Design A Secure Cloud Storage for Data Privacy Using Artificial Intelligence

Vikas Gaund[1], Vinay Kumar[2], Mrs. Richa Pandey[3]
[1,2]*Department of Computer Application BBD University, Lucknow - 226 028, India*
[3]*Assistant Professor Department of Computer Application, BBD University, Lucknow - 226 028, India*
doi.org/10.64643/IJIRT209613

***Abstract*—Storing information with an outside cloud vendor gives users flexible, pay-as-needed capacity, yet it also puts privacy, confidentiality, integrity and access control at risk. This paper describes the design of a cloud storage platform that pairs cryptographic protection with machine intelligence to keep user files safe. The planned architecture is built from six tiers: the user interface, authentication and authorization, activity monitoring, AI-based detection, encryption with storage, and a security response tier. Every file is encrypted before it is saved and is decrypted only once the requester passes authorization. A machine learning module studies how users behave, labels each session as normal or suspicious, and raises alerts or demands extra verification when something looks wrong. The work follows an experimental design-and-development approach in which the AI model is trained and tested on its own prior to integration. The intended result is a functioning prototype that shows encrypted storage together with AI-driven threat detection.**

***Index Terms*—Cloud Storage, Data Storage, Cloud Services, Data Privacy, Data Security, Artificial Intelligence.**

I. INTRODUCTION

The term “cloud” has its roots in network drawings, in which engineers sketched a cloud outline to represent a set of linked machines whose inner workings were unimportant to the diagram. [1]

Today the cloud is a distributed and highly scalable setting where processing power, storage and software are supplied as network services. Businesses of all sizes rely on it to rent virtual resources when they need them, without buying or looking after physical hardware. [2]

Fig. 1. Cloud computing overview.

A. Cloud Architecture

A cloud platform is commonly described as two sides that work together:

1. Frontend: the part that customers touch, meaning the web pages and applications used to reach cloud services.
2. Backend: the provider-managed part, which contains the servers, storage systems, virtual machines, traffic handling and security mechanisms that keep the services running.

B. Cloud Computing Reference Models

1) Service Models

Software as a Service (SaaS): Finished applications are offered over the internet, and users simply sign in to use them.

Platform as a Service (PaaS): Developers get a managed environment in which they can write and run their own applications, with no need to administer the servers beneath.

Infrastructure as a Service (IaaS): Basic computing building blocks, namely virtual machines, storage and network capacity, are leased to customers, who set them up as they see fit.

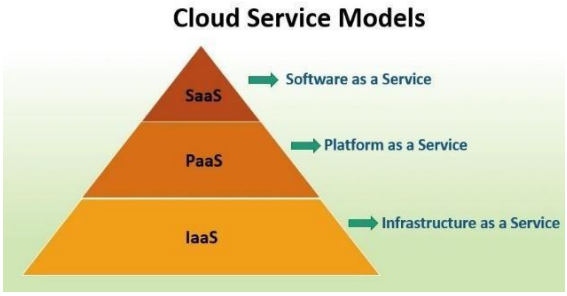

Fig. 2. Cloud service models.

2) Deployment Models

Public: An external vendor owns and runs a public cloud and shares it among many clients, so pay-per-use billing keeps expenses small.

Private: A private cloud is reserved for one organization, which therefore keeps closer control of its information.

Hybrid: A hybrid cloud joins public and private environments, letting workloads shift between them according to need.

Fig. 3. Cloud deployment models.

II. RELATED WORK

1. Several authors present the move to cloud computing as a change that creates fresh difficulties for data protection and access management. [3]
2. Because customers pay only for what they use and can expand almost without limit, cloud storage has become attractive to firms that want elastic capacity.
3. After data is uploaded, its owners stop operating the machines that hold it, which causes concern over privacy and safety. At present no single standard addresses all of these concerns. [4]
4. Since clouds depend on pooled resources, distant infrastructure and many concurrent users, published studies keep returning to confidentiality, integrity, availability, authentication and access control.
5. Attackers are typically grouped into insiders, who abuse the access they legitimately hold, and outsiders, who strike through the network or capture data handled by third parties.
6. One line of research concentrates on identity management and proposes designs centred on authentication and authorization services for cloud applications. [5]
7. Where data is sensitive, a password alone is usually regarded as inadequate; extra factors such as fingerprints or one-time keys raise the level of protection. [6]
8. Newer investigations look at framework-oriented, malware-prevention and AI-based techniques for protecting cloud storage and computation. [8]–[17]

III. PROBLEM FORMULATION

This study investigates how files can remain private inside a cloud run by another party while unusual user behaviour is still found automatically. The project is named “Design a Secure Cloud Storage for Data Privacy Using Artificial Intelligence.” [7]

Its design is experimental and analytical, joining quantitative modelling with validation by simulation. [7]

The overall strategy is a hybrid one, mixing data-driven learning, system modelling and a side-by-side comparison of measured results. [7]

IV. CLOUD COMPUTING AND SECURITY MODEL

Danger to cloud data arrives from two sources. Insiders can misuse the access they are granted, whereas outsiders may attempt to break in or intercept data managed by third parties, which could expose personal details of users. In addition, the infrastructure has to scale well so that information stays reachable. [1]

Six principal security concerns are listed here:

In simple terms: when files are kept on someone else’s servers, six things can go wrong. Each concern below is a question the system must be able to answer; Table I explains each one and shows how this project addresses it.

