Procedia of Engineering and Life Science Vol. 8 No. 2 (2025)
Proceedings of the 8th Seminar Nasional Sains 2025
Universitas Muhammadiyah Sidoarjo

The Use of Attribute-Based Encryption for Secure Data Access

Penggunaan Enkripsi Berbasis Atribut untuk Akses Data yang Aman

Malath Sabri Kareem
{malath-sabri@mtu.edu.iq }
Middle Technical University, Iraq

Abstract. *General Background: Secure data sharing in cloud computing and Internet of Things environments requires advanced cryptographic mechanisms to ensure privacy and controlled access. Specific Background: Attribute-based encryption provides fine-grained access control, while blockchain technology introduces decentralized trust and data integrity. Knowledge Gap: Existing approaches often lack an integrated framework that combines encryption flexibility with decentralized security for scalable data sharing systems. Aims: This study aims to develop a secure data sharing framework by integrating attribute-based encryption with blockchain technology. Results: The findings indicate that the proposed approach enables fine-grained access control, strengthens data confidentiality, and supports secure and verifiable transactions in distributed environments. The framework also demonstrates improved reliability in managing encrypted data across multiple systems. Novelty: This study presents a combined architecture that integrates attribute-based encryption with blockchain to address limitations in traditional centralized security models. Implications: The results suggest that the proposed framework can support secure data sharing in cloud and IoT applications, offering a scalable solution for modern distributed systems.*

Keywords: *Attribute Based Encryption, Blockchain Security, Data Sharing, Cloud Computing, Access Control*

Abstrak. *Latar Belakang Umum: Berbagi data yang aman dalam lingkungan komputasi awan dan Internet of Things memerlukan mekanisme kriptografi canggih untuk menjamin privasi dan akses yang terkendali. Latar Belakang Khusus: Enkripsi berbasis atribut menyediakan kontrol akses yang terperinci, sementara teknologi blockchain menghadirkan kepercayaan terdesentralisasi dan integritas data. Kesenjangan Pengetahuan: Pendekatan yang ada saat ini sering kali tidak memiliki kerangka kerja terintegrasi yang menggabungkan fleksibilitas enkripsi dengan keamanan terdesentralisasi untuk sistem berbagi data yang dapat diskalakan. Tujuan: Penelitian ini bertujuan untuk mengembangkan kerangka kerja berbagi data yang aman dengan mengintegrasikan enkripsi berbasis atribut dengan teknologi blockchain. Hasil: Temuan menunjukkan bahwa pendekatan yang diusulkan memungkinkan kontrol akses yang terperinci, memperkuat kerahasiaan data, dan mendukung transaksi yang aman dan dapat diverifikasi dalam lingkungan terdistribusi. Kerangka kerja ini juga menunjukkan peningkatan keandalan dalam mengelola data terenkripsi di berbagai sistem. Kebaruan: Penelitian ini menyajikan arsitektur gabungan yang mengintegrasikan enkripsi berbasis atribut dengan blockchain untuk mengatasi keterbatasan dalam model keamanan terpusat tradisional. Implikasi: Hasil penelitian menunjukkan bahwa kerangka kerja yang diusulkan dapat mendukung berbagi data yang aman dalam aplikasi cloud dan IoT, menawarkan solusi yang dapat diskalakan untuk sistem terdistribusi modern.*

Kata Kunci: *Enkripsi Berbasis Atribut, Keamanan Blockchain, Berbagi Data, Komputasi Awan, Kontrol Akses*

