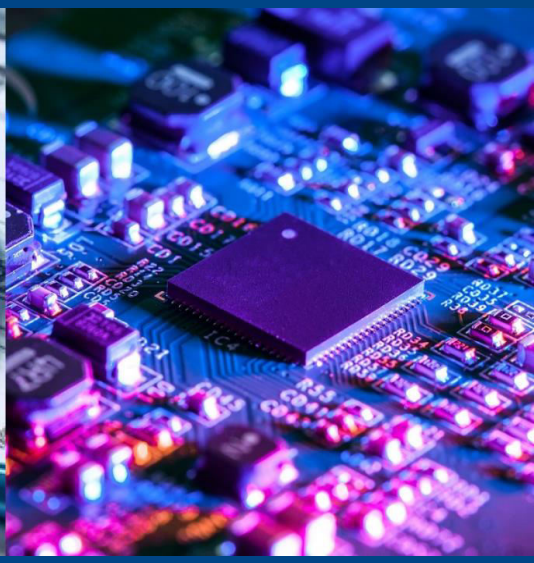
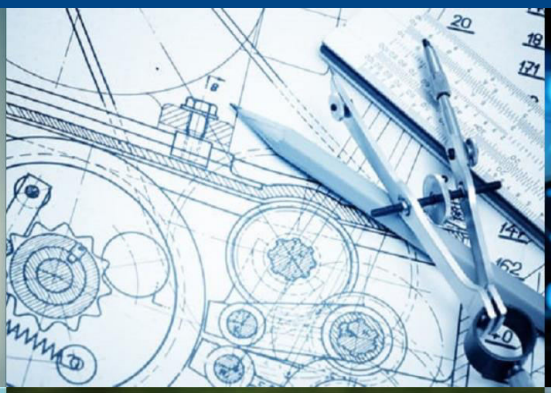
ISSN: 2582-7219

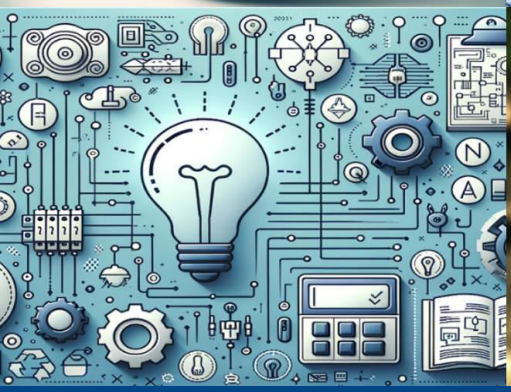




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904186

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cloud Based File Storage with Encryption

Arun Kumar S, Prof. Dr. Charles Arockiaraj M

Student, Department of MCA, AMC Engineering College, Bengaluru, India

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Cloud computing which offers cost-effectiveness scalability and flexibility has completely changed how data is accessed and stored. However there are serious security and privacy issues when storing sensitive data on cloud platforms.

This paper describes a cloud-based file storage system that is integrated with cutting-edge encryption methods to guarantee data integrity and confidentiality. Users can safely upload store and retrieve files from the cloud using the suggested system which also shields them from unwanted access.

Strong encryption algorithms are used to encrypt files prior to uploading guaranteeing that even in the event that data is intercepted or accessed by malicious parties it will remain unreadable without the appropriate decryption key. To improve security the system also includes user authentication procedures. This solution also maintains high security standards while offering dependable performance easy accessibility and effective file management. The suggested model guarantees a safe and convenient setting for data storage by fusing cloud technology with encryption.

KEYWORDS: Cloud computing file storage, encryption data privacy secure storage, cloud security,cryptography data protection and user authentication.

I. INTERODUCTION

The cloud It is very effective and economical for both individuals and businesses because it offers on-demand services like networking storage and processing power. Cloud-based file storage systems are becoming more and more in demand as smartphones laptops and internet services are used more frequently.

Cloud storage ensures high availability and convenience by enabling users to upload access and share files from any location in the world. Cloud storage is frequently used for file sharing data backup large-scale data management and collaboration. Despite these advantages there are a number of serious security issues with cloud computing that need to be resolved. Data security and privacy are among the main issues with cloud storage.

In conclusion a solid solution to todays data storage problems is offered by combining cloud computing with robust encryption techniques. . This project aims to deliver a reliable cloud storage system that meets the growing demand for data protection in today's digital world.

