International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Improving Security and Privacy in Attribute-Based Data Sharing in Cloud Computing

Dr. Shrikant V. Sonekar[1] Professor Rohan B Kokate[2], Miss. Samiksha S Raut[3]
JD College of Engineering & Management, Khandala, Borgaon Phata, Kalmeshwar Road, Nagpur, Maharashtra, India[1]
Department Of Computer Applications, JD College of Engineering & Management, Khandala, Borgaon Phata, Kalmeshwar Road, Nagpur, Maharashtra, India[2,3]

Abstract- — Cloud computing has revolutionized the way data is stored, processed, and shared by providing scalable, flexible, and on-demand access to computational resources over the internet. It has enabled individuals, enterprises, and government organizations to efficiently manage large volumes of data without investing heavily in physical infrastructure. Despite these advantages, the rapid adoption of cloud platforms has introduced significant challenges related to data security, privacy preservation, and fine-grained access control. Since data is stored on third-party servers, users lose direct control over their sensitive information, increasing the risk of unauthorized access, insider threats, and data breaches. Traditional encryption techniques such as symmetric and asymmetric cryptography ensure data confidentiality but fail to provide flexible and scalable access control mechanisms in dynamic, multi-user cloud environments. These methods rely heavily on complex key management systems and are not suitable for scenarios where access permissions need to be defined based on user roles, attributes, or contextual conditions. To address these limitations, Attribute-Based Encryption (ABE) has emerged as a powerful cryptographic approach that enables secure and flexible data sharing by enforcing access policies based on user attributes rather than identities. In particular, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) allows data owners to define access structures directly within the encrypted data, ensuring that only users whose attributes satisfy the defined policies can decrypt and access the information. This paper presents the design and implementation of a secure and privacy-preserving data-sharing framework based on CP-ABE in cloud computing environments. The proposed system incorporates advanced security features such as fine-grained access control, secure key generation and distribution, user authentication, and protection against common attacks including collusion attacks and unauthorized data access. Additionally, privacy-preserving mechanisms are integrated to ensure that sensitive user attributes and data remain protected even from cloud service providers. The system architecture includes key components such as data owners, attribute authorities, cloud servers, and data users, working together to provide a secure and efficient data-sharing environment. Experimental evaluation demonstrates that the proposed framework significantly improves data security, reduces the risk of data breaches, and enhances access control efficiency compared to traditional encryption-based systems.

Keywords— Cloud Computing, Data Security, Privacy Preservation, Attribute-Based Encryption (ABE), CP-ABE, Access Control, Data Sharing, Cryptography

I. INTRODUCTION

Cloud computing has emerged as a fundamental pillar of modern digital infrastructure, enabling organizations and individuals to store, process, and share data efficiently over the internet. By offering scalable, flexible, and cost-effective solutions, cloud platforms eliminate the need for maintaining physical storage systems and IT infrastructure. Service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) have significantly transformed the way data and applications are accessed, deployed, and managed across various sectors including healthcare, education, finance, and government.

Despite its numerous advantages, cloud computing introduces critical challenges related to data security and privacy. Since sensitive data is outsourced to third-party cloud service providers, users lose direct control over their information. This raises concerns about unauthorized access, data breaches, insider attacks, and misuse of confidential information. Ensuring secure data sharing while maintaining user privacy has therefore become one of the most important issues in cloud computing environments.

One of the major challenges in cloud security is implementing efficient and scalable access control mechanisms. Traditional encryption techniques, such as symmetric and asymmetric cryptography, primarily rely on identity-based access control. While these methods ensure data confidentiality, they lack

flexibility in dynamic and distributed systems where access requirements frequently change. Additionally, managing and distributing encryption keys among a large number of users becomes complex, time-consuming, and prone to security vulnerabilities.

To overcome these limitations, Attribute-Based Encryption (ABE) has been introduced as an advanced cryptographic solution. ABE enables fine-grained access control by associating data access policies with user attributes such as role, department, designation, or clearance level. Among its variants, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is particularly effective, as it allows data owners to define access policies directly within the encrypted data. Only users whose attributes satisfy the specified policy can decrypt and access the information, thereby ensuring both security and controlled data sharing.