I. INTRODUCTION

The modern-day digital environment is marked by an ever-increasing volume of sensitive data that is stored, processed, and shared within distributed environments such as cloud computing, Internet of Things, and collaborative data sharing. Despite the obvious advantages offered by these technologies, they are marked by critical security challenges that are linked to data confidentiality. In this regard, traditional models of access control are usually centered on authorities or servers that are assumed to be implementing access control. However, this approach is not effective when dealing with external environments. Therefore, there is a critical research-related need to attain secure access control over sensitive data within modern-day information systems. In this connection, access control models that are based on cryptography have been extensively studied as potential solutions to this problem. Among the methods, the Attribute-Based Encryption (ABE) has become one of the promising cryptographic methods through which access controls can be fined in that the access privileges are assigned to user attributes instead of identities. ABE enables the data owners to establish advanced access policies that identify the users capable of decrypting particular data. A number of studies have shown that ABE can be used to secure distributed systems and cloud-based settings. As an illustration, Ganesan [1] came up with a dynamic secure data management framework powered by ABE on mobile financial cloud setting to facilitate flexibility in policy-driven access to data. Correspondingly, Rasori et al. [2] and Jemihin et al. [3] offered detailed reviews of ABE schemes and emphasized their relevance to the IoT systems and big data environment. Other review articles like Khoachev [4] also reaffirmed the relevance of ABE as a

core technology in the distribution of secure data in the contemporary distributed infrastructures. More recent studies have investigated the use of ABE in a number of fields, such as healthcare, IoT, cloud computing, and industrial networks. Walid et al. [5] examined the efficiency of various ABE schemes in safeguarding healthcare data, whereas Jiang et al. [6] and Xiang and Zhao [7] suggested blockchain-based ABE schemes to protect electronic health records and e-health systems. Thus, the present study explores the usage of the Attribute-Based Encryption as a viable tool in the context of attaining fine-grained data access control in a distributed environment. The paper takes a specific interest in the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model and evaluates how this tool can be used to secure data management in cloud-based infrastructures. Moreover, the study offers a useful framework that illustrates how ABE can be implemented to enforce secure access control to encrypted information, and it also overcomes the main obstacles including scalability, attribute management, and computational overhead. This research is important as it discusses the increasing demand of data access control mechanisms in distributed computing systems including cloud computing and IoT systems that require secure and flexible mechanisms. Under such settings, centralized access control systems will not provide adequate security since sensitive information can be subject to security risks in case the storage infrastructure is breached. Attribute-Based Encryption (ABE) is an alternative method, which allows access control policies to be integrated with the encrypted data, thus enabling only authorized users with the required attributes to access the data. The study aims at contributing towards bridging the gap between the theoretical aspects of cryptographic systems and the practical considerations involved in the implementation of Attribute-Based Encryption-based access control systems by providing insights into the practical aspects of ABE-based access control systems. The study has implications for the design of ABE-based access control systems for data sharing in the contemporary business environment. The aim of this study is to evaluate the efficacy of Attribute-Based Encryption as an access control system that allows for safe access of data in a distributed data sharing environment. The study evaluates the theoretical aspects of Attribute-Based Encryption, including its variants, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), as well as the efficacy of CP-ABE as a viable access control system. The study also aims at evaluating a framework for a real-world system that allows for the integration of attribute-based systems with encryption systems for authenticating data stored in cloud computing environments. The research will also examine the practical issues related to ABE implementation such as attribute management, policy update, user revocation and computational overhead. Finally, the study will offer implementation design considerations of efficient and scalable attribute-based encryption frameworks to offer secure data sharing of the present day distributed systems.

1- Theoretical Background and Core Concepts

A. Traditional Access Control and Its Limitations

Conventional access control models in information systems are based on centralized models of authorization whereby a central trusted server authenticates the user to gain access to the resource with protection. These mechanisms usually involve identity-based access control, access control list, role-based access control model techniques that controls the permissions based on a set of predefined roles or identities. Although these methods have proven useful in regulated enterprise settings, their constraints are become apparent when implemented in a contemporary distributed infrastructure, e.g. cloud computing systems, Internet of Things (IoT) systems, collaborative data sharing systems.

The sensitive data in the distributed environment is frequently stored in a third-party cloud server or shared among multiple organizations that might not be absolutely confident in each other. According to various research works on secure cloud and IoT systems, the use of centralized access control systems only leaves data vulnerable to any security threat in case the storage system is attacked or acts maliciously in such a case [1], [2]. Even in this case, when access policies have been correctly defined, a compromised server can still gain an unauthorized access to the stored data. Moreover, the emergence of dynamic user privileges, scale-related challenges, and policy management is caused by the fast-growing distributed systems and large-scale IoT infrastructures [3], [9].
Such issues have compelled scholars to consider other security mechanisms that can enforce the access control without dependence on the storage infrastructure. Specifically, contemporary security conceptions have tried to incorporate access control into the encryption process itself so that even in case the data has been stored on untrusted platforms, it is not compromised. Some articles have focused on highlighting the fact that access control systems based on encryptions offer greater security assurances in distributed systems since only under specified conditions can the data be decrypted [6], [11]. Consequently, cryptographic solutions like the Attribute-Based Encryption have become a potentially useful model of secure data sharing in cloud and distributed systems.