TABLE I. SIX PRINCIPAL SECURITY CONCERNS

#	Concern	Simple meaning	How addressed
1	Integrity of stored data	Files must not be changed or corrupted without permission	Access checks before any file operation
2	Privacy and confidentiality of user data	Only the owner should be able to read the data	Encryption before storage
3	Physical or geographic location of data	You should know where your data physically sits	Defined in the architecture and storage design
4	Continuous availability of data	Files must be reachable whenever needed	Monitoring and security response layer
5	Storage, backup and recovery arrangements	Data must survive crashes or loss	Secure storage layer (backup is future work)
6	Verifying the identity of data users	The system must be sure who is logging in	Authentication and authorization layer

Cloud security is the set of controls, policies and technologies that guard cloud-based infrastructure, applications and data. [2]

A. Access Control Model

1) Role-Based Access Control (RBAC): Permissions are attached to job roles, so administrators maintain roles rather than handling each person one by one.

2) Attribute-Based Access Control (ABAC): Decisions rest on properties of the user, the resource and the circumstances, such as the time of day or the location.

3) Fine-Grained Access Control: This extends the idea further by tuning access to the sensitivity of the data, the behaviour seen from the user and the surrounding context.

TABLE II. ACCESS CONTROL MODELS COMPARED

Model	Basis of the access decision
RBAC	User's job role
ABAC	Attributes of the user, the resource and the situation (e.g., time, location)
Fine-grained	Data sensitivity, observed user behavior and context

B. Typical Components of a Cloud Security Model

In simple terms: a cloud security model is like the security of a bank, with guards, locks, ID checks, cameras and rules. Each component protects one part of the system (Table III).

TABLE III. TYPICAL COMPONENTS OF A CLOUD SECURITY MODEL

#	Component	Simple meaning	Bank analogy
1	Physical protection of data centers	Guards, locks and CCTV around the buildings that hold the servers	Bank building and vault door
2	Network security	Firewalls and safe connections that block attackers	Armored van and secure routes
3	Identity and access management (IAM)	Deciding who you are and what you may access	ID card and account permissions
4	Data protection	Encrypting and safely handling the data itself	Locking cash in a safe
5	Application security	Software and apps without weak spots	Counters and machines that cannot be tricked
6	Monitoring and incident response	Watching activity and acting fast when something looks wrong	Cameras and alarm response team
7	Compliance and legal requirements	Following laws and standards on data handling	Banking regulations and audits
8	Security practices of the cloud provider	How well the cloud company protects its own systems	The bank's own staff rules

C. Security Reference Model of Cloud Computing

The cloud security reference model is independent of the deployment choice, so one method fits private, community and hybrid clouds alike.

It adopts a risk-driven perspective. For each participant in the cloud, it identifies the controls that participant must answer for during the whole service lifecycle, and each component is reviewed in every cloud instance to judge how much each participant contributes to implementing it. [2]

D. Cloud Computing Security Issues and Problems

1. Data loss or leakage
2. Hijacking of user accounts
3. Insecure interfaces and APIs
4. Denial-of-service (DoS) attacks

V. METHODOLOGY

A design-and-development method will guide the research. The first step is a literature study of the cloud-storage security problem. The second is to define system requirements and architecture. The prototype is then built module by module.

The AI module will be trained and assessed independently, and only afterwards merged with the storage application. The final step is testing and evaluating the complete system.

In simple terms: the research follows a step-by-step plan, like building a house: study first, then plan, then build in parts, then test everything (Table IV).

TABLE IV. STAGES OF THE RESEARCH METHODOLOGY

#	Stage	What happens	Simple example
1	Literature study	Read existing research on cloud-storage security	Learning how others solved the problem
2	Requirements and architecture	Decide what the system must do and draw its design	Making the house blueprint
3	Build module by module	Create each part (login, upload, encryption) separately	Building one room at a time
4	Train and test the AI module alone	Teach and check the AI before merging it	Testing the alarm before installing it
5	Merge, test and evaluate	Combine all parts and test the full system	Final inspection of the house

A. Proposed Architecture

The architecture is organised into six layers: user interface, authentication and authorization, activity monitoring, AI detection, encryption and storage, and security response.

The monitoring path runs User Interface → Authentication → Activity Monitoring → AI Detection → Security Decision.

Alongside it, uploaded files pass through Encryption → Secure Storage. When an authorized download is requested, the system checks authorization first and only then performs Decryption → User.

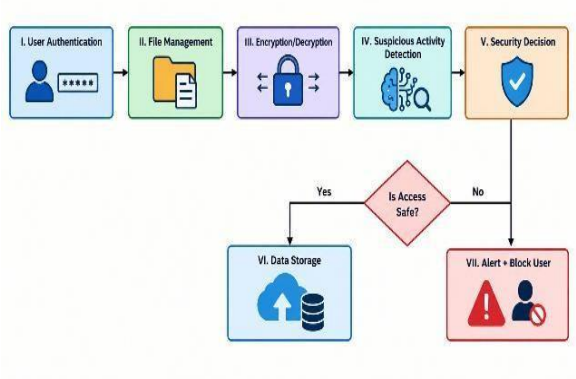

Fig. 4. Proposed system architecture.