In addition to access control, preserving user privacy is equally important. In many cloud systems, user attributes and access patterns may reveal sensitive information. Therefore, integrating privacy-preserving mechanisms along with ABE is essential to protect user identity and prevent data leakage.

This paper proposes a secure and privacy-preserving framework for cloud data sharing based on CP-ABE. The system incorporates fine-grained access control, secure key management, and user authentication to ensure that only authorized users can access specific data. It also addresses common security threats such as collusion attacks, unauthorized data access, and data leakage. The proposed framework is designed to be scalable, efficient, and suitable for real-world applications including healthcare systems, financial services, and e-governance platforms.

The remainder of this paper is organized as follows: Section II presents a review of related work; Section III describes the system architecture; Section IV discusses implementation details; Section V presents results and analysis; and Section VI concludes the paper with future research directions.

II. LITERATURE REVIEW

This section reviews existing research and technologies related to cloud security, Attribute-Based Encryption (ABE), privacy-preserving mechanisms, and current cloud storage systems. It highlights the limitations of traditional approaches and establishes the need for a more secure and flexible data-sharing framework.

1. Cloud Security Challenges

Cloud computing environments are inherently distributed and rely on third-party infrastructure, which introduces multiple security and privacy challenges. One of the most critical issues is data breaches, where sensitive information is exposed due to vulnerabilities in cloud systems or cyberattacks. Since data is stored remotely, users have limited control over its protection, making it a prime target for attackers.

Another major concern is unauthorized access, where malicious users gain access to confidential data due to weak authentication mechanisms or improper access control policies. In addition, insider threats pose a serious risk, as employees or administrators of cloud service providers may misuse their privileges to access sensitive data.

Data loss is also a significant issue, which may occur due to accidental deletion, hardware failure, or malicious attacks such as ransomware. Furthermore, ensuring data integrity and availability in cloud environments remains a challenge due to network failures and system downtime.

Traditional security mechanisms, including firewalls and basic encryption, are not sufficient to address these challenges effectively because they do not provide dynamic and fine-grained access control required in modern cloud systems. This necessitates the adoption of advanced cryptographic techniques.

2. Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) has emerged as a powerful cryptographic approach for secure data sharing in distributed systems. Unlike traditional encryption methods that rely on user identities, ABE uses attributes (such as role, department, or designation) to determine access permissions.

There are two primary types of ABE:

Key-Policy Attribute-Based Encryption (KP-ABE)

In KP-ABE, the access policy is embedded in the user's private key, while the ciphertext is associated with a set of attributes. A user can decrypt the data only if the attributes of the ciphertext satisfy the policy defined in their key. However, this approach limits the control of data owners, as they cannot directly define access policies for their data.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

In CP-ABE, the access policy is embedded in the ciphertext, and the user's private key is associated with a set of attributes. This allows data owners to define flexible access policies such as:

(Role = Doctor AND Department = Cardiology)

Only users whose attributes satisfy this condition can decrypt the data. CP-ABE provides better flexibility, scalability, and control, making it more suitable for cloud-based applications.
Despite its advantages, ABE faces challenges such as high computational overhead, complex key management, and scalability issues in large systems.

3. Privacy-Preserving Techniques
In addition to access control, protecting user privacy is a critical requirement in cloud computing. Privacy-preserving techniques ensure that sensitive information is not exposed to unauthorized entities, including cloud service providers.
Some widely used privacy-preserving methods include:

- **Anonymization:** Removes or hides personally identifiable information (PII) from datasets to prevent user identification.
- **Homomorphic Encryption:** Allows computations to be performed directly on encrypted data without decrypting it, ensuring data confidentiality during processing.
- **Secure Multi-Party Computation (SMPC):** Enables multiple parties to jointly compute a function over their inputs while keeping those inputs private.
- **Data Masking and Tokenization:** Replaces sensitive data with masked or tokenized values to prevent exposure.

These techniques enhance privacy but often introduce computational complexity and performance overhead. Therefore, integrating them efficiently with encryption mechanisms like ABE is essential for practical deployment.

