RESEARCH ARTICLE OPEN ACCESS

A Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage

Lakshmipathy S V[1], Dr. Manjunath B N[2]

[1,2] Department of Computer Science and Engineering, RL Jalappa Institute of Technology, Doddaballapur, Karnataka

ABSTRACT

Cloud computing has become a widely adopted platform for storing and sharing data due to its scalability, flexibility, and cost-effectiveness. However, ensuring data confidentiality, fine-grained access control, and secure policy management remains a significant challenge, particularly in environments involving multiple organizations. Conventional access control mechanisms often rely on centralized authorities or require costly re-encryption whenever access policies change, resulting in increased computational overhead and reduced system efficiency. This paper proposes a **Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage**. The framework integrates **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)** with **Multiple Attribute Authorities (MAAs)** to provide decentralized and fine-grained access control while eliminating dependence on a single trusted authority. A dynamic policy updating mechanism enables secure modification of access policies without requiring re-encryption of previously stored data. In addition, the framework incorporates efficient key management and attribute verification to strengthen data confidentiality and improve access control. The implementation and functional validation demonstrate that the proposed framework provides secure data sharing, efficient policy management, improved scalability, and enhanced privacy preservation while reducing computational overhead. The proposed solution offers a practical and scalable approach for secure cloud storage in multi-owner and multi-organizational environments.

Keywords:--- Cloud Computing, Secure Cloud Storage, Multi-Authority Access Control, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Dynamic Policy Updating, Privacy Preservation, Fine-Grained Access Control, Data Security.

I. INTRODUCTION

Cloud computing has transformed the way organizations store, manage, and access digital information by providing scalable, on-demand, and cost-effective computing resources over the Internet. The rapid adoption of cloud services has enabled individuals, enterprises, healthcare institutions, educational organizations, and government agencies to outsource massive volumes of data to remote cloud servers while reducing infrastructure and maintenance costs [1]. Despite these advantages, outsourcing sensitive information to third-party cloud service providers introduces significant security and privacy concerns, particularly regarding data confidentiality, unauthorized access, and secure data sharing among multiple users [2].

To protect outsourced data from unauthorized disclosure, encryption techniques have become an essential component of cloud security. Conventional encryption methods effectively protect data confidentiality; however, they often fail to provide flexible and fine-grained access control in dynamic cloud environments where multiple users possess different access privileges. Managing encryption keys for a large number of users becomes increasingly complex, resulting in higher computational overhead and administrative burden [3].

Attribute-Based Encryption (ABE) has emerged as an efficient cryptographic technique for achieving fine-grained access control in cloud storage systems. In particular, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) enables data owners to define access policies directly within the encrypted data, allowing only users whose attributes satisfy the specified policy to decrypt the information [4]. This approach offers greater flexibility compared to traditional public-key encryption methods and has been widely adopted in secure cloud storage applications.

Although CP-ABE provides an effective mechanism for enforcing attribute-based access control, most existing solutions rely on a single attribute authority responsible for managing user attributes and cryptographic keys.

Such centralized architectures introduce several limitations, including single points of failure, scalability issues, administrative bottlenecks, and increased security risks. Furthermore, cloud environments involving multiple organizations often require independent authorities to manage different categories of user attributes, making centralized access control impractical [5].

Another significant challenge in cloud-based access control is the dynamic modification of access policies. In practical applications, user roles, organizational responsibilities, and security requirements frequently change over time. Traditional approaches require data owners to download previously encrypted files, modify the access policy, re-encrypt the data, and upload it again to the cloud. This process results in considerable communication overhead, increased computation time, and inefficient utilization of cloud resources, especially when dealing with large-scale datasets [6].

In addition, attribute revocation remains an open research issue in many existing cloud security frameworks. When users leave an organization or their privileges are revoked, the system must ensure that they can no longer access newly protected data while preventing unauthorized reuse of previously issued cryptographic credentials. Designing an efficient attribute revocation mechanism without significantly affecting system performance continues to be a challenging research problem [7].