Cloud-based file storage systems have become increasingly popular due to the quick rise in digital data and internet usage. Cloud storage enhances productivity and teamwork by enabling users to upload access and share files at any time and from any location. Data backup file sharing online collaboration and enterprise data management are just a few of the many uses for it. However these benefits come with a number of unavoidable security risks associated with cloud computing. Privacy and data security are two of the main issues.

II. ARCHITECTURE IN WEBSITE

In order to offer safe and effective cloud file storage with encryption the suggested system is built as a web-based application using a client-server architecture. The architecture is made up of several parts such as the database cloud storage front-end and back-end server all of which cooperate to guarantee data security and seamless operation.

Users can register log in upload download and manage their files using the user-friendly interface of the front-end which was created using web technologies. Between the user and the system it serves as the interaction layer.When a

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

user uploads a file the back-end first transforms it into a secure format by processing it and applying encryption. After that this encrypted file is kept in cloud storage which offers high availability scalability and dependability.

The database is used to safely store user credentials file information and other essential data hashing techniques are frequently used for sensitive data. The encrypted file is retrieved from cloud storage and sent to the server during file retrieval where it is decrypted using the proper key While preserving effective performance and usability this layered architecture guarantees that data is shielded from unwanted access.

III. RELATED WORK

In order to address concerns about data privacy confidentiality and secure access numerous studies have been conducted in the field of cloud storage security. Many researchers have concentrated on incorporating access control and encryption methods to improve the security of stored data as cloud computing becomes more widely used.

Previous systems were susceptible to data breaches and unauthorized access because they primarily concentrated on offering basic cloud storage services without robust security measures. Several encryption-based strategies were introduced to get around these restrictions.

The high speed and effectiveness of symmetric encryption algorithms like AES in protecting vast volumes of data have led to their extensive use. Conversely secure key exchange and authentication are accomplished through asymmetric encryption methods such as RSA. Hybrid encryption models which combine symmetric and asymmetric techniques to enhance overall security and performance have been proposed in some research studies.

Symmetric keys are used in these systems to encrypt data and asymmetric encryption is employed to safely distribute the keys among users. Strong security and efficiency are provided by this method. To stop unwanted access a number of studies have concentrated on using sophisticated authentication methods like multi-factor authentication and role-based access control in addition to encryption.

To further bolster cloud security additional strategies include intrusion detection systems secure data sharing and data integrity verification. Notwithstanding these developments issues like key management system complexity and performance overhead persist. By combining effective encryption methods with an intuitive web-based system this project expands on previous research and offers safe dependable and user-friendly cloud file storage.

IV. METHODOLOGY

The suggested system designs and implements a safe encrypted cloud-based file storage system using a methodical approach. To guarantee data security effective processing and user accessibility the methodology entails a number of steps. First by entering the required information users can register and create an account. Users can safely log in with their credentials after registering. To confirm user identity and stop illegal access to the system authentication procedures are used.

The web interface allows users to upload files once they have successfully logged in. The system uses encryption to transform the original data into a safe unintelligible format before storing the file in the cloud. High security and efficiency are ensured by using an appropriate encryption algorithm such as AES

After that the encrypted file is uploaded and kept in the cloud. In order to facilitate management and retrieval the file is stored in the database along with essential metadata like file name size and upload time.

This guarantees that stored files are properly organized and accessible. The file is then restored to its original format by applying the decryption process with the appropriate key. Finally the authorized user receives the decrypted file.By limiting file access to only authorized users the system protects the confidentiality and integrity of data.

The system uses encryption to transform the original data into a safe unintelligible format before storing the file in the cloud. High security and efficiency are ensured by using an appropriate encryption algorithm such as AES.

