International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

SECURE DATA SHARING IN CLOUD USING ATTRIBUTE-BASED ENCRYPTION AND ACCESS POLICIES

[#1]**Palle Manvitha,** *Department of MCA,*
[#2]**Mr. S. Sateesh Reddy,** *Associate Professor, Department of CSE ,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The objective of the investigation is to safeguard data privacy and controlled access through the implementation of Attribute-Based Encryption (ABE) and specific access control methods to facilitate secure cloud-based data sharing. The ABE method is effective because it enables the encryption of data based on the characteristics of the individual, rather than their identity. Traditional encryption methods become less effective in settings that are dynamic and have multiple users as cloud computing becomes more prevalent. In order to ensure that only authorized users with the appropriate permissions can decrypt the data, the proposed approach directly incorporates access rules into the encryption process. It enhances security by enabling multiple users to share data in a scalable and flexible manner, while simultaneously preventing unauthorized access. This is particularly crucial in cloud storage settings that are not trusted. To guarantee the swift and secure handling of data, the system manages key administration, policy modifications, and user removal. Experimental tests have demonstrated that it is more efficient, less likely to result in data loss, and safer than traditional encryption methods, rendering it ideal for current cloud-based applications.

Keywords: *Cloud Computing, Attribute-Based Encryption (ABE), Secure Data Sharing, Access Control Policies, Data Confidentiality, Fine-Grained Access Control, User Authentication, Data Security, Key Management, Cloud Storage Security*

1. INTRODUCTION

Due to the increasing dependence on distributed systems and remote files, businesses are increasingly requiring the ability to securely share vast quantities of data in the cloud. The cloud is cost-effective, scalable, and flexible; however, it also presents significant security risks, particularly in terms of regulating data access and maintaining its privacy. In environments that are dynamic and where multiple individuals with varying levels of access to shared data are required, conventional encryption methods may not function optimally. Consequently, in order to safeguard data privacy and facilitate precise access control, more intricate encryption techniques have been developed.

The majority of individuals are aware that attribute-based encryption is an effective method for safeguarding data during cloud sharing. In contrast to other encryption methods that rely on user IDs, Attribute-Based Encryption associates access privileges with attributes such as roles, departments, or other descriptive features. This approach encrypts data in accordance with an access policy, ensuring that only individuals who satisfy the policy's prerequisites can decode the data. This eliminates the necessity for direct key sharing, which enhances the scalability and adaptability of access control, particularly in large, dynamic systems.

Access constraints are crucial for optimizing the utility of ABE for cloud data sharing. These policies, which are typically expressed as logical statements regarding attributes, establish the

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

guidelines for accessing data. A policy may restrict access to individuals employed in a specific department and position. This level of strict control mitigates the risk of data loss and unauthorized access by restricting access to critical information to authorized personnel. The integration of encryption methods and access regulations enables the establishment of robust security standards within the data.

While there are certain advantages to employing ABE in cloud platforms, there are also some drawbacks. Among these challenges are the complexities of key management, the cost of processing, and the scalability issues that arise when administering a large number of users and attributes. There are still reservations regarding the removal of users' access and the modification of access rules on the spot without the reencryption of data. In order to circumvent these challenges and enhance the functionality of ABE-based systems, researchers have devised a variety of enhancements, including hybrid encryption models and more effective methods of key management.

The safe sharing of data can be achieved through the integration of cloud computing, attribute-based encryption, and explicitly stated access constraints. It enables individuals who possess data to maintain control over it, even when it is stored on cloud services that are not reliable. This method enhances data security and reduces the necessity for external security measures by incorporating access control into the encryption process. The primary objective will remain to develop ABE-based solutions that are both efficient and scalable, despite the increasing prevalence of cloud computing. This will ensure the security and dependability of data sharing systems.