To overcome these limitations, this paper proposes a **Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage**. The proposed framework employs multiple independent Attribute Authorities (AAs) to distribute attribute management responsibilities, thereby eliminating dependence on a centralized authority and improving scalability. A secure dynamic policy updating mechanism is introduced that enables cloud servers to update ciphertext access policies without exposing plaintext data or requiring data owners to perform repeated encryption operations. Furthermore, secure key management and attribute verification mechanisms are incorporated to strengthen privacy preservation while reducing computational and communication overhead.

The proposed framework offers several advantages over conventional cloud access control systems, including decentralized attribute management, efficient policy updates, secure multi-owner data sharing, reduced computation costs, and improved scalability. By integrating privacy-preserving encryption with dynamic policy management, the proposed solution enhances the security and efficiency of cloud storage environments while maintaining fine-grained access control for authorized users.

The major contributions of this research are summarized as follows:

- **A decentralized multi-authority access control framework** is proposed to eliminate the limitations associated with centralized attribute management.
- **A dynamic policy updating mechanism** is introduced to securely modify access policies without requiring data re-encryption by data owners.
- **An efficient key management and attribute verification approach** is incorporated to strengthen user authentication and authorization.
- **The proposed framework improves scalability, reduces communication overhead, and enhances privacy preservation** while supporting secure multi-owner cloud storage.
- **Performance evaluation demonstrates the effectiveness of the proposed framework** in terms of secure access control, policy management efficiency, and computational performance compared with existing cloud security approaches.

II. RELATED WORK

Cloud security has become one of the most active research areas due to the rapid adoption of cloud computing across various industries. Numerous studies have focused on developing secure access control mechanisms that preserve data confidentiality while allowing authorized users to access outsourced information efficiently. Among these mechanisms, Attribute-Based Encryption (ABE) has emerged as one of the most effective cryptographic approaches for enforcing fine-grained access control in cloud environments [8].

Sahai and Waters introduced the concept of Attribute-Based Encryption, establishing the foundation for attribute-driven encryption schemes that enable access decisions based on user attributes rather than individual identities [9]. This approach significantly improved flexibility in distributed systems by allowing data owners to define access privileges according to predefined attribute sets. However, the initial ABE model lacked scalability and practical policy management mechanisms for large cloud storage systems.

To address these limitations, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was proposed, enabling data owners to embed access policies directly into encrypted data while allowing users possessing matching attributes to decrypt the ciphertext [10]. CP-ABE provides greater control to data owners and has become one of the most widely adopted encryption techniques for secure cloud storage. Despite its effectiveness, traditional CP-ABE schemes generally rely on a centralized authority responsible for issuing user attributes and secret keys, making the system vulnerable to bottlenecks, single points of failure, and administrative overload.

Researchers subsequently introduced Multi-Authority Attribute-Based Encryption (MA-ABE) to distribute attribute management across multiple independent authorities [11]. In this model, different organizations or departments independently issue and manage user attributes, improving scalability and reducing the dependence on a single trusted authority. Multi-authority frameworks are particularly suitable for collaborative cloud environments where multiple organizations share resources while maintaining independent

administrative control. However, several existing MA-ABE schemes still experience increased communication overhead during user registration and key generation, limiting their efficiency in large-scale deployments.

Another important research direction focuses on dynamic access policy management. In practical cloud environments, user roles and organizational responsibilities frequently change, requiring modifications to existing access policies. Conventional approaches require data owners to retrieve encrypted files, modify the policy, re-encrypt the data, and upload it back to the cloud [12]. This process significantly increases communication cost, computation time, and storage overhead, especially for large datasets or frequently updated information. Several policy updating techniques have been proposed to reduce these overheads; however, many of them support only restricted policy modifications or depend heavily on trusted cloud servers.