B. Definition of Attribute-Based Encryption

Attribute-Based Encryption (ABE) is a high-end paradigm of the public-key encryption aimed at providing fine-grained access control in decentralized system. Unlike the conventional encryption systems where access is earned on

the basis of the identity of the user, ABE relates the ability to decrypt to a set of attributes assigned to an individual user. Such attributes can be office features like office position, department, level of security clearance, or system privileges. The information will not be decipherable unless the attributes used by a user match the established access policy within the encryption scheme. Recently, it has been emphasized that ABE is very useful in allowing safe data exchange in distributed contexts like cloud computing platforms, IoT networks, and healthcare systems. Indicatively, Ganesan [1] introduced a scheme of ABE-based data management in mobile financial clouds, which shows that ABE can enforce data access according to a flexible policy. In a similar fashion, Rasori et al. [2] and Jemihin et al. [3] noted the appropriateness of ABE mechanisms to IoT systems and big data environments to secure with more flexibility than traditional access control models can offer. Functionally, an ABE system will usually be composed of a number of basic algorithms that handle encryption and access control policies. These algorithms contain a setup algorithm that produces the system public parameters and master secret key, key generation algorithm producing the private keys that are related to the user attributes, encryption algorithm that will encrypt the data based on a given access policy, and a decryption algorithm to allow recovery of the data as long as the user attributes meet the policy requirements. This cryptography design lets data owners to establish dynamic access control policies that are not disregarded even when data are stored in partly trusted infrastructures like cloud systems or distributed storage systems [10], [12].

C. The Two Main Models: KP-ABE and CP-ABE

Attribute-Based Encryption may be applied using various architectural models, which decide on the form in which the access policies and user attributes should be incorporated into the encryption system. The literature on the subject has recognized two major versions of ABE, including Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). It is necessary to realize the distinctions between such models in the context of a design of secure data access systems in distributed environments. In the Key-Policy Attribute-Based Encryption (KP-ABE) model, the encrypted data has been linked with a group of attributes that characterize it, as well as the access policy is stored in the user personal key. With the scheme, there is a trusted authority, which determines access structures in generating user keys, and the user can decrypt any ciphertext with attributes that meet the policy coded in the key. Although this model has the advantage of being able to offer flexible access control, it constrains the data owners in specifying access policies during the encryption process, which can make it less appropriate in a decentralized data-sharing environment. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model, on the contrary, integrates the access policy with the encrypted information and user keys are stored only with the attribute information. The design allows the data owner to state explicitly the access policies at the time of encryption, which combinations of the attributes must be present to be able to decrypt them. Due to such flexibility, CP-ABE has gained a lot of popularity with real-life systems in which data sharing is needed to be secure, over distributed platforms. Several research works have shown the practical applicability of Ciphertext Policy Attribute Based Encryption (CP-ABE) in various scenarios, including cloud storage services, medical information sharing, and Internet of Things (IoT) infrastructures [5], [7], [8]. More recent research works have extended the ABE schemes with additional functionalities. For example, multi-authority ABE, revocable ABE, blockchain-based ABE schemes, etc. In these recent research works, revocable ABE schemes have been proposed to provide dynamic control of user access privileges [14]. Similarly, blockchain-based ABE schemes have been proposed to provide additional transparency to the access control services in data sharing environments [13], [17]. All these research works show that ABE is still evolving as a viable security framework that can address access control services in modern distributed environments.

