Journal of Advances in Developmental Research (IJAIDR)
E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Secure Data Storage and Retrieval Using Cloud Computing

N.Sunil Kumar[1], L. Yuvaraju[2], G. Swathi[3], K. Sai Pavani[4], D. Shekshavali[5]

[1,2,3,4,5]Department Of CSE, Tadipatri Engineering College, Tadipatri.

Abstract:
Cloud computing provides a flexible, scalable, and cost-effective platform for storing and managing data. However, data security and privacy remain major concerns due to the remote nature of cloud storage. This project focuses on developing a secure data storage and retrieval system. The Cloud provides service to the user on demand basis. The trend of using cloud environments is growing for storage and data processing needs. Data security is one of the major issues in cloud environment. The data owner has not control over the data after it is uploaded on cloud. We proposed a scheme in this the original data get encrypted into two different values Using sha-256 (Hashing Technique) and Homomorphic are combined to provide encryption. The data in each slice can be encrypted by using different cryptographic algorithm's and encryption key before storing them in the Cloud. The objective of this technique is to store data in a proper secure and safe manner in order to avoid intrusions and data attacks meanwhile it will reduce the cost and time to store the encrypted data in the Cloud Storage. Users can securely upload, store, and retrieve data without exposing it to unauthorized access

Keywords: Encryption, Decryption, AES Algorithm, RSA Algorithm, SHA256.

INTRODUCTION:

This project proposes a secure storage and retrieval system using SHA-256 and homomorphic encryption. Data is divided and encrypted with different algorithms before cloud storage. The main aim is to protect user data stored in the cloud from unauthorized access and cyberattacks. It is motivated by the growing need for data privacy and security in cloud environments. This project introduces strong encryption techniques like AES/RSA for secure storage. It also implements user authentication and access control to prevent misuse. Data integrity is ensured using cryptographic hash functions.

The system enables secure and efficient data retrieval. It provides a reliable and scalable solution for safe cloud storage. The project Secure Data Storage and Retrieval Using Cloud Computing focuses on addressing these security concerns by ensuring that data stored in the cloud remains confidential, intact, and accessible only to authorized users. This system uses security mechanisms such as data encryption, secure authentication, and integrity verification to protect sensitive information from attackers and malicious users.

By encrypting data before storing it in the cloud and decrypting it only during authorized retrieval, the proposed system ensures strong data protection. During data retrieval, the system decrypts the data only after successful authentication, ensuring secure and accurate access. By combining encryption,

authentication, and integrity verification, the proposed system enhances trust, privacy, and reliability in cloud environments. This project provides a secure framework suitable for applications such as healthcare, finance, and enterprise data management.

LITERATURE REVIEW:

[1] **The Authors "**C. Lou *"* **worked on the project"** A Secure Key-Aggregate Keyword Retrieval Scheme Over Encrypted Data in Cloud Computing," based on Servers, Public key , Cloud computing , Key-aggregate ,keyword retrieval , privacy, practicability . This approach is also inefficient. Firstly, the number of secret keys is proportional to the amount of shared files. A secure channel is needed to securely deliver the secret keys of all files and storing these key also requires secure storage. Nextly, the amount of trapdoors that users need to generate and submit for keyword search also relies on the number of files, with 86% accuracy. [2] The Authors "M. Morales-Sandoval, M. H. Cabello, H. M. Marin-Castro and J. L. G. Compean" worked on the project "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud " based on the Encryption, Access control , Task analysis , Attribute based encryption, asymmetric pairings, cloud storage, information retrieval, security , searchable encryption. n this paper we address the security concerns of cloud storage under the scenario where users encrypt-then-outsource data, share their outsourced data with other users, and the service provider can be queried for searching and retrieval of encrypted data, with 80% accuracy. [3] The Authors " L. Yong, L. Hefei, S. Xiujuan, Y. Bin and W. Kun" worked on the project "Keyword Semantic Extended Top-k Ciphertext Retrieval Scheme Over Hybrid Government Cloud Environment " based on the ;Government, Security, Semantics, Indexes, Data privacy, Hybrid government cloud, semantic extension, correlation score, ciphertext retrieval, privacy protection. The perspective of data security and confidentiality, its security and confidentiality will be challenged by all parties, which greatly hinder the construction and development of government cloud information sharing platform with 75% accuracy.[4] The Authors "M. Al-Shabi" worked on the project "An Enhance the Performance of Mining Vehicular and Machinery Security Systems Using Artificial Intelligence in VANET Cloud Computing" based on Measurement, Data dissemination, Clustering algorithms, Authentication, Artificial neural networks, Throughput Delays, Vehicular ad-hoc network-cloud, RSU, hash based authentication, firm aware clustering, emergency dissemination. Our major intention is to provide high level security in VANET-Cloud environment. In addition to it, we also reduce delay in emergency dissemination. Our proposed Delay aware Emergency Message Dissemination and Data Retrieval in secure (DEMD2RS) VANET-Cloud is composed of four sequential processes: Authentication, Clustering, Data Retrieval and Data dissemination with 78% accuracy.[5] The Authors" S. Chaterji" worked on the project " Lattice: A Vision for Machine Learning, Data Engineering, and Policy Considerations for Digital Agriculture at Scale" based on the Data integration, Soil, Digital agriculture, Fertilizers, Distributed databases, Data analysis, Intelligent sensors, Data integration , data analysis. Our paper starts off with the types of datasets in typical field operations, followed by the lifecycle for the data and storage, cloud and edge analytics, and fast information-retrieval solutions. We discuss what algorithms are proving to be most impactful in this space, with 80%accuracy. [6] The Authors "J. Liu " worked on the project "Secure Cloud-Aided Approximate Nearest Neighbor Search on High-Dimensional Data " based on the Outsourcing, Security, Nearest neighbor methods, Behavioral sciences, Hash functions, secure outsourcing, local sensitive hashing. The improper behavior of the cloud server, we also provide a verification method to check the results returned from the cloud server. Meanwhile, for the implementation of this scheme on resource-constrained devices, we proposed