Attribute revocation has also received considerable attention in secure cloud storage research. Revoking user privileges while maintaining data confidentiality remains a challenging problem because previously issued secret keys may continue to provide unauthorized access if not managed efficiently. Existing revocation mechanisms generally rely on periodic key updates, ciphertext re-encryption, or proxy re-encryption techniques [13]. Although these methods improve security, they often introduce additional computational costs and increase system complexity, making them less suitable for dynamic cloud environments with frequent user changes.

Recent studies have further explored privacy-preserving search techniques that allow users to retrieve encrypted cloud data without revealing sensitive information to cloud service providers [14]. Searchable encryption and ranked multi-keyword search algorithms improve data retrieval efficiency while preserving user privacy. Nevertheless, integrating searchable encryption with decentralized attribute-based access control and dynamic policy management remains an open research challenge due to the increased complexity of key distribution and policy enforcement.

Several researchers have also investigated hybrid security frameworks that combine Attribute-Based Encryption with symmetric encryption algorithms to reduce computational overhead while maintaining strong security guarantees [15]. In these approaches, large files are encrypted using efficient symmetric encryption algorithms, whereas ABE is employed only for encrypting secret keys and enforcing access control policies. Although hybrid encryption significantly improves encryption performance, secure policy updating and decentralized key management continue to require further enhancement.

Despite the considerable progress achieved in cloud access control research, several limitations remain unresolved. Many existing frameworks depend on centralized authorities, incur high communication overhead during policy updates, provide limited support for dynamic attribute management, or require repeated data re-encryption whenever access policies change. These challenges reduce scalability and negatively impact the performance of cloud storage systems deployed in collaborative environments involving multiple independent organizations.

To address these research gaps, this paper proposes a Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage. The proposed framework combines decentralized attribute management, efficient policy updating, secure key management, and fine-grained access control within a unified architecture. Unlike many existing approaches, the proposed solution minimizes computational overhead on data owners while maintaining confidentiality, scalability, and efficient access control in dynamic cloud environments.

Based on the existing literature, the following research gaps have been identified:

- Most existing CP-ABE frameworks rely on a centralized authority, creating scalability and reliability issues **[10]**.
- Dynamic access policy modification often requires expensive ciphertext downloading and re-encryption **[12]**.
- Efficient attribute revocation without affecting legitimate users remains a challenging problem **[13]**.
- Existing multi-authority schemes increase communication and computation overhead during attribute management **[11]**.
- Very few frameworks integrate decentralized access control, dynamic policy updating, and privacy-preserving cloud storage into a single unified solution **[14], [15]**.

These limitations motivate the development of the proposed framework, which aims to provide a scalable, efficient, and privacy-preserving access control mechanism for secure cloud storage environments.

III. PROBLEM STATEMENT

Cloud computing has emerged as a preferred platform for storing and sharing large volumes of sensitive information due to its scalability, flexibility, and cost-effectiveness. However, outsourcing confidential data to third-party cloud service providers introduces significant challenges in maintaining data security, user privacy, and fine-grained access control. Organizations require secure mechanisms that allow only authorized users to access encrypted information while ensuring that cloud servers cannot disclose sensitive data to unauthorized entities [16], [24].

Existing cloud access control mechanisms primarily rely on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enforce fine-grained authorization policies. Although CP-ABE

enables data owners to define attribute-based access policies, many existing implementations depend on a centralized Attribute Authority for user attribute management and key generation. This centralized architecture introduces several limitations, including scalability issues, administrative bottlenecks, and the risk of a single point of failure. As the number of users and attributes increases, centralized management significantly affects the efficiency and reliability of the access control system[24], [27].

Another major limitation of existing cloud storage systems is the inefficient handling of dynamic access policy modifications. In practical environments, user roles, organizational responsibilities, and security requirements frequently change. Conventional CP-ABE-based systems require data owners to download encrypted files, modify access policies, re-encrypt the data, and upload the updated ciphertext back to the cloud. This repetitive process increases computational complexity, communication overhead, and storage costs, making it unsuitable for large-scale cloud environments where policy updates occur frequently [31], [32].