4. Existing Systems
Popular cloud storage platforms such as Google Drive, Dropbox, and OneDrive provide basic security features, including data encryption during transmission and storage. However, these systems primarily rely on centralized access control mechanisms and do not support fine-grained, attribute-based access policies.

In such systems, access is typically granted based on user identity (e.g., email ID), which limits flexibility. For example, it is difficult to enforce complex policies like:

“Only users with role = Manager AND experience > 5 years can access this file”

Research studies have proposed ABE-based cloud storage systems to overcome these limitations. These systems provide fine-grained access control and improved security. However, they still face several challenges:

- High computational cost during encryption and decryption
- Complex key management for large numbers of users
- Scalability issues in real-time applications
- Difficulty in updating access policies dynamically

These limitations highlight the need for an improved framework that combines ABE with efficient key management and privacy-preserving techniques to achieve secure, scalable, and flexible cloud data sharing.

III. SYSTEM ARCHITECTURE

The proposed system is designed to provide a secure and privacy-preserving framework for data sharing in cloud computing environments using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The architecture ensures that sensitive data is encrypted before being stored in the cloud and can only be accessed by authorized users whose attributes satisfy predefined access policies.

The system consists of four primary components: Data Owner, Cloud Server, Attribute Authority (AA), and Data User.
These components interact with each other to ensure secure data storage, controlled access, and efficient key management.

1. Data Owner
The Data Owner is the entity responsible for uploading data to the cloud. This can be an individual, organization, or system that generates sensitive information and wants to share it securely.

Before uploading data, the Data Owner performs the following operations:

- Defines access control policies based on attributes (e.g., role, department, designation)
- Encrypts the data using the CP-ABE algorithm
- Attaches the access policy to the encrypted data (ciphertext)
- Uploads the encrypted data to the cloud server

2. Cloud Server
The Cloud Server acts as a storage and service provider. It is responsible for storing encrypted data and handling user requests for data access.

It is important to note that the cloud server is considered semi-trusted, meaning:

- It correctly stores and delivers data
- But it should not be able to read or decrypt the data

Functions of Cloud Server:

International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

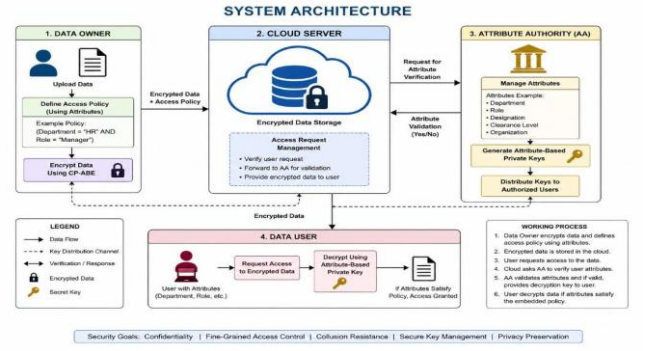


Fig. 1: Overall System Architecture Diagram

- Stores encrypted files securely
- Manages data access requests from users
- Provides data availability and scalability
- Maintains logs of access activities

Since all data is encrypted before storage, the cloud server cannot access the original data, ensuring data confidentiality.

3. Attribute Authority (AA)

The Attribute Authority (AA) is a trusted entity responsible for managing user attributes and generating cryptographic keys within the system. It plays a crucial role in ensuring secure and controlled access to encrypted data by verifying that only legitimate users receive valid decryption keys. The AA performs multiple functions, including verifying user identity and associated attributes, generating private keys based on these attributes, and securely distributing the keys to authorized users. Additionally, it is responsible for updating or revoking user attributes whenever necessary to maintain system security and adaptability. Typical attributes managed by the AA include role (such as Doctor, Manager, or Student), department (such as IT, HR, or Finance), and clearance level (such as High, Medium, or Low). By assigning attribute-based keys to users, the AA ensures that data decryption is only possible when a user's attributes satisfy the access policy defined by the data owner, thereby enforcing fine-grai