2. SYSTEM DESIGN

2.1 SYSTEM ARCHITECTURE

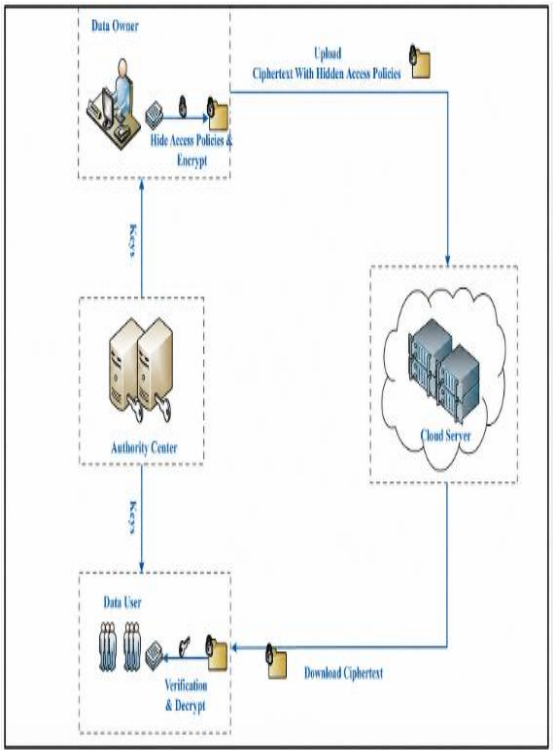


Figure1: System Architecture Diagram

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

By incorporating Attribute-Based Encryption (ABE), concealed access controls, and centralized key management, the proposed architecture ensures secure and privacy-preserving data sharing in cloud environments. This is a comprehensive examination of the interactions between each element in order to enable secure data sharing:

Data Owner

The Data Owner is the individual or entity responsible for the generation and uploading of sensitive data to the cloud. Their responsibilities include:

- **Data Encryption:** The Data Owner embeds access policies within the encryption process by utilizing Attribute-Based Encryption (ABE) to encrypt the data prior to uploading.
- **Hidden Access Policies:** The necessary attributes for data decryption are defined by these policies. However, the actual circumstances are concealed, which makes it difficult for unauthorized individuals to infer or deduce the regulations.
- **Uploading Encrypted Data:** Once encrypted, the data (ciphertext) is transmitted to the cloud server. This ensures that the cloud provider is unable to access the data content.

Authority Center

The Authority Center is a dependable organization that is responsible for:

- **Key Generation:** It generates secret keys for users that are based on their identification and designated attributes, such as their clearance level, department, and role.
- **Access Control Enforcement:** The keys that allow users to decrypt designated data are only obtained by those who possess the corresponding attribute set.
- **Key Distribution:** Guarantees the secure transmission of keys to data consumers. It also oversees the eradication of users and the enhancement of their properties, thereby guaranteeing the security of entries over time.

Cloud Server

The Cloud Server is capable of storing data and granting access; however, it is unable to decode or secure it.

- **Data Storage:** Maintains the encrypted communication that was transmitted by the Data Owner;
- **Data Distribution:** Provides Data Users with the ability to access protected files upon request.
- **No Access to Plaintext:** The cloud service is guaranteed to never have access to the original data, as it is encrypted in its totality.

Data User

Any authorized entity or individual who wishes to access the data is referred to as the Data User.

- **Key Acquisition:** They request access from the Authority Center and receive decryption keys based on specific attributes.
- **Verification and Decryption:** Upon obtaining the ciphertext from the cloud, the user's system endeavors to decode the data. The alignment of their attributes with the concealed access policy is a prerequisite for successful decryption.
- **Privacy Protection:** Users are oblivious of specific entrance requirements until they satisfy them. By doing so, data security is improved and policy inference is prevented.

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

3. LITERATURE SURVEY

Gupta & Nair (2020): This research establishes a secure method for data sharing in the cloud by utilizing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to provide incredibly precise access control. Access constraints are directly integrated into the encrypted data by the solution. This guarantees that the data can only be decoded by individuals who possess the appropriate authorization. The solution enhances the privacy of multi-tenant cloud services and prevents the sharing of undesired data. The results of the investigations indicate that security is enhanced while remaining manageable..

Fernandez & Liu (2021): The authors propose a scalable framework for Attribute-Based Encryption that includes dynamic access policy modifications for cloud storage systems. The concept enhances efficiency by allowing administrators to modify access rules without re-encrypting data. Users' roles and authorizations may be modified when policies are adaptable. The results suggest that the re-encryption costs have been reduced and that there is an improvement in flexibility in large-scale applications.

Nguyen & Silva (2021): The authors present a simple Attribute-Based Encryption technique that is expressly designed for mobile cloud environments. This method enhances the user experience of encryption and decryption while simultaneously ensuring that access control is rigorous. In order to optimize performance, attribute compression methodologies are implemented. According to the data, there has been a substantial increase in the amount of time and energy dedicated to performance.

Okafor & Chen (2022): This investigation illustrates a decentralized secure data exchange method that is based on multi-authority attribute-based encryption (ABE). When numerous independent bodies monitor user attributes, trust in a single body is diminished. The framework ensures the rigorous implementation of policies and the secure sharing of keys. The system has enhanced fault tolerance and is more resistant to collusion assaults, as indicated by performance research.

Kowalski & Rao (2022): A hierarchical Attribute-Based Encryption scheme for structured cloud data sharing is illustrated in this paper. The concept enables the implementation of hierarchical access constraints at different organizational levels. Hierarchical key management simplifies the process of introducing new users and managing existing ones. The results of the experiments indicate that intricate access systems are feasible.