Attribute revocation also remains a critical challenge in secure cloud storage. When users leave an organization or their access privileges are modified, the system must ensure that revoked users cannot continue accessing protected information. Many existing revocation mechanisms rely on complete key regeneration or ciphertext re-encryption, which introduces additional computational overhead and negatively impacts system performance, particularly in environments with a large number of users and frequent access changes [13].

Furthermore, collaborative cloud environments often involve multiple independent organizations that maintain separate administrative domains. Existing single-authority architectures cannot efficiently manage attributes issued by different organizations while preserving user privacy and reducing communication overhead. Consequently, organizations face challenges in implementing secure data sharing across multiple domains without compromising scalability and administrative flexibility [27], [29].

Although several Multi-Authority Attribute-Based Encryption (MA-ABE) schemes have been proposed to address centralized key management, many existing approaches still experience high communication costs during attribute verification, increased complexity in secret key generation, and limited support for efficient dynamic policy updating. These limitations reduce the practicality of existing solutions in real-world cloud storage environments [29], [32].

Therefore, there is a need for a secure, scalable, and privacy-preserving cloud access control framework that supports decentralized attribute management, efficient dynamic policy updating, and fine-grained authorization without requiring repeated ciphertext re-encryption by data owners. Such a framework should minimize computational and communication overhead while ensuring secure multi-owner data sharing and protecting sensitive information from unauthorized access.

To address these challenges, this research proposes a **Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage**. The proposed framework integrates multiple independent Attribute Authorities, secure key management, dynamic policy updating, and efficient attribute verification into a unified architecture. The objective is to improve scalability, strengthen privacy preservation, reduce computational overhead, and provide secure access control for dynamic cloud storage environments.

The primary objective of this research is to develop a secure and scalable cloud storage framework that enables decentralized access control through multiple independent Attribute Authorities, thereby eliminating the limitations associated with centralized attribute management. The proposed framework aims to provide fine-grained access control using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), ensuring that only authorized users whose attributes satisfy the defined access policies can access sensitive information. To improve the efficiency of cloud data management, the framework incorporates a dynamic policy updating mechanism that allows access policies to be modified securely without requiring repeated downloading and re-encryption of stored data by the data owner. Furthermore, the proposed solution employs the **Advanced Encryption Standard (AES)** algorithm for encrypting data files, providing efficient and robust protection of sensitive information, while **CP-ABE** is utilized to securely manage encryption keys and enforce attribute-based access control. In addition, the framework focuses on secure key management, efficient attribute verification, reduced computational complexity, minimized communication overhead during user authentication and policy updates, and enhanced privacy preservation. Overall, the research aims to improve the confidentiality, scalability, and efficiency of secure cloud storage systems while supporting collaborative data sharing among multiple independent organizations.

IV. METHODOLOGY

The proposed framework is designed to provide secure, scalable, and privacy-preserving cloud storage by integrating **Advanced Encryption Standard (AES)**, **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**, and a **Multi-Authority Access Control** mechanism. The framework enables data owners to securely store encrypted information in the cloud while ensuring that only authorized users possessing the required attributes can access the stored data. Unlike conventional cloud storage systems that depend on a centralized authority, the proposed model distributes attribute management responsibilities among multiple independent Attribute Authorities (AAs), thereby improving scalability, reliability, and administrative flexibility.

To enhance encryption efficiency, the framework adopts a hybrid cryptographic approach. Instead of encrypting large data files directly using CP-ABE, the original data is encrypted using the Advanced Encryption Standard (AES), which provides high-speed symmetric encryption with strong security guarantees. Subsequently, the AES secret key is encrypted using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), where the data owner specifies the access policy based on user attributes. As a result, only users whose attributes satisfy the predefined policy can recover the AES key and decrypt the original data. This hybrid approach significantly reduces computational overhead while maintaining fine-grained access control and strong data confidentiality.