4. Data User

The Data User is the entity responsible for requesting access to encrypted data stored in the cloud environment. To gain access, the user must possess valid attribute-based private keys issued by the Attribute Authority (AA), which define their access privileges. The working process begins when the Data User sends a request to access specific data stored on the cloud server. Upon receiving the request, the cloud server provides the corresponding encrypted data to the user. The Data User then attempts to decrypt the data using their attribute-based private key. Decryption is successful only if the user's attributes satisfy the access policy embedded within the ciphertext by the Data Owner. This ensures that unauthorized users cannot access sensitive information. The key responsibilities of the Data User include requesting data access, utilizing attribute-based keys for decryption, and ensuring the secure handling and usage of decrypted data. This mechanism enforces fine-grained access control and enhances ove

```python
import os
import json
import base64
import hashlib
import datetime
import re
from typing import Dict, List, Set, Tuple, Optional
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.backends import default_backend

class BlockchainLogger:
    def __init__(self):
        self.chain = []
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = {
            'index': 0,
            'timestamp': str(datetime.datetime.now()),
            'transaction': "GENESIS_BLOCK",
            'previous_hash': "0",
            'hash': self.calculate_hash(0, "GENESIS_BLOCK", "0")
```

5. Overall Working Flow

The overall working flow of the proposed system ensures secure and privacy-preserving data sharing in a cloud computing environment using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The process begins with the Data Owner, who encrypts sensitive data before uploading it to the cloud. While encrypting, the data owner defines an access policy based on attributes such as role, department, or clearance policy, is then stored on the cloud server. When a Data User wants to access the data, they send a request to the cloud server. The cloud server, acting as a semi-trusted entity, processes the request and may interact with the Attribute Authority (AA) to verify the user's attributes.

The Attribute Authority is responsible for managing user identities and issuing attribute-based private keys. It verifies whether the user possesses valid attributes and provides the corresponding cryptographic keys. Once verified, the cloud server sends the encrypted data to the user. The Data User then attempts to decrypt the data using their private key. Decryption is successful only if the user's attributes satisfy the access policy defined by the Data Owner. If the policy conditions are not met, access is denied, ensuring data confidentiality and security.

This workflow guarantees that sensitive data remains protected throughout the process, as it is always stored in encrypted form on the cloud. Only authorized users with matching attributes can access the original data, enabling fine-grained access control, preventing unauthorized access, and ensuring privacy preservation in cloud-based data sharing systems.