2- Related Work

One of the most widely accepted cryptographic techniques is Attribute-Based Encryption (ABE), which is being utilized for fine-grained access control in distributed environments such as cloud computing, IoT applications, and data sharing. Initial research focused on improving secure data management in cloud environments using ABE. For instance, a dynamic secure data management framework for mobile financial clouds was proposed to provide flexible access control for data using attribute-based encryption. Several survey papers have been presented to analyze the development of ABE techniques and their applicability in various domains. Rasori et al. [2] presented a comprehensive survey of ABE techniques for secure data exchange in IoT applications. Similarly, Jemihin et al. [6] focused their survey paper on ABE techniques for post-quantum security. Another survey paper presented by Khoachev [7] focused on the development of ABE schemes, including some of the challenges involved in their development. All these survey papers indicate that attribute-based encryption is gaining popularity for secure data access in modern distributed environments. Moreover, the usage of ABE has increased significantly in medical applications as well as IoT systems, which rely heavily on data sharing and access control. In determining the usability of ABE in healthcare systems, Walid et al. [3] presented a comparative analysis of ABE systems. In addition, blockchain-based ABE systems have been proposed for improving information autonomy as well as access control in medical as well as IoT systems. For instance, a blockchain-based ABE system has been presented for protecting EHR systems, as presented by Jiang et al. [9]. In addition, a blockchain-based searchable ABE system has been presented for improving security in e-health systems, as presented by Xiang and Zhao [22]. Furthermore, Yang and Zhang [29] have extended a blockchain-based multi-authority ABE system for improving security in access control of medical

data. In addition, Yang et al. [8] have proposed an attribute-based access control model for improving the security of IoT data in IoT environment through the usage of blockchain technology. Another important area of research is enhancing the efficiency and flexibility of ABE schemes. Various publications have proposed improved encryption models to facilitate fine-grained access control with lower computational overhead. As an illustration, Hohenberger et al. [10] presented a registered ABE scheme that aims at enhancing access control and identity registration. Wang et al. [12] proposed a better dual-policy ABE-based scheme to accommodate flexible access-control policies in cloud data-sharing systems. On the same note, Luo et al. [13] proposed a key-policy ABE model with switchable attributes to enable more flexible access control over encrypted data. Hierarchical and revocable ABE schemes have also been studied to support some of the main management and dynamic policy changes. Sasikumar et al. [14] suggested a hierarchical blockchain-based ABE protocol to industrial IoT systems, and Chen et al. [26] came up with an effective revocable ABE scheme that verifies data integrity. Furthermore, Yang et al. [15] examined ABE for secure data classification in a multi-cloud setup. In contrast, Pionero et al. [16] examined its use in a military IoT system. Other recent researches have investigated the integration of ABE with new technologies including artificial intelligence, blockchain, and digital twin systems. Dai et al. [19] proposed a blockchain-based access control system for digital twin systems that uses ABE to safeguard sensitive operational information. On the same note, Almasian and Shafieinejad [20] have presented a safe and secure cloud file-sharing system that integrates blockchain technology with ABE to enhance the confidentiality of data. ABE-based artificial intelligence-enhanced cloud security mechanisms have also been investigated; e.g., Ejeofobiri et al. [18] described the system that combines the use of artificial intelligence with ABE in securing cloud databases. In addition to this, Rani and Srivastava [27] proposed a safe fog-based computing architecture to Industry 5.0 through the ABE-based encryption tools. Huang et al. [28] also suggested a zero-trust access control architecture with ABE to complicate the network of IoT systems in breach of a device. Lastly, a number of studies have been directed towards tackling the lingering issues in ABE-based systems, such as preserving privacy, scalability, and issues on practical implementation. Venema et al. [23] examined the basic characteristics of pairing-based ABE schemes and determined the most significant issues associated with practical implementation. There are other studies which have suggested new encryption architectures that can enhance data protection and confidentiality in distributed setting. An example is that Arasi et al. [24] presented an auditable ABE-based data access controls model in cloud storage networks, and Routray and Bera [25] presented a privacy preserving spatio-temporal ABE framework in secure cloud-based applications. Moreover, Wu et al. [30] introduced a blockchain-based ABE-based data-sharing system that is applicable in privacy-preserving computation. All these works prove that even though ABE has made a great progress towards facilitating fine-grained access control, more studies are needed to enhance efficiency, scalability, and flexibility to support large-scale distributed systems. Although there is a great development in the research on attribute-based encryption, there are a number of limitations in the present practice. The way to enhance the encryption mechanisms or combine ABE with blockchain and IoT technologies are the most common topics of contemporary research, but the problem of scalability, changing policies, and computational efficiency of large-scale distributed settings are still untackled. Specifically, available frameworks are either associated with high computational cost or they suffer significantly due to centralized management units which could be restrictive to their performance in highly dynamic and resource constrained systems. Moreover, whereas solutions based on ABE with the help of blockchain enhance transparency and security, these systems can add new latency and storage costs. Thus, an even more effective and scalable secure data-sharing framework that ensures a high level of access control and reduces system complexity and performance overhead is still required. There are also some secure data sharing models with ABE that are proposed to work in cloud storage and distributed settings, such as blockchain-based access control systems and privacy-enhancing models of encryption [26], [27], [28], [29],30]. Most of the available literature is dedicated to implementing attribute-based encryptions in connection to blockchain or cloud environments (see Table 1), but most of them have high computational costs and fail to scale as the number of participants increases, which is why a more efficient and flexible secure data-sharing model is desirable.