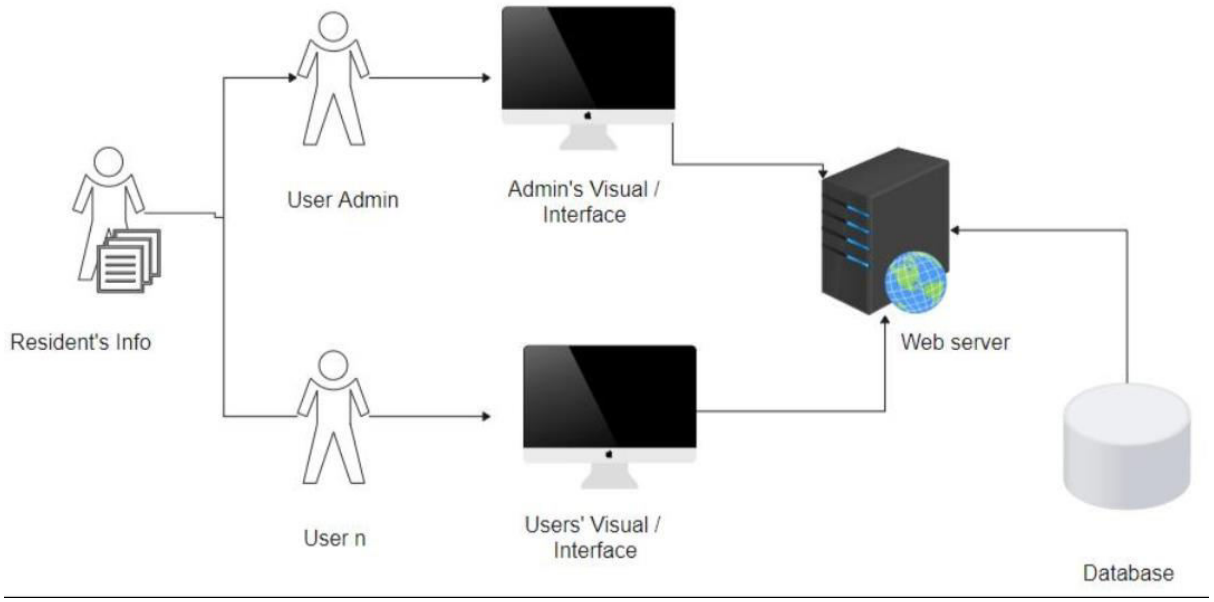
© 2026 IJMRSET | Volume 9, Issue 4, April 2026| DOI:10.15680/IJMRSET.2026.0904186

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 1:Flow Digram of Architecture.



IV.1. PROBLEM IDENTIFICATION & REQUIREMENTS ANALYSIS:

Cloud computings quick uptake has revolutionized data access and storage but it has also created serious security risks. Since users store their private data on third-party cloud servers one of the main issues is the lack of data control. Concerns regarding illegal access data breaches and improper use of private information are brought up by this Data integrity where stored files may be changed or corrupted without the users knowledge is another significant concern. Because incorrect handling of encryption keys can jeopardize the security system as a whole key management is another difficult task. Additionally a lot of cloud storage solutions have performance problems like sluggish data access file transfer delays and restricted scalability when managing massive data volumes.

These issues show that a more effective and secure system is required. The suggested system focuses on putting robust encryption methods in place in addition to safe authentication and access control procedures in order to overcome these difficulties. In order to prevent unwanted access the system makes sure that files are encrypted before being uploaded to the cloud.

IV.2. ARCHITECTURAL DESIGN

The suggested systems architecture is built on a layered client-server model that guarantees effective scalable and safe cloud-based file storage with encryption. To maintain appropriate system organization and security the system is divided into several layers such as the presentation layer application layer and data storage layer. he user interface that allows users to interact with the system is provided by the presentation layer or front-end. It enables users to carry out tasks like registering logging in uploading and downloading files. This layer is made to be responsive and easy to use making accessibility and navigation simple.

IV.3. TECHNOLOGY STACK & DEVELOPMENT ENVIRONMENT:A combination of front-end back-end database and cloud technologies are needed to develop the suggested cloud-based file storage system with encryption Technologies like HTML CSS and JavaScript are used in front-end design to create an interface that is both responsive and easy to use Python Java and Node are examples of programming languages used for the back-end. The server-side logic can be implemented with js. Encryption and decryption file processing session management and user requests are all handled by the back-end. frameworks such as Express and Django (Python). js (Node. js) can enhance performance and make development easier. Depending on the needs of the system databases like MySQL PostgreSQL or MongoDB may be utilized. Hashing techniques are used to securely store sensitive information such as passwords. Standard

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

cryptographic algorithms like RSA (Rivest–Shamir–Adleman) and AES (Advanced Encryption Standard) are used for encryption to guarantee data security and confidentiality. These algorithms aid in data security during transmission and storage.