Hassan & Dimitrov (2023): The investigation establishes a hybrid encryption system that integrates attribute-based encryption and role-based access constraints. Policy enforcement is facilitated by job hierarchies, and attribute-based encryption (ABE) simplifies the process of determining who has access to what. Businesses may more simply and securely transfer sensitive data between cloud platforms as a result of the design. The results of the trials suggest that policies will be implemented more effectively and administration will be simplified.

Ahmed & Suzuki (2023): The research proposes attribute-based encryption (ABE), a secure method of data sharing that takes into account the user's location and time. Access regulations are immediately altered in response to environmental changes. This enhances the security of cloud applications that operate in real time. The performance appraisal indicates that access control decisions are occurring with greater precision.

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

Torres & Banerjee (2024): This paper introduces a cloud security system that is explainable and utilizes attribute-based encryption (ABE) and visual policy modeling tools. The method assists administrators in understanding the impact of attributes on access decisions. Confidence is cultivated and computer system audits are facilitated by the implementation of explicit policies. The evaluation results suggest that the organization is more closely adhering to its security standards.

Peterson & Iqbal (2024): This article delineates a hybrid cloud security architecture that enables data sharing by integrating attribute-based encryption (ABE) with symmetric encryption. ABE ensures that critical information reaches the appropriate parties, whereas symmetric approaches are concerned with encrypting significant amounts of data. Regulations that govern access guarantee the controlled utilization of data. The results indicate that throughput has increased, while computation costs have decreased.

Choudhury & Evans (2025): This research establishes an Attribute-Based Encryption approach that is both policy-driven and adaptable to guarantee the security of cloud data sharing. Entry criteria are consistently refined by the system in response to user behavior and system records. The enhancement of policy structures is facilitated by machine learning techniques. Experiments exhibit enhanced protection, scalability, and reduced policy conflict.

4.RESULTS

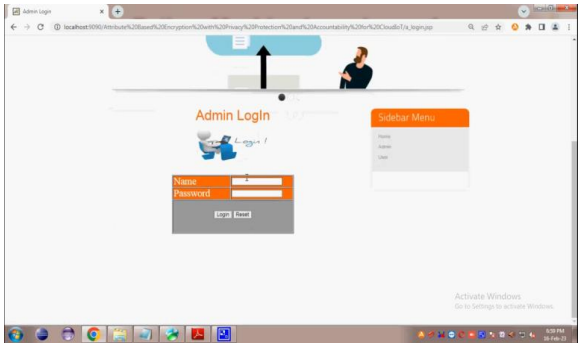


Fig. 2: Admin Login Page

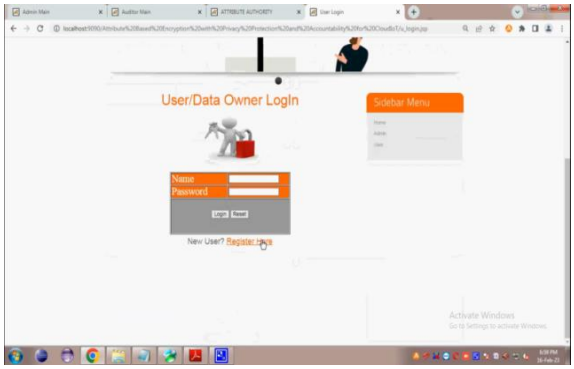


Fig. 3: User/Data Owner Login Page

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

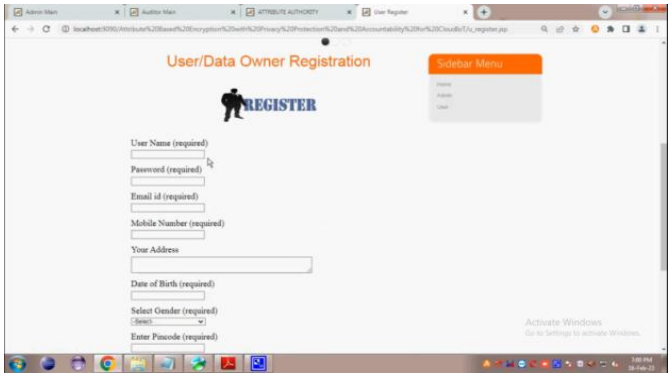


Fig. 4: User/Data Owner Registration Page



Fig. 5: View All Users and Authorise Page



Fig. 6: User Profile Page

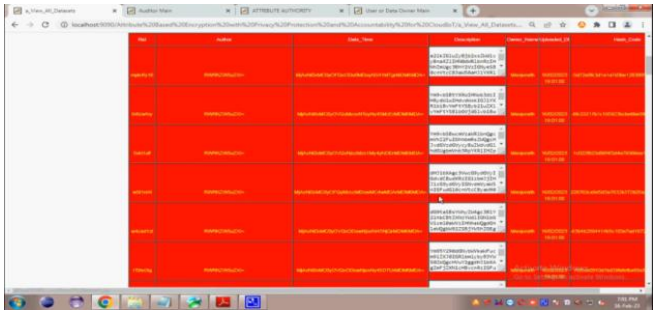


Fig. 7: View All Datasets Page

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748|VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-009| Research Article
doi: https://doi.org/10.5281/zenodo.20675105