a model for the real application of this scheme. To verify the efficiency and correctness of the proposed scheme, theoretical analysis and experiments are conducted with 78% accuracy. [7] The Authors "F. M. Ali, R. Latip, M. A. Alrshah, A. Abdullah and H. Ibrahim" worked on the project "Vigorous Replication Strategy With Balanced Quorum for Minimizing the Storage Consumption and Response Time in Cloud Environments" based on the Performance evaluation, Cloud computing, Time-frequency analysis, Power demand, Telecommunication traffic, Production processes, Time factors, Business continuity, Data models. This research proposes a new replication technique to improve the performance with a low vulnerability that would satisfy replication cloud users. Essentially, cloud replication must be able to secure huge data by enabling comprehensive replication strategies, optimal data availability, fast data retrieval, and cost-effective data management and maintenance with the 83% accuracy.[8] The Authors "A. F. S. Devaraj " worked on the project "An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme" based on the Feature extraction, Convolution, Image archival, secure image retrieval, deep learning, secret sharing scheme, multiple share creation. This article introduces a new secure image archival and retrieval system (SIARS) using deep learning and multiple share creation schemes. The proposed model involves adagrad based convolutional neural network (AG-CNN) based feature extractor to extract the feature vectors of the input images with 85% accuracy. [9] The Authors "S. Liu" worked on the project "Secure and Efficient Cross-Modal Data Retrieval in Internet of Things " based on the Cross modal retrieval, Cross-modal retrieval, K-modes clustering algorithm, locality-sensitive hashing (LSH);multimodal medical data. Building a privacy-preserving cross-modal retrieval (PPCMR) system that can achieve semantic association matching between different modalities and prevent data leakage has become one of the core challenges in the current field of secure integration of smart healthcare with 76% accuracy.[10] The Authors "H. Kwon and C. Hahn" worked on the project "Asymptotically Optimal and Secure Multi writer Multi reader Similarity Search," based on the Cryptography, Search problems, cloud computing security. These schemes use deterministic algorithms to encrypt data, which not only violates the privacy of data but also complicates the proof of semantic security. In this paper, we propose an efficient and secure multi writer/multi reader similarity search scheme over encrypted data in cloud storage. In the proposed scheme, the cloud server is able to perform searches without incurring any interaction between users and data owners. Thus, we achieve asymptotically optimal communication cost with 80% accuracy.[11] The Authors " Y. -W. Ti, C. -F. Wu, C. -M. Yu and S. -Y. Kuo" worked on the project "Benchmarking Dynamic Searchable Symmetric Encryption Scheme for Cloud-Internet of Things Applications" Servers, Indexes, Cloud computing, Encryption, Searchable encryption, dynamic searchable encryption. In these systems, to protect privacy, users query some information multiple times and receive the content of the query, but their identity or the content of the stored message is not revealed. Over the years, several studies have focused on protecting databases from malicious users. An attacker can recreate a valuable message by querying the database with 83% accuracy.[12] The Authors " A. Alkhalil " worked on the project "A Framework for Blockchain-Based Secure Management of Mobile Healthcare (mHealth) Systems," based on the Energy efficiency, Blockchains, Computational efficiency, Inter Planetary File System, Time factors, Mobile computing. The proposed framework has been implemented as a frontend using a mobile application interface that exploits the backend via the Inter Planetary File System (IPFS) system and Ethereum blockchain for secure management of mHealth data. We use a case-study-based approach demonstrating how health units, medics, and patients can securely access and distribute health-critical data with 76% accuracy.[13] The Authors "E. U. Haque" worked on the project "Scalable EdgeIoT Blockchain Framework Using EOSIO"