Comparison of Related Attribute-Based Encryption Approaches

Ref.	Model / Technique Used	Goal of the Study	Achieved Result	Limitation
[1]	Attribute-Based Encryption (ABE) for mobile financial clouds	Secure dynamic data management in mobile cloud environments	Improved flexible access control and data confidentiality in financial cloud services	High computational overhead for large-scale cloud environments
[2]	Survey of ABE schemes for IoT	Analyze different ABE models suitable for IoT systems	Identified suitable ABE architectures for constrained IoT devices	Lacks practical implementation and experimental validation

[3]	Post-quantum ABE survey	Evaluate ABE techniques against quantum security threats	Provided classification of post-quantum secure ABE schemes	Mostly theoretical; limited real-world deployment
[5]	Comparative analysis of ABE schemes for healthcare	Secure medical data sharing in healthcare systems	Demonstrated improved confidentiality for Electronic Health Records (EHR)	High computational complexity for medical data systems
[6]	Blockchain-based ABE for EHR systems	Protect medical records using blockchain and encryption	Achieved tamper-resistant and secure patient data sharing	Blockchain latency may affect system performance
[7]	Searchable ABE with blockchain	Secure and searchable healthcare data systems	Improved privacy-preserving data retrieval	Increased storage and computation overhead
[8]	Multi-authority ABE for EHR	Decentralized access control for healthcare records	Reduced dependency on single authority for key management	Complex key distribution mechanism
[9]	Blockchain-based attribute access control for IoT	Secure IoT data protection using distributed ledger	Enhanced transparency and decentralized access management	Blockchain scalability challenges
[10]	Registered ABE scheme	Improve identity registration and access management	Stronger identity-based access control mechanism	Implementation complexity in distributed environments
[12]	Key-policy ABE with switchable attributes	Flexible fine-grained access control for encrypted data	Improved adaptability of encryption policies	Increased system complexity
[13]	Hierarchical blockchain-assisted ABE	Secure industrial IoT communication	Improved hierarchical data sharing and scalability	Blockchain overhead for large networks
[14]	Revocable ABE with verifiable integrity	Dynamic user revocation and secure data integrity	Efficient key revocation with verification mechanism	Additional computation during revocation process
[15]	Multi-cloud ABE with data classification	Secure distributed cloud storage environments	Improved secure data classification and access control	Increased complexity in multi-cloud key management
[17]	Blockchain-enabled ABE for digital twin systems	Secure operational data in digital twin environments	Achieved secure access control for industrial data	High storage overhead
[21]	Zero-trust architecture combined with ABE	Secure IoT networks against compromised devices	Strengthened access control with zero-trust model	Requires high computational resources
[25]	Blockchain-based ABE data sharing system	Secure distributed data sharing with privacy protection	Achieved privacy-preserving computation	Blockchain overhead and scalability concerns