The proposed methodology also incorporates a dynamic policy updating mechanism that enables modification of access policies without requiring data owners to download and re-encrypt previously stored files. Whenever organizational policies or user privileges change, the cloud server updates the encrypted access policy through secure policy transformation while preserving data confidentiality. This mechanism minimizes communication overhead and improves the overall efficiency of cloud storage management.

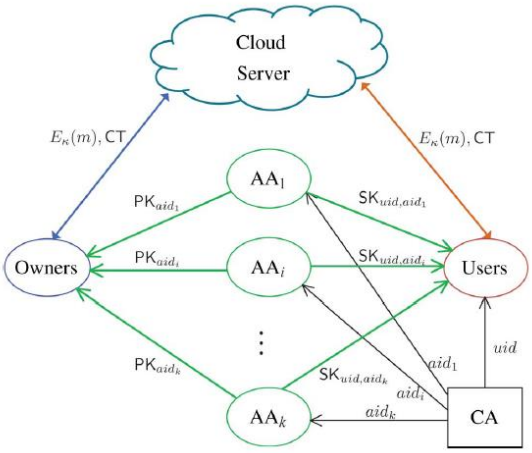

Figure 1: System Architecture

The overall architecture of the proposed framework is illustrated in *Figure 1*. It depicts the interaction among the Data Owner, Cloud Server, Multiple Attribute Authorities, and Data Users during secure data storage and retrieval.

Working Methodology

The complete workflow of the proposed framework is presented in *Figure 2*. The figure illustrates the sequence of operations performed during data encryption, secure key management, cloud storage, user authentication, and data decryption.

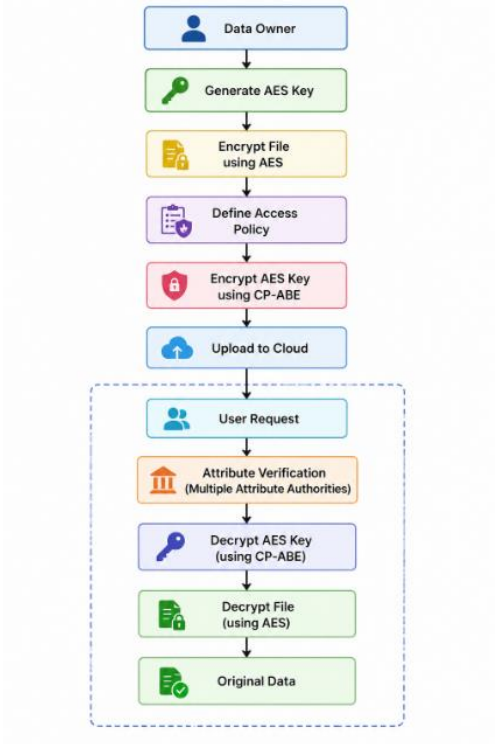

Figure 2: Working flow of the System

The operation of the proposed framework begins when a data owner intends to upload a confidential file to the cloud storage environment. Initially, the data owner generates a unique symmetric encryption key using the AES algorithm. The selected file is then encrypted using this AES key, producing ciphertext that protects the data from unauthorized disclosure. Since AES performs encryption much faster than public-key cryptographic techniques, it is highly suitable for securing large volumes of cloud data.

After completing data encryption, the data owner defines an access control policy specifying the attributes required for data access. These attributes may represent organizational roles, departments, designations, security levels, or any other access criteria relevant to the application.

The generated AES key is then encrypted using Ciphertext-Policy Attribute-Based Encryption under the specified access policy. Consequently, the cloud stores two protected components: the AES-encrypted data file and the CP-ABE-encrypted AES secret key.

The encrypted data is subsequently uploaded to the cloud server, where it remains inaccessible to the cloud service provider because both the data and the encryption key are securely protected. Since only encrypted information is stored, the cloud server cannot interpret or disclose the original content, thereby preserving user privacy.

To support decentralized administration, multiple independent Attribute Authorities are responsible for issuing and managing user attributes.