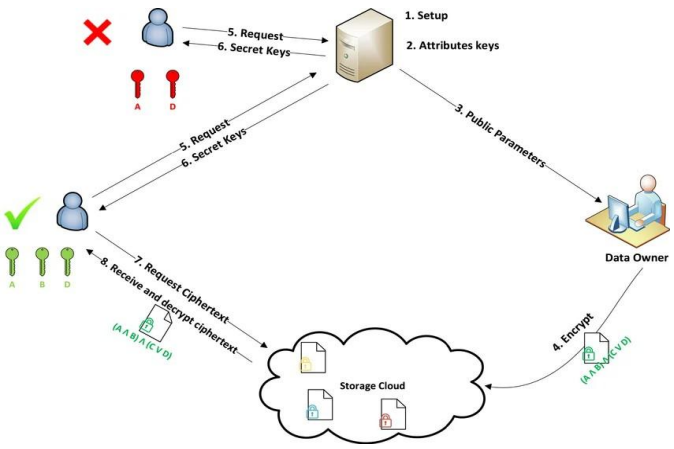


Fig. 2: Overall Working Flow of CP-ABE System diagram

IV. IMPLEMENTATION AND EXPERIMENTAL SETUP

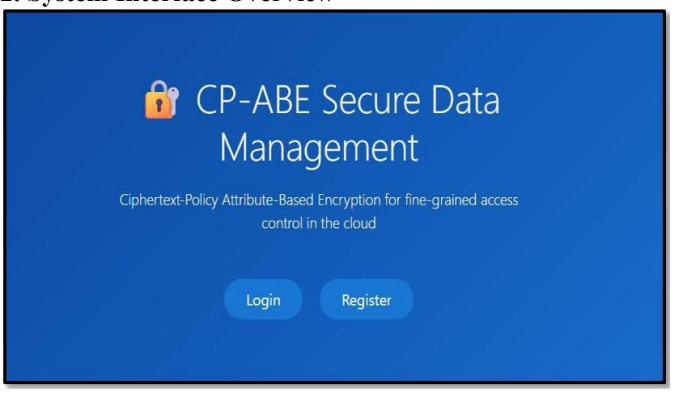
1. Technology Stack

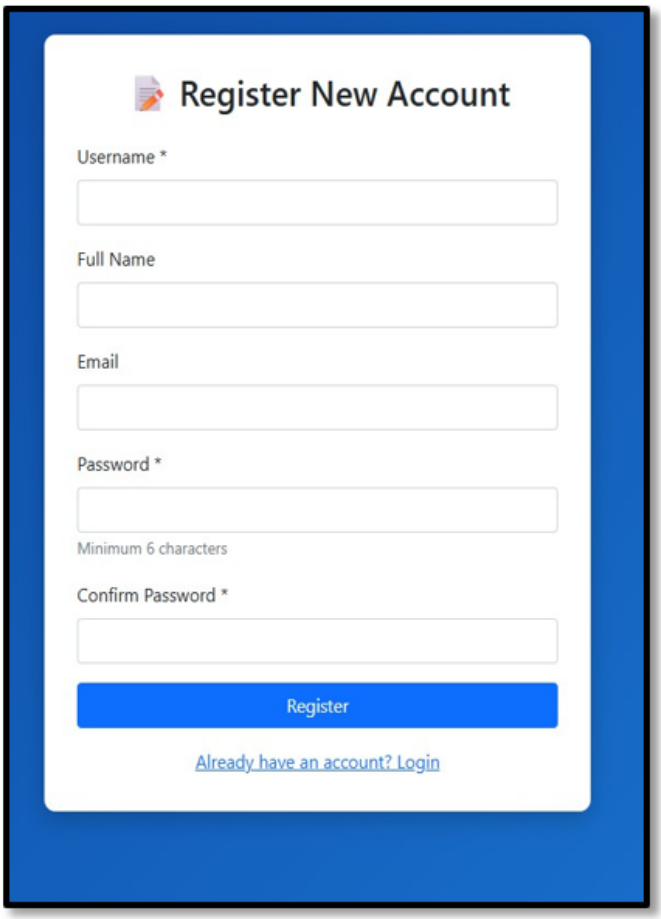
The proposed system is implemented using a well-structured technology stack that ensures both functionality and security. The frontend layer, built using HTML, CSS, and JavaScript, provides an interactive interface for users. The backend is developed using Python or Node.js, which handles application logic, encryption processes, and authentication mechanisms. The database layer utilizes MySQL or SQLite to store user data, attributes, and system records securely. For encryption, the CP-ABE algorithm is used to enforce fine-grained access control and protect sensitive data. This integrated approach ensures a secure, scalable, and efficient cloud data-sharing system.