based on the edge computing, data sharing, delegated proof of stake, interplanetary file system. The proposed framework is implemented in the EOSIO blockchain. This study experiments show significant improvement in the throughput, latency and resource utilization compared to the state-of-the-art solutions in the blockchain with the accuracy 80% accuracy.[14] The Authors "S. Mehrban" worked on the project "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges " based on the Investment, FinTech, security privacy, cyber security threats, fraud detection. The development of FinTech is indebted to the mutual integration of different state of the art technologies, for example, technologies related to a mobile embedded system, mobile networks, mobile cloud computing, big data, data analytics techniques, and cloud computing with the 80% accuracy. [15] The Authors "Blockchain X. Yang, G. Chen, M. Wang, T. Li and C. Wang" worked on the project "Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme" based on certificateless cryptosystem, multi-keyword, searchable encryption. We propose a multi-keyword certificateless searchable public key authenticated encryption scheme based on blockchain. We use certificateless cryptosystem to encrypt keywords, which avoids the problems of certificate management in traditional cryptosystem and key escrow in identity-based cryptosystem with the 75% accuracy.

PROPOSED METHODOLOGY:

In this project we can observe that the proposed system is designed to securely store and retrieve data using cloud computing. First, users register and log in to the system using valid credentials. Only authorized users are allowed to access the cloud services. Before storing any data in the cloud, the data is encrypted using secure encryption techniques so that the information remains confidential. The encrypted data is then uploaded and stored in the cloud server. This ensures that even the cloud service provider cannot read the original data. To maintain data integrity, a hash value is generated for each file before storage. When a user requests the data, the system verifies the user's identity and access permissions. After successful verification, the encrypted data is retrieved from the cloud. When a data retrieval request is initiated, the system validates the user's authorization. Upon successful verification, the encrypted data is downloaded from the cloud and decrypted using appropriate keys at the client side. The integrity of the retrieved data is verified by comparing hash values. This methodology ensures confidentiality, integrity, and secure access to cloud-based data. The system also provides data integrity verification to ensure that stored data has not been modified or tampered with in addition, secure login and access control mechanisms are implemented to prevent unauthorized access. This ensures data privacy, integrity, and trustworthiness for users storing their information in the cloud.

SYSTEM ARCHITECTURE:

FIG 1.SYSTEM ARCHITECTURE

The system architecture for secure data storage and retrieval using cloud computing is designed to protect data confidentiality, integrity, and authorized access. Initially, the data owner or user provides plain data, which is processed by the encryption module using secure algorithms such as AES or RSA. This encryption converts the original data into unreadable ciphertext before it is uploaded to the cloud. As a result, even if the cloud storage is accessed by unauthorized parties, the stored data remains secure and protected from misuse.

When an authorized user requests the data, the request is verified through the access control and authentication mechanism. After successful verification, the encrypted data is retrieved from the cloud storage and passed to the decryption module. Using valid secret keys, the data is converted back into its original readable form and delivered to the user. This process ensures that only authenticated users can access the data while maintaining security during storage and transmission.

RESULT AND DISCUSSION:

CSecure data storage and retrivel using cloud computing has been successfully completed using both software and hardware components. The system allowed only authenticated users to upload and retrieve data from the cloud, ensuring secure access control. All files were encrypted before being stored in the cloud, which prevented unauthorized users and cloud service providers from accessing the original data. The encryption and decryption processes worked efficiently with minimal delay during data upload and download. Hash-based integrity verification successfully detected any unauthorized modifications to stored data. Whenever the file content was altered, the hash values did not match, indicating data tampering. User authentication ensured that only valid users could access the system, thereby strengthening access control. The use of hash functions for integrity verification ensured that stored data remained unchanged and trustworthy during storage and transmission. Although the system introduced slight computational overhead due to encryption and hashing, the security benefits greatly outweighed the performance cost. The proposed approach is suitable for applications that require secure cloud storage, such as business data management, academic records, and personal file storage.

SCREENSHOTS

FIG 2.HOME PAGE

FIG 3. REGISTER PAGE

FIG 4. LOGIN PAGE

FIG 5.DATA STORE

FIG 6.CLOUD STORAGE

CONCLUSION AND FUTURE SCOPE:

This project demonstrates about the successfully addresses major security challenges related to cloud-based data storage. The system ensures that data is protected from unauthorized access by using user authentication, data encryption, and integrity verification techniques. All data is encrypted before being stored in the cloud, which maintains confidentiality and prevents data misuse by attackers or cloud service providers. The implemented methodology provides secure and reliable data retrieval only to authorized users. Hash-based integrity checking ensures that stored data remains unaltered during storage and transmission. The results demonstrate that the proposed system improves data security while maintaining efficient performance. Overall, this project proves that secure data storage and retrieval in cloud environments can be effectively achieved using cryptographic techniques.