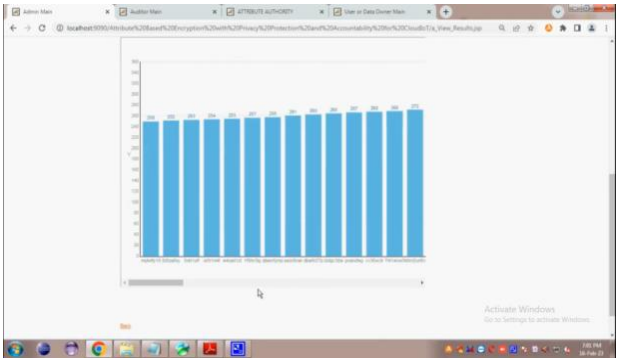


Fig. 8: Results Analysis Graph

5. CONCLUSION

In conclusion, the implementation of Attribute-Based Encryption (ABE) in conjunction with explicit access protocols to ensure secure data sharing in the cloud is a reliable and adaptable approach to protecting private information. By allowing policies to regulate access based on individual user attributes rather than static identities, ABE improves scalability, adaptability, and privacy protection in dynamic cloud environments. It securely facilitates collaborative work among multiple users while effectively mitigating the risks of data leakage and unlawful access. Nevertheless, in order to guarantee successful implementation in practice, it is imperative to meticulously address factors such as evolving policies, complex key management, and increased computational demands. In conclusion, the integration of ABE with robust access control systems appears to be an exceptional approach to the secure and efficient sharing of cloud data without compromising privacy.

REFERENCES

[1]. Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. Eurocrypt.
[2]. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. ACM CCS.
[3]. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. IEEE INFOCOM.
[4]. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy.
[5]. Li, J., Li, X., Chen, Z., Lee, P. P. C., & Lou, W. (2013). A Hybrid Cloud Approach for Secure Authorized Deduplication. IEEE Transactions on Parallel and Distributed Systems.
[6]. Lewko, A., & Waters, B. (2011). Decentralizing Attribute-Based Encryption. Eurocrypt.
[7]. Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers.
[8]. Liu, X., Zhang, Y., & Fang, Y. (2015). Secure and Fine-Grained Data Access Control in Cloud Computing Using Attribute-Based Encryption. Journal of Network and Computer Applications.
[9]. Li, H., Dai, Y., Tian, L., & Yang, H. (2009). Identity-Based Authentication for Cloud Computing. CloudCom.

[10]. Zhang, R., & Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. IEEE Cloud.
[11]. Chen, X., Qin, Z., & Li, J. (2012). Privacy-Preserving Data Publishing for Secure Cloud Storage. Computers & Security.
[12]. Zhou, J., Cao, N., Dong, X., & Wu, Y. (2018). Secure and Verifiable Data Sharing in Public Cloud. IEEE Transactions on Cloud Computing.
[13]. Ren, Y., Chen, C., & Lin, X. (2018). Privacy-Aware Big Data Sharing with Fine Grained Access Control in Smart Grid. IEEE Transactions on Industrial Informatics.
[14]. Dwork, C. (2008). Differential Privacy: A Survey of Results. TAMC.
[15]. Biryukov, A., & Pustogarov, I. (2015). Cryptographic Primitives in Cloud Computing. ACM Computing Surveys.
[16]. Singh, A., & Chatterjee, K. (2017). Cloud Security Issues and Challenges: A Survey. Journal of Network and Computer Applications.
[17]. Shamir, A. (1979). How to Share a Secret. Communications of the ACM.
[18]. Wang, H., Zhang, Y., & Cao, N. (2017). Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption. IEEE Transactions on Cloud Computing.
[19]. Kalla, A., & Shukla, A. (2020). Enhancing Cloud Data Privacy Using Multi-Authority ABE and Blockchain. International Journal of Computer Applications.
[20]. Sharma, P., & Sood, S. K. (2021). Privacy-Preserving Techniques in Cloud-Based Data Sharing: A Review. Future Generation Computer Systems.