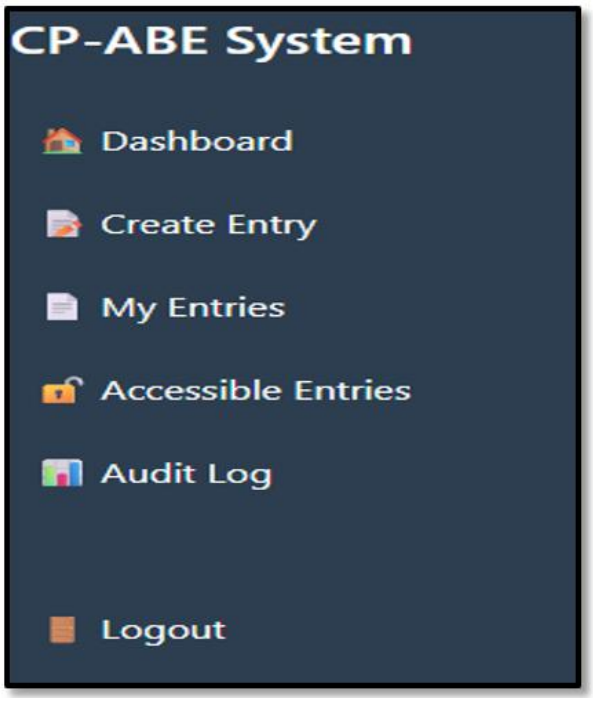
Table 1: Technology Stack Summary

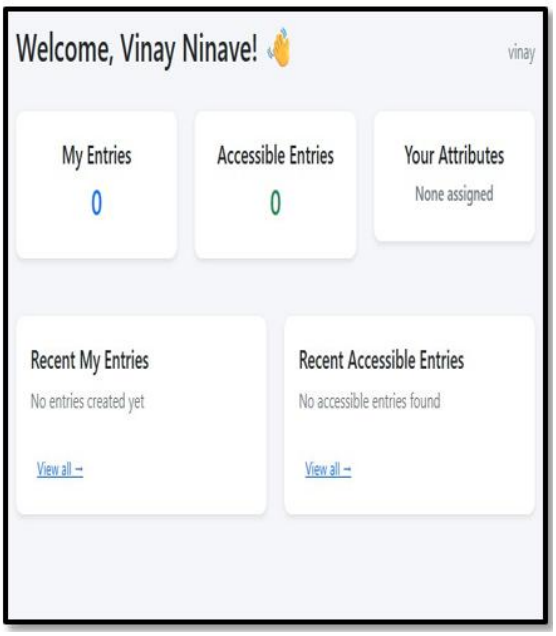
Layer	Technology	Purpose
Frontend	HTML, CSS, JavaScript	User Interface
Backend	Python / Node.js	Logic & Encryption
Database	MySQL / SQLite	Data Storage
Encryption	CP-ABE Algorithm	Security

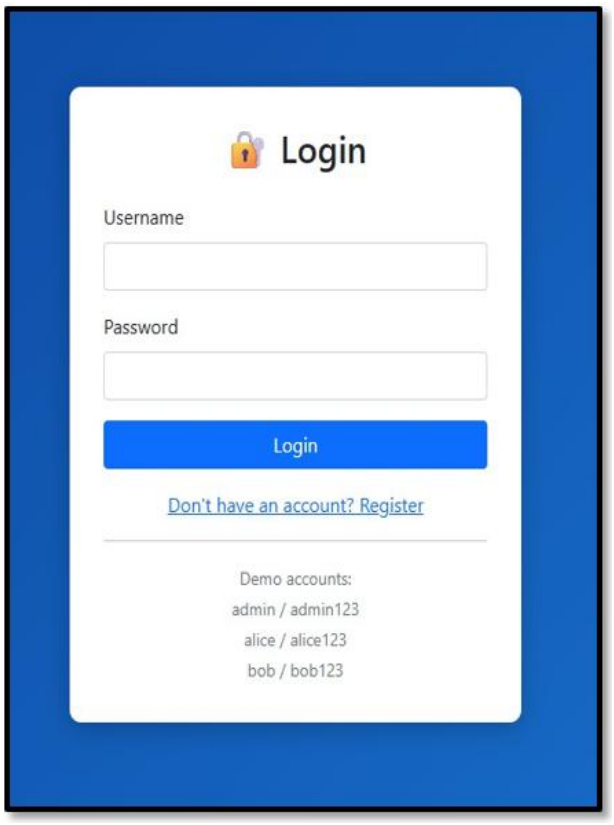
2. System Interface Overview











3. Algorithm (CP-ABE)

The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm is used in the proposed system to ensure secure and fine-grained access control over cloud-stored data. It consists of four main phases: Setup, Key Generation, Encryption, and Decryption.

Setup():

This phase is executed by the Attribute Authority (AA). It initializes the system by generating the public key and master key. The public key is made available to all users, while the master key is kept secret by the AA for generating user-specific private keys.

KeyGen():

In this phase, the Attribute Authority generates a private key for each user based on their attributes such as role, department, and clearance level. This key is securely distributed to the user and is used later for decryption.