Each authority independently verifies user credentials within its administrative domain and generates the corresponding attribute keys. This decentralized architecture eliminates reliance on a single trusted authority and significantly improves scalability in collaborative cloud environments involving multiple organizations.

When an authorized user requests access to a stored file, the user first authenticates with the relevant Attribute Authorities and obtains attribute-based secret keys. The cloud server provides the encrypted AES key together with the encrypted data file. The user then attempts to decrypt the CP-ABE protected AES key using the received attribute keys. Successful decryption is possible only when the user's attributes satisfy the access policy specified by the data owner. If the access policy is satisfied, the recovered AES key is subsequently used to decrypt the encrypted file, allowing the authorized user to obtain the original plaintext information. Unauthorized users whose attributes do not satisfy the access policy cannot recover the AES key and therefore cannot decrypt the stored data.

The proposed framework also supports dynamic modification of access policies. Whenever access permissions change because of organizational restructuring, role reassignment, or user revocation, the access policy associated with the encrypted AES key can be updated securely without requiring re-encryption of the entire data file. Since only the encrypted access policy is modified while the AES-encrypted data remains unchanged, computational complexity and communication overhead are significantly reduced. This capability makes the framework particularly suitable for dynamic cloud environments where user privileges frequently change.

Overall, the proposed methodology combines efficient symmetric encryption, fine-grained attribute-based access control, decentralized attribute management, and dynamic policy updating into a unified cloud security framework. The integration of AES with Multi-Authority CP-ABE improves encryption efficiency, enhances privacy preservation, reduces administrative complexity, and provides scalable access control for secure cloud storage systems.

The proposed methodology offers several advantages over conventional cloud access control systems by integrating **AES**, **CP-ABE**, and **Multi-Authority Access Control** into a unified framework. The use of **AES** ensures efficient encryption and decryption of large data files with low computational overhead, while **CP-ABE** provides fine-grained access control based on user attributes. The adoption of multiple independent Attribute Authorities improves scalability and eliminates the limitations of centralized key management. Furthermore, the framework supports dynamic policy updating without requiring repeated data re-encryption, thereby reducing communication overhead and processing time. By storing only encrypted data and encrypted secret keys in the cloud, the proposed solution enhances data confidentiality, preserves user privacy, and provides a secure and scalable environment for cloud-based data sharing.

V. SYSTEM IMPLEMENTAION AND FUNCTIONAL VALIDATION

The proposed framework was implemented to validate the secure cloud storage model based on the integration of the **Advanced Encryption Standard (AES)**, **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)**, and **Multiple Attribute Authorities (MAAs)**. The implementation focuses on achieving secure file storage, fine-grained access control, decentralized attribute management, and dynamic policy updating while preserving data confidentiality and user privacy. The functional validation confirms that the proposed framework performs the intended operations efficiently and securely in a cloud environment.

Secure Data Encryption and Storage

The implementation begins with the data owner selecting a file for cloud storage. A unique AES secret key is generated to encrypt the selected file, ensuring efficient protection of large data files. The AES secret key is subsequently encrypted using CP-ABE based on the access policy defined by the data owner. Both the encrypted file and the encrypted AES key are securely stored on the cloud server. This hybrid encryption approach combines the computational efficiency of AES with the fine-grained access control provided by CP-ABE.

User Authentication and Access Control

When a user requests access to a stored file, the system authenticates the user and verifies the assigned attributes through the Multiple Attribute Authorities. Secret keys associated with the user's attributes are generated only after successful verification. The encrypted AES key is decrypted only if the user's attributes satisfy the access policy specified by the data owner. Once the AES key is recovered, it is used to decrypt the encrypted file and retrieve the original information. Users who do not satisfy the required access policy are denied access, thereby ensuring secure and controlled data sharing.