The future scope of this project can be extended in several ways to enhance security and functionality advanced encryption algorithms and hybrid cryptographic techniques can be implemented to further strengthen data security. Multi-factor authentication can be added to improve user identity verification. Blockchain technology can be integrated to provide tamper-proof data storage and transparent auditing. Role-based access control can be enhanced to support large-scale organizations. Machine learning techniques can be used to detect abnormal access patterns and security threats.

REFERENCES:

1. C. Lou *et al*., "A Secure Key-Aggregate Keyword Retrieval Scheme Over Encrypted Data in Cloud Computing," in *IEEE Access*, vol. 13, pp. 123429-123439, 2025, doi: 10.1109/ACCESS.2020.2980886**.**
2. M. Morales-Sandoval, M. H. Cabello, H. M. Marin-Castro and J. L. G. Compean, "Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud," in *IEEE Access*, vol. 8, pp. 170101-170116, 2020, doi: 10.1109/ACCESS.2020.3023893.
3. L. Yong, L. Hefei, S. Xiujuan, Y. Bin and W. Kun, "Keyword Semantic Extended Top-k Ciphertext Retrieval Scheme Over Hybrid Government Cloud Environment," in *IEEE Access*, vol. 9, pp. 155249-155259, 2021, doi: 10.1109/ACCESS.2021.3128933.
4. M. Al-Shabi, "An Enhance the Performance of Mining Vehicular and Machinery Security Systems Using Artificial Intelligence in VANET Cloud Computing," in *Journal of Mobile Multimedia*, vol. 18, no. 6, pp. 1733-1776, November 2022, doi: 10.13052/jmm1550-4646.18612.
5. S. Chaterji *et al*., "Lattice: A Vision for Machine Learning, Data Engineering, and Policy Considerations for Digital Agriculture at Scale," in *IEEE Open Journal of the Computer Society*, vol. 2, pp. 227-240, 2021, doi: 10.1109/OJCS.2021.3085846.
6. J. Liu *et al*., "Secure Cloud-Aided Approximate Nearest Neighbor Search on High-Dimensional Data," in *IEEE Access*, vol. 11, pp. 109027-109037, 2023, doi: 10.1109/ACCESS.2023.3321457.
7. F. M. Ali, R. Latip, M. A. Alrshah, A. Abdullah and H. Ibrahim, "Vigorous Replication Strategy With Balanced Quorum for Minimizing the Storage Consumption and Response Time in Cloud Environments," in *IEEE Access*, vol. 9, pp. 121771-121785, 2021, doi: 10.1109/ACCESS.2021.3108765.
8. A. F. S. Devaraj *et al*., "An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme," in *IEEE Access*, vol. 8, pp. 144310-144320, 2020, doi: 10.1109/ACCESS.2020.3014346.
9. S. Liu *et al*., "Secure and Efficient Cross-Modal Data Retrieval in Internet of Things," in *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 42239-42249, 15 Oct.15, 2025, doi: 10.1109/JIOT.2025.3592790.
10. H. Kwon and C. Hahn, "Asymptotically Optimal and Secure Multiwriter/Multireader Similarity Search," in *IEEE Access*, vol. 10, pp. 101957-101971, 2022, doi: 10.1109/ACCESS.2022.3208962.
11. Y. -W. Ti, C. -F. Wu, C. -M. Yu and S. -Y. Kuo, "Benchmarking Dynamic Searchable Symmetric Encryption Scheme for Cloud-Internet of Things Applications," in *IEEE Access*, vol. 8, pp. 1715-1732, 2020, doi: 10.1109/ACCESS.2019.2961971.
12. A. Alkhalil *et al*., "A Framework for Blockchain-Based Secure Management of Mobile Healthcare (mHealth) Systems," in *Journal of Web Engineering*, vol. 24, no. 3, pp. 317-354, May 2025, doi: 10.13052/jwe1540-9589.2431.

13. E. U. Haque *et al*., "Scalable EdgeIoT Blockchain Framework Using EOSIO," in *IEEE Access*, vol. 12, pp. 41763-41772, 2024, doi: 10.1109/ACCESS.2024.3377119.
14. S. Mehrban *et al*., "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges," in *IEEE Access*, vol. 8, pp. 23391-23406, 2020, doi: 10.1109/ACCESS.2020.2970430.
15. Blockchain X. Yang, G. Chen, M. Wang, T. Li and C. Wang, "Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on," in *IEEE Access*, vol. 8, pp. 158765-158777, 2020, doi: 10.1109/ACCESS.2020.3020841.