Encrypt():

The Data Owner encrypts the data using the public key along with an access policy defined over a set of attributes. The policy determines which users are eligible to access the data.

Decrypt():

The Data User attempts to decrypt the ciphertext using their private key. Decryption is successful only if the user's attributes satisfy the access policy embedded in the encrypted data.

4. Security Features

The proposed system incorporates multiple security features to protect sensitive data in the cloud environment. It provides fine-grained access control by allowing access decisions based on user attributes rather than identities, ensuring flexibility and precision. Data confidentiality is maintained as all data is encrypted before being stored in the cloud, preventing unauthorized access even by the cloud provider. The system is resistant to collusion attacks, meaning that multiple users cannot combine their attributes or keys to gain unauthorized access to restricted data. Additionally, secure key distribution is ensured through the Attribute Authority, which manages the generation, distribution, and revocation of cryptographic keys in a controlled and secure manner

V. RESULTS AND DISCUSSION

1. Performance Analysis

The performance analysis clearly demonstrates that the proposed system outperforms traditional encryption techniques in multiple aspects. In terms of security level, traditional methods provide only medium protection, whereas the proposed CP-ABE-based system ensures a higher level of security by incorporating attribute-based access policies. Access control in traditional systems is limited and primarily identity-based, making it less flexible. In contrast, the proposed system offers fine-grained access control, allowing data owners to define detailed policies based on user attributes.

Data privacy is also significantly improved in the proposed system, as sensitive information remains encrypted and accessible only to authorized users, ensuring strong confidentiality. Additionally, scalability is a major advantage, as the system efficiently supports a growing number of users and attributes without significantly increasing complexity. Overall, the results indicate that the proposed approach provides a more secure, flexible, and scalable solution for cloud-based data sharing compared to conventional encryption methods.

Table 2: Performance Comparison Between Traditional Encryption and Proposed CP-ABE System

Metric	Traditional Encryption	Proposed System
Security Level	Medium	High
Access Control	Limited	Fine-grained
Data Privacy	Moderate	Strong
Scalability	Low	High

2. Observations

The experimental results and analysis highlight several key observations regarding the effectiveness of the proposed CP-ABE-based system. Firstly, there is a significant improvement in data protection, as sensitive information remains encrypted and accessible only to authorized users whose attributes satisfy the defined access policies. The system effectively reduces unauthorized access by enforcing strict attribute-based authentication and decryption mechanisms. Additionally, the use of Attribute Authority enables efficient key management by securely generating and distributing attribute-based keys to users. Another important observation is the enhancement in privacy preservation, as even the cloud service provider cannot access the plaintext data, ensuring complete confidentiality of user information.

3. Limitations

Despite its advantages, the proposed system has certain limitations. One of the primary challenges is the high computational overhead associated with encryption and decryption processes in CP-ABE, especially when dealing with complex access policies and large datasets. The implementation of the system is also relatively complex, requiring a deep understanding of cryptographic techniques and careful system design. Furthermore, key management becomes increasingly challenging as the number of users and attributes grows, particularly in dynamic environments where attributes need to be frequently updated or revoked. Addressing these limitations is essential for improving the efficiency and practicality of the system in real-world applications.

VI. CONCLUSION AND FUTURE SCOPE

1. Conclusion

In this paper, a secure and efficient framework for cloud-based data sharing has been proposed using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). With the rapid growth of cloud computing, ensuring data security, privacy, and controlled access has become a critical challenge. Traditional encryption techniques, which rely on identity-based access control, often fail to provide flexibility and scalability in dynamic cloud environments. To overcome these limitations, the proposed system adopts CP-ABE, which enables fine-grained access control based on user attributes rather than identities.