Dynamic Policy Updating

The implemented framework supports dynamic modification of access policies without requiring the data owner to re-encrypt previously stored files. Whenever changes occur in user roles or organizational permissions, the access policy associated with the encrypted AES key is securely updated while leaving the encrypted data unchanged. This mechanism reduces computational complexity, minimizes communication overhead, and simplifies policy management in dynamic cloud environments.

Functional Validation

The implemented framework was functionally validated by executing the major operational modules of the proposed system. The validation confirmed that data files are successfully encrypted using AES before cloud storage, while CP-ABE effectively protects the AES secret key according to the specified access policy. The authentication mechanism accurately verifies user attributes through multiple Attribute Authorities, ensuring that only authorized users can retrieve and decrypt stored information. Furthermore, the dynamic policy updating mechanism successfully modifies access permissions without affecting the encrypted data, demonstrating the effectiveness of the proposed approach in supporting secure and flexible cloud storage.

The implementation and functional validation demonstrate that the proposed framework successfully integrates AES encryption, CP-ABE-based access control, and decentralized attribute management into a unified cloud security solution. The use of AES ensures efficient encryption and decryption of data files, while CP-ABE provides secure and fine-grained access control by protecting the encryption key based on user attributes. The adoption of Multiple Attribute Authorities improves scalability and eliminates the limitations associated with centralized key management. Additionally, the dynamic policy updating mechanism enables secure modification of access permissions without repeated data re-encryption, thereby improving the efficiency and practicality of the proposed framework. Overall, the implementation validates the feasibility of the proposed approach for secure, scalable, and privacy-preserving cloud storage environments.

VI. CONCLUSION AND FUTURE WORK

This paper presented a **Privacy-Preserving Multi-Authority Attribute-Based Access Control Framework with Dynamic Policy Updating for Secure Cloud Storage** to address the challenges associated with secure data sharing in cloud environments. The proposed framework integrates the **Advanced Encryption Standard (AES)** for efficient data encryption with **Ciphertext-Policy Attribute-Based Encryption (CP-ABE)** to provide fine-grained attribute-based access control. The adoption of Multiple Attribute Authorities eliminates the limitations of centralized attribute management, thereby improving scalability, reliability, and administrative flexibility. Furthermore, the dynamic policy updating mechanism enables secure modification of access policies without requiring repeated re-encryption of stored data, reducing computational and communication overhead. The implementation and functional validation confirm that the proposed framework successfully ensures secure data storage, controlled data access, and efficient policy management while preserving user privacy and data confidentiality. Overall, the proposed solution provides a practical, scalable, and secure approach for cloud storage environments involving multiple organizations and collaborative data sharing.

Although the proposed framework effectively addresses secure cloud storage and fine-grained access control, several opportunities exist for further enhancement. Future work may focus on integrating **blockchain technology** to provide decentralized audit trails and improve the transparency of access control operations. The framework can also be extended by incorporating **Artificial Intelligence (AI)** and **Machine Learning (ML)** techniques to detect abnormal user behavior and support intelligent access control decisions. In addition, the implementation of more efficient attribute revocation mechanisms and lightweight cryptographic techniques can further reduce computational overhead for resource-constrained devices. The proposed framework may also be deployed in real-world cloud environments involving healthcare, financial institutions, and Internet of Things (IoT) applications to evaluate its scalability and performance under large-scale workloads. These enhancements would further strengthen the security, efficiency, and adaptability of the proposed cloud storage framework.

REFERENCES

[1] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA, Sept. 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2007, pp. 321–334.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, USA, 2006, pp. 89–98.

[5] M. Chase, "Multi-Authority Attribute-Based Encryption," in *Theory of Cryptography Conference (TCC)*, Springer, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in *Proc. ACM CCS*, Chicago, IL, USA, 2009, pp. 121–130.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," in *Public Key Cryptography (PKC)*, Springer, 2011, pp. 53–70.

[9] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2005*, Springer, 2005, pp. 457–473.

[10] National Institute of Standards and Technology (NIST), *Advanced Encryption Standard (AES)*, FIPS PUB 197, Nov. 2001.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[12] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717–1726, Sept. 2013.