3- Methodology

This research adopted a combined methodology that integrates the descriptive–analytical approach with an applied–experimental approach, aiming to study Attribute-Based Encryption as an advanced mechanism for fine-grained data access control and to verify its practical applicability in cloud and distributed environments that cannot be fully trusted. In the initial stages, the descriptive–analytical approach was employed to analyze traditional access control models and highlight their limitations, as well as to review the relevant literature on attribute-based encryption and its various models, with particular emphasis on the theoretical and practical differences between KP-ABE and CP-ABE. This phase helped in the establishment of the theoretical framework of the study, the identification of the research gap, and the determination of the research objectives. In the next phase, the study moved towards the applied experimental research approach with the design and implementation of an extensive practical framework, which is based on the CP-ABE model. In this regard, the study implemented the establishment of the cryptographic infrastructure, the determination of the public parameters and the master key, the binding of the user key to different attribute sets, the

encryption of the data and the data encryption key with attribute-based access policies, and the evaluation of the access and decryption mechanisms with the help of scenarios simulating real-world situations, encompassing both legal and illegal access scenarios. The analysis is supplemented by the support of a comparative perspective in the analysis of the results, where the behavior of the implemented system is compared with traditional access control mechanisms in terms of security, independence, and applicability. Therefore, this study falls into the category of an applied and experimental research study, which is supported by theoretical analysis, where scientific analysis, practical implementation, and evaluation of the results are combined to create a comprehensive understanding of the effectiveness of attribute-based encryption in modern enterprise environments.

Applied Framework

1. Experimental Execution Environment

The experimental application of this concept took place within a real software environment to assess the viability of attribute-based encryption (ABE) as an access control method for data. The software system was built using the Python programming language, utilizing an existing scholarly library that offers the implementation of Ciphertext Policy Attribute-Based Encryption (CP-ABE), as well as a traditional symmetric encryption technique. The software environment uses a multitasking operating system and a regular software stack, without any specific hardware requirements. These results show that the suggested method can be used within a real enterprise environment.

2. Description of the Data Used

The system was tested with a real-world document related to administration, which was in PDF format. The document contained sensitive information related to the organization as well as financial data. This document was selected for testing as it belongs to a particular category of data that usually exists in an enterprise environment, which typically requires fine-grained access control as it contains sensitive information. The document was considered as a whole data object, which means that the data was fully encrypted prior to its storage, without any part of the document remaining unencrypted, thus providing complete confidentiality. This is a realistic approach towards data management, as enterprise data, especially sensitive data, usually exists as a whole document, which remains stored or shared with access control restrictions using strong cryptographic techniques.

3. Setting Up the Attribute-Based Encryption System

In the first practical implementation phase, a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework was established as a structural base for the proposed framework in the context of the proposed access control architecture. This initial phase sought to develop the basic framework on which the proposed architecture would be built. The standard Ciphertext-Policy ABE algorithm, which has been widely documented in the literature and relies on a sound mathematical foundation based on bilinear pairing-based cryptography, has been implemented. In the context of the proposed framework, a specific cryptographic group has been instantiated, which provides the mathematical properties required in the context of attribute-based encryption and decryption, resisting user collusion attacks and ensuring that access keys cannot be derived from ciphertexts. In the following discourse, we will elaborate on the creation of a CP-ABE system object that will be responsible for executing system-level operations after the creation of the cryptographic group. This phase's setup process has been successfully implemented, resulting in the creation of the system's public parameters and the master key of the attribute authority. The public parameters are a set of data that are shared by the processes of both encryption and decryption, while the master key will be maintained by the attribute authority to generate the private keys of the users based on an authorized attribute set. This phase can be considered the fundamental part of the suggested framework, as all other processes are dependent on the results of this phase. This phase's separation into public parameters and master keys will add an extra layer of security to the overall process, as an unauthorized entity will not be able to obtain access keys even if the ciphertext or storage environment is compromised. This phase's implementation will be carried out using the following code:

```
from charm.toolbox.pairinggroup import
PairingGroup
from charm.schemes.abenc.abenc_bsw07 import
CPabe_BSW07

group = PairingGroup('SS512')
cpabe = CPabe_BSW07(group)

public_key, master_key = cpabe.setup()
```

The result of this code will represent the actual point of initialization of the system, as the computed public parameters (public_key) are eventually used to encrypt the data encryption keys according to the access control policies. On the other hand, the master key (master_key) is solely used to generate attribute-based private keys for users within the scope of their assigned permissions. This distinction in the use of keys enhances the security of the access control process by preventing any unauthorized entity from gaining access.