IV.4 DATASET COLLECTION & PREPROCESSING: The idea of a traditional dataset is somewhat different in the suggested cloud-based file storage system with encryption since the system mainly manages user-uploaded files rather than a fixed dataset Through the web interface users input data is gathered as part of the data collection process. In addition to the files other data is gathered and kept in the database as metadata including file name file size file type and upload time. During registration user-related data is also gathered such as the username password and access credentials. Preprocessing is done before the data is stored in the cloud to guarantee efficiency security and consistency. To stop malicious or unsupported files from being uploaded this involves verifying the file type and size. In order to maximize storage capacity and enhance performance the system may also format and compress files. Data encryption is a crucial component of preprocessing encryption algorithms like AES are used to transform the uploaded file into an unintelligible format. This guarantees that even in the event of unauthorized access the data stays safe. Additionally before being stored in the database sensitive user data like passwords is processed using hashing techniques.

IV.5 CNN MODEL IMPLEMENTATION: Although the primary focus of this project is secure cloud-based file storage with encryption, a Convolutional Neural Network (CNN) model can be integrated for advanced functionalities such as image classification, file content analysis, or intelligent data management.The CNN (Convolutional Neural Network) is a deep learning algorithm commonly used for processing image data. It consists of multiple layers such as convolutional layers, pooling layers, and fully connected layers, which help in extracting features and making predictions.In this system, the CNN model can be used to analyze image files uploaded by users. During implementation, image datasets are first collected and preprocessed, which includes resizing images, normalization, and labeling. The preprocessed data is then fed into the CNN model for training.

IV.6 PERFORMANCE EVALUATION: The suggested cloud-based encrypted file storage systems performance is assessed using a number of crucial criteria including scalability security efficiency and dependability. The assessment guarantees that the system satisfies the necessary goals and operates efficiently in various scenarios. Security performance is one of the main factors taken into account. Before storing data in the cloud the system encrypts it using robust methods. This guarantees that the data is unreadable even in the event of unauthorized access. By limiting access to only those who are authorized user authentication techniques further improve security. System efficiency which is gauged by file upload and download speeds is another crucial component. Appropriate optimization strategies are used to speed up processing and boost system responsiveness. The systems ability to reliably store and retrieve data without errors or failures is how reliability is assessed. Users can access their files at any time without interruption thanks to cloud storages high availability. Data loss can also be avoided with the use of backup systems.

V. FUTURE UPDATES:

A number of cutting-edge features and enhancements can be added to the suggested cloud-based file storage system with encryption to boost its effectiveness security and usability. The goal of upcoming updates is to improve performance by incorporating contemporary technologies and resolving current issues. Using multi-factor authentication (MFA) to add an extra layer of security is one of the main upcoming improvements. This lowers the possibility of unwanted access by requiring users to confirm their identity using several techniques. To further strengthen data protection more sophisticated encryption methods and better key management systems have been integrated. Real-time file sharing and collaboration features which enable numerous users to safely access and work on files at once can also be added to the system. Additionally managing user privileges more successfully can be achieved by putting access control mechanisms like role-based permissions into place.

VI. CONCLUSIONl:

In conclusion the suggested encrypted cloud-based file storage system offers a safe and effective way to manage data in cloud environments The system protects sensitive data even in the event of security breaches by encrypting files before storing them in the cloud. Users can upload access and manage their files with ease from any location at any time thanks to the integration of a web-based interface. High availability scalability and dependability are further benefits of using cloud storage. In terms of speed efficiency and data integrity the system also performs well. Strong security is

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

maintained with little delay when encryption and decryption procedures are handled correctly. The system is adaptable and simple to maintain or upgrade in the future thanks to its modular architecture. All things considered this project effectively integrates encryption and cloud computing technologies to produce a dependable safe and user-friendly file storage system. It satisfies the increasing need for secure data storage options and offers a solid base for upcoming improvements and cutting-edge features.

REFERENCES

1. Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology.
2. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
3. Kaufman, C., Perlman, R., & Speciner, M. (2015). *Network Security: Private Communication in a Public World*. Prentice Hall.
4. Zhang, Q., Chen, M., Li, L., & Tseng, M. (2010). *Cloud Computing: State-of-the-Art and Research Challenges*. Journal of Internet Services and Applications.
5. Armbrust, M., et al. (2010). *A View of Cloud Computing*. Communications of the ACM.
6. Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM.
7. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer.
8. Amazon Web Services (AWS). *Cloud Storage Documentation*.
9. Google Cloud Platform. *Cloud Storage and Security Documentation*.
10. Microsoft Azure. *Cloud Security and Storage Services Documentation*.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com