TABLE V. LAYERS OF THE PROPOSED ARCHITECTURE

Layer	Role in the proposed design
User interface	Web front end for uploading and fetching files
Authentication and authorization	Confirms identity and checks permissions before access is given
Activity monitoring	Collects features of user activity for analysis
AI detection	ML module that labels behavior as normal or suspicious
Encryption/storage	Encrypts files before saving; decrypts only after authorization
Security response	Warning, extra verification or temporary restriction

VI. RESULT & DISCUSSIONS

In simple terms: the project promises four results at the end, summarized in Table VI and described below.

TABLE VI. EXPECTED OUTCOMES OF THE PROJECT

Outcome	What it means	How success is shown
A. Secure cloud storage prototype	A working web app where an authorized user can upload and download files	The app runs and core functions work
B. Encrypted file storage	Files are saved as unreadable ciphertext and decrypted only after authorization	Stored files cannot be read directly
C. AI-based suspicious activity detection	An ML model labels user behavior as normal or suspicious	Measured by experiments (accuracy, false positives)
D. Security alert mechanism	The system reacts when something suspicious is found	A warning, extra verification or temporary restriction is triggered

A. Secure Cloud Storage Prototype

The first anticipated result is a working prototype through which an authorized user can upload and download files using a web interface. It will illustrate the core behaviour of a cloud storage service without trying to match every feature of a commercial provider.

B. Encrypted File Storage

Files will be encrypted prior to being saved. The work will show that what sits in storage is ciphertext and not readable content, and that authorized retrieval decrypts the file only after the proper checks.

C. AI-Based Suspicious Activity Detection

The second main result is an ML component that examines activity features and labels behaviour as normal or suspicious. Its effectiveness will be measured through experiments and not taken for granted.

D. Security Alert Mechanism

When suspicious activity is found, the system will respond with an alert or a security action. Depending on the final prototype, this may be a warning, a request for additional verification, or a temporary restriction.

VII. CONCLUSION

In simple terms, the main points of this work are:

1. The problem: users give up direct control over where and how their data is kept, so privacy is a core difficulty in cloud storage.
2. The solution: this paper puts forward a layered design that combines encryption, access control and AI-based detection of suspicious activity.
3. Encryption protects confidentiality, because files are locked before they are stored.
4. AI monitoring adds forward-looking protection that static controls cannot offer.
5. Honest limits: the prototype is not expected to defend against every attack; its results depend on the quality of the dataset, the rate of false positives and careful handling of keys.
6. Overall value: joining cryptographic protection with intelligent monitoring is a promising path toward stronger cloud security.
7. Future work: testing the model on larger, more realistic datasets, improving key management and evaluating the system at greater scale.

REFERENCES

[1] N. Sahu and S. Sharma, “Resolving data security issues and challenges through the encryption algorithm,” Shodhganga, 2024.

[2] A. A. Yusufzai and M. Vora, “Design and development of security model for cloud computing,” Shodhganga, 2023.

[3] A. Agarwal, “A review of cloud security issues and challenges,” Google Scholar, 2023.

[4] S. V. Divya and R. S. Shaji, “An efficient and secured data forwarding scheme for cloud storage environment,” Shodhganga, 2017.

[5] A. A. Yusufzai, “Design and development of security model for cloud computing,” Shodhganga, 2023.

[6] S. B. Patel, “New method in data security and privacy in cloud computing,” Shodhganga, 2024.
[7] A. Kumar, “Framework development to upgrade security aspect in cloud computing using artificial neural networks,” Shodhganga, 2026.
[8] “IoT-enabled secure and scalable cloud architecture for multi-user.”
[9] A. Agarwal, S. B. Verma, B. K. Gupta, S. K. Patel, and S. M. Tiwari, “Enhancing cloud security: A hypervisor-level framework for malware prevention and detection,” 2025.
[10] S. P. Shaik, “Enhancing cloud computing security through deep learning: An artificial neural network approach.”
[11] N. Shivani, “A study for improved secure cloud data storage frameworks by providing data privacy, integrity and availability of single owner and multi user data,” Shodhganga, 2025.
[12] A. Mohammed, “Secure data storage and malicious TPA detection in a cloud environment using public auditing,” Shodhganga, 2022.
[13] “Artificial intelligence techniques for secure cloud data storage and retrieval using giant trevally optimizer with quantum convolutional neural network-based encryption algorithm: Trends and challenges,” ResearchGate, 2025.
[14] “The application of artificial intelligence technology in cloud computing environment resources,” IEEE Xplore, 2021.
[15] V. Kumar, “Security for data access and control in cloud computing,” Shodhganga, 2025.
[16] “Enhancing security in cloud computing using artificial intelligence (AI),” 2024.
[17] “AI-enabled distributed cloud frameworks for big data analytics with privacy preservation,” 2025.