4. User Key Generation and Attribute Binding

Following the completion of the attribute-based encryption framework setup, which involved the creation of public parameters and the master key, the implementation moved on to the next phase, which involved the issuing of users' access keys. The objective of this phase was to map each system user to a specific set of authorized organizational attributes, which accurately represented the users' real permissions in the organization, and which were subsequently used to verify users' eligibility in accessing the encrypted information. The generation of users' keys involved the attribute authority, which possessed the master key of the system, and which issued users' private encryption keys directly linked to their assigned attribute sets. The keys formed the only means through which users attempted the decryption of the encrypted information, without depending on other means of verification or authorization at the access level.

In the experimental system, there were two user groups created, which were intended to evaluate the effectiveness of fine-grained access control. The first group of users had attribute sets that met the specified access policy, while the second group of users had attribute sets that failed to satisfy the specified policy. This enabled the evaluation of the system's ability to differentiate between authorized and unauthorized users, based on their attributes, irrespective of their identities.

In practice, each user's attribute set was input into the key generation algorithm, which produced a private encryption key containing the users' attributes in its cryptographic structure. The generated key was used in attempting the decryption of the data encryption keys, which could not be combined with other keys or modified to satisfy unauthorized access policy.

The user key generation process:

```
attributes_client1 = ['HR', 'Manager',
'Confidential']
sk_client1 = cpabe.keygen(public_key, master_key,
attributes_client1)

attributes_client2 = ['HR', 'Staff']
sk_client2 = cpabe.keygen(public_key, master_key,
attributes_client2)
```

The personal key of each user is a direct result of the interaction between the authorized set of attributes and the master key of the system, which cannot be reproduced or derived without the possession of the master key. The empirical evaluation also reveals that the variation in the attribute set results in a fundamental difference in the users' ability to decrypt the information at a later stage, even when there is partial sharing of the attributes. This phase is a critical part of the applied framework, as it transforms the access control from a centralized decision-making approach to a fundamental property of the users' keys, thus differentiating it from other conventional access control schemes. The generation of the users' keys also removes the necessity of modifying the users' keys in accordance with their access requests, thus providing a distinction between attribute management and data storage.

5. Encrypting the Data Encryption Key According to the Access Policy

After that, the symmetric data encryption key was encrypted using the Ciphertext Policy Attribute-Based Encryption (CP-ABE) model with an embedded access policy based on the approved organizational requirements. This ensures that key recovery is possible only for users whose attributes meet the conditions. In this way, data is secured in a multi-level security environment where data content is secured using symmetric encryption to ensure maximum efficiency and performance, and the encryption key is secured using an attribute-based access policy. In this way, data access is controlled in a fine-grained manner at the encryption level, and data cannot be decrypted by unauthorized users even in cases where the ciphertext or storage environment is compromised.

```
policy = '(HR and (Manager or Auditor) and
Confidential)'
ct_abekey = cpabe.encrypt(public_key, dek, policy)
```

By carrying out this step, the protection of the data is ensured through a two-layered security approach. Firstly, the content of the data is protected using symmetric key encryption, which provides efficient processes in the encryption and decryption of the data, especially when dealing with large amounts of data. Secondly, the symmetric key is protected using attribute-based access control, which provides restrictions on the access of the symmetric key under certain circumstances. The use of a two-layered approach provides a more secure system against unauthorized use in case of storage compromise. The use of attribute-based access control provides a high level of flexibility in managing the system without re-encrypting the data.

6. Data Access Execution, Decryption, and Implementation Findings

After successfully developing the data encryption process and binding the data encryption key to an attribute-based access policy, the implementation process moved to the testing phase of the access/decryption process. This phase

was designed to assess whether the developed system offers fine-grained access control to the data such that only authorized users are allowed to decrypt the data. This evaluation process began by simulating an actual process of accessing the data, decrypting the data encryption key, and retrieving the contents of the file or failing to do so based on user permissions.