The system architecture integrates key components such as the Data Owner, Cloud Server, Attribute Authority, and Data User, each playing a vital role in ensuring secure data flow and access control. The Data Owner encrypts the data using defined access policies, while the Attribute Authority is responsible for

managing user attributes and securely generating and distributing cryptographic keys. The Cloud Server stores only encrypted data, ensuring that sensitive information remains protected even in the case of unauthorized access. The Data User can decrypt the data only if their attributes satisfy the specified access policy, thereby enforcing strict access control. The implementation of the proposed system using modern technologies such as HTML, CSS, JavaScript, Python/Node.js, and MySQL/SQLite demonstrates its practical applicability. The integration of CP-ABE ensures that the system provides enhanced data confidentiality, fine-grained access control, and resistance to common security threats such as unauthorized access and collusion attacks. Furthermore, the performance analysis shows that the proposed system outperforms traditional encryption methods in terms of security level, scalability, and privacy preservation.

Despite certain challenges such as computational overhead and complex key management, the system offers a robust and reliable solution for secure data sharing in cloud environments. Overall, the proposed approach successfully addresses major security concerns and provides a scalable framework suitable for real-world applications such as healthcare systems, financial institutions, and government organizations, where secure and controlled access to sensitive data is essential.

2. Future Scope

Although the proposed CP-ABE-based system provides a secure and efficient framework for cloud data sharing, there are several areas where further improvements and enhancements can be made. One important direction for future work is the optimization of computational efficiency. Since CP-ABE involves complex encryption and decryption operations, reducing computational overhead and improving processing speed will make the system more suitable for real-time and large-scale applications.

Another potential improvement is the integration of advanced key management techniques. As the number of users and attributes increases, managing and updating keys becomes more challenging. Future systems can incorporate automated key revocation and dynamic attribute management to handle changes in user roles more effectively. Additionally, implementing decentralized Attribute Authority using blockchain technology can enhance transparency, trust, and security in key distribution.

The system can also be extended by integrating privacy-enhancing technologies such as homomorphic encryption and secure multi-party computation, which allow data processing without revealing sensitive information. Furthermore, incorporating machine learning techniques can help in detecting suspicious activities and strengthening system security through intelligent threat detection.

Another area of future enhancement is improving user experience and system usability by developing more intuitive interfaces and reducing system complexity. The proposed framework can also be adapted for mobile and IoT environments, where secure data sharing is increasingly important. Finally, real-world deployment and testing in domains such as healthcare, finance, and e-governance can provide valuable insights and help in refining the system for practical applications.

In conclusion, with continuous advancements and improvements, the proposed system has strong potential to evolve into a highly secure, scalable, and efficient solution for next-generation cloud data sharing.

REFERENCES

1. A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” EUROCRYPT, 2005.
2. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” IEEE Symposium on Security and Privacy, 2007.
3. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control,” ACM CCS, 2006.
4. M. Armbrust et al., “A View of Cloud Computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
5. K. Yang and X. Jia, “Attribute-Based Access Control for Multi-Authority Systems,” IEEE TPDS, vol. 24, no. 2, pp. 233–242, 2013.
6. S. Yu, C. Wang, K. Ren, and W. Lou, “Secure and Fine-Grained Data Access Control in Cloud Computing,” IEEE INFOCOM, 2010.
7. R. Buyya, C. S. Yeo, and S. Venugopal, “Market-Oriented Cloud Computing,” IEEE HPCC, 2008.
8. D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM Journal on Computing, vol. 32, no. 3, 2003.
9. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” IEEE IWQoS, 2009.
10. H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” CloudCom, 2009.

11. X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups,” IEEE TPDS, 2013.
12. G. Ateniese et al., “Provable Data Possession at Untrusted Stores,” ACM CCS, 2007.
13. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability for Data Storage Security,” IEEE TIFS, 2011.
14. S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” IEEE TrustCom, 2011.
15. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABE Ciphertexts,” USENIX Security Symposium, 2011.
16. J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, “Secure Data Sharing in Cloud Storage Using ABE,” Future Generation Computer Systems, 2013.
17. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated Ciphertext-Policy ABE,” Information Security Applications, 2009.
18. Z. Wan, J. Liu, and R. Deng, “HASBE: Hierarchical Attribute-Based Encryption,” IEEE Transactions on Information Forensics and Security, 2012.
19. B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” Public Key Cryptography (PKC), 2011.
20. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Financial Cryptography and Data Security, 2010.