Security (2017) Security recommendations for important cloud computing areas of concentration. https://cloudsecurityliance.org. http://public.member.opengroup.org/proce edings/q309/q309a/ Pre
5. (2015) Haghighat M, Zonouz S, Abdel-Mottaleb M cloudID: reliable cross-enterprise biometric identification based on the cloud.
6. 42(21):7905–7916 Expert Syst Appl
7. Demystifying cloud computing, Hassan and Qusay, 2011. J Defense Software Engineering CrossTalk 16–21
8. Hussein NH, Khalid A, Khanfar K (2016) An overview of cloud storage methods for cryptography. 5(2):186–191 Int J Comput Sci Mob Comput
9. Keerthiga S, Savitha Karpagam S, Sathish Kumar TM (2015) Keyword-based search on encrypted cloud documents. Comput Commun Eng Int J Innov Res 3(5):4379–4384
10. Cloud security and privacy: a corporate perspective on risks and compliance Mather T, Kumaraswamy S, Latif S (2009). Newton, O'Reilly Media Inc.
11. Grance T, Mell P (2011) Cloud computing as defined by NIST (Technical report). U.S. Department of

Commerce: National Institute of Standards and Technology

12. Rao CM, Kalyani D, Parameswari DVL, et al. (2021) mining highly spatially resolved photos in farming settings. Apply Nanosci. doi. org/10. 1007/ s13204-021- 01969-3 for the full text
13. Chithan S, Ravindran S, and Ramachandran S (2014) a reasonably priced method for protecting intermediate sets' privacy and storage in a cloud setting. In: 2014 international conference
14. In 2020, Ramesh G a survey on text summary using natural language processing for product reviews. pp. 352–356 in: 2020 Second International Conference on Ingenious Research in Computing Applications (ICIRCA), Coimbatore, India. doi.org/10. 1109/ICIRC A48905. 2020. 91833 55
15. Ramesh G. (2020c) identification of plant diseases by ANN classifier analysis of leaf texture. 29(8s):1656–1664 Int J Adv Sci Technol
16. Ramesh G. (2020d) Temporary Keyword Search Scheme Based on Key-Policy Attribute-Based Cloud Data Storage (KP-ABTKS). Notes for the Lecture System Netw 98:630–636
17. Ramesh G. [2021] An IoT with machine learning that offers a security intrusion detection system. 82:103741 Microprocess Microsyst
18. A survey on hybrid machine translation, Ramesh G. (2020). In: ICMED 2020, vol. 184, 2nd International Conference on Design and Manufacturing Aspects for Sustainable Energy
19. Aung KM, Chang V, Tan BH, Sundaram S, Wang T, Ng Y, and Ren SQ (2016) Homomorphic indexing improves cloud storage security searches. 65:102–110 in J Future Generation Computer System.