[13] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, Jun. 2014.

[14] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, Jan.–Feb. 2012.

[15] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[16] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," in *Advances in Cryptology – EUROCRYPT 2004*, Springer, pp. 506–522.

[17] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, Feb. 1996.

[18] S. Yu, K. Ren, W. Lou, and J. Li, "Defending Against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1139–1152, Sept. 2011.

[19] B. Waters, "Functional Encryption: Past, Present, and Future," *IACR Cryptology ePrint Archive*, 2013.

[20] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," *USENIX Security Symposium*, 2011, pp. 34–34.

[21] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, May 2011.

[22] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[23] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[24] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[25] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," *CloudCom*, IEEE, 2009.

[26] X. Liang, R. Lu, X. Lin, and X. Shen, "Ciphertext Policy Attribute-Based Encryption with Efficient Revocation," *Technical Report*, University of Waterloo, 2010.

[27] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2011*, Springer, pp. 568–588.

[28] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy Updating in Attribute-Based Encryption," *IEEE Access*, vol. 8, pp. 165432–165444, 2020.

[29] H. Wang, Z. Zheng, S. Xie, H. Dai, and X. Chen, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[30] S. Kumar, R. Kumar, and A. K. Das, "Blockchain-Based Secure Data Sharing in Cloud Computing: A Survey," *Journal of Network and Computer Applications*, vol. 186, 2021.

[31] A. K. Das, S. Zeadally, N. Kumar, and J. J. P. C. Rodrigues, "Secure and Efficient Data Sharing in Cloud-Assisted Internet of Things Using Attribute-Based Encryption: A Survey," *IEEE Access*, vol. 9, pp. 104591–104620, 2021.

[32] Y. Zhang, X. Chen, J. Li, H. Li, and W. Susilo, "Recent Advances in Attribute-Based Encryption for Secure Cloud Storage: A Survey," *IEEE Access*, vol. 10, pp. 40685–40712, 2022.

Authors Profile

Mr. Lakshmipathy S. V. completed his Diploma in Computer Science and Engineering from Government Polytechnic**,** Chintamani, Karnataka, India**,** during the academic year 2017–2018. He received his Bachelor of Engineering (B.E.) degree **in** Computer Science and Engineering from M. S. Ramaiah Institute of Technology (MSRIT), Bengaluru, in 2021. Following his graduation, he worked as an Assistant Professor in the Department of Computer Science and Applications at Dolphin's Degree College, Sidlaghatta, Karnataka, until the academic year 2024–2025. He is currently pursuing his Master of Technology (M.Tech.) in Computer Science and Engineering at R. L. Jalappa Institute of Technology (RLJIT), Doddaballapur, Karnataka, India. His academic interests include Cloud Computing, Cyber Security, Artificial Intelligence, Software Engineering, Data Structures, and Emerging Computing Technologies.

Dr. Manjunatha B. N. received the **B.E. degree** in Information Science and Engineering from **R. L. Jalappa Institute of Technology (RLJIT), Doddaballapur**, affiliated with **Visvesvaraya Technological University (VTU), Belagavi**, in **2009**. He obtained the **M.Tech. degree** in Computer Science and Engineering from **S.J.C. Institute of Technology, Chikkaballapur**, affiliated with VTU, in **2014**, and was awarded the **Ph.D. degree** in Computer Science and Engineering from the **R&D Centre, Malnad College of Engineering, Hassan**, VTU, Belagavi, in **2022**. He is currently working as an **Associate Professor and Head** of the **Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning)** at **R. L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India**. He has over **16 years of teaching, research, and academic administration experience**. His research interests include **Artificial Intelligence, Machine Learning, Context Computing, Internet of Things (IoT), Cloud Computing, Wireless Sensor Networks, and Data Science**. He has published numerous research papers in reputed national and international journals and conferences, authored technical books, holds several patents, and has received recognition for his contributions to teaching, research, and academic quality initiatives.