6.1 Operational Flow

Upon receipt of a request to access a file that has been stored in encrypted form, the process of access will be carried out according to several steps that are intended to enforce the access control policy directly at the level of encryption without relying on a trusted server. This process could be explained as follows:

1. Retrieval of Encrypted Data: In the first part of this process, the encrypted file and the associated encrypted data key are retrieved from the storage environment, which may be either cloud-based or distributed. This retrieval happens without any user authentication or request authorization by the server. The role of the server here is limited to providing the stored data. This scenario highlights the concept of minimal trust.

2. Attempt to Decrypt the Data Encryption Key: Once the encrypted data is received, the user, using his own private key derived from the corresponding attribute set, attempts to decrypt the data encryption key, which is encrypted using the CP-ABE policy. This is a crucial aspect of the access control system, in which the attribute-based encryption process is triggered in order to verify the permissions of the user in executing the action without disclosing the actual data content.

3. Implicit Evaluation of the Access Policy: In the process of attempting to decrypt the data key, the congruence between the attributes of the user and the access policy embedded in the ciphertext is checked implicitly and automatically. This is done without depending on any external factors or any decisions by the central administration; rather, it is based on the inherent characteristics of the attempt to decrypt. If the conditions in the policy are not satisfied, the attempt to decrypt is rejected mathematically without any further information being provided to the user and the storage server.

4. Transition to Content Decryption or Failure: If the policy evaluation is successful and the data encryption key is decrypted correctly, the next step is to apply the decrypted key to decrypt the content of the file to restore it to its original form. However, if any of the steps fails to execute correctly, especially the attribute matching with the access policy, the process is terminated, and no content is retrieved to maintain data confidentiality.

6.2 Authorized Access Case (Client 1)

In this case, the key of client (1), which had been previously generated based on an attribute set satisfying the access policy, was used. The decryption of the data encryption key completed successfully, enabling the system to proceed to decrypt the file and retrieve its original content without any data loss or corruption.

This operation was practically executed using the following code:

```
recovered_dek = cpabe.decrypt(public_key, sk_client1, ct_abekey)

# Decrypt the file using the recovered data encryption key
cipher_dec = AES.new(recovered_dek, AES.MODE_EAX, nonce=nonce)
plaintext = cipher_dec.decrypt(ciphertext)

with open('decrypted_client1.pdf', 'wb') as f:
    f.write(plaintext)
```

The result of this operation clearly proves that the direct and deterministic satisfaction of the access policy enables the user to access the file in its original form without losing any of the file's content. This proves that the access control decision is not being satisfied at the storage level or using any other control mechanism; rather, it is being satisfied at the encryption level through the decryption of the data encryption key. The result of this operation also proves the

efficacy of the fine-grained attribute-based access control model in which the single condition for access is the decryption of the data. Additionally, the result proves that access control decisions are being satisfied with complete accuracy and reliability even in a partially untrusted environment; hence, the system is more likely to be used in a real-world environment.

6.3 Unauthorized Access Case (Client 2)

When the access process was repeated using the client with the identifier (2), which does not satisfy the requisite access policy in its attribute set, decryption of the data encryption key failed. The process ended at this point, and there was no valid data encryption key, which prevented the content decryption. This shows the enforcement of the access policy at the cryptographic level, which prevents users without the required attributes from accessing the information without the use of other access control mechanisms.

```
# Attempt to decrypt the data encryption key using client (2) key
recovered_dek = cpabe.decrypt(
    public_key,
    sk_client2,
    ct_abekey
)
```

This procedure resulted in a decryption failure due to the access policy not being satisfied, leaving the encrypted file unusable. This outcome confirms that possession of the ciphertext alone—even when attempting to decrypt it—does not grant any additional access capability unless the required attributes are satisfied.

6.4 Practical Implementation Findings

The results of this phase's execution will be several fundamental findings that not only validate the effectiveness of the proposed applied framework but will also illustrate, at a practical level, how attribute-based encryption could be utilized as a fine-grained access control technique within a partially untrusted environment. These findings can be summarized as follows:

1. Access Control Embedded in Encryption: Empirical findings show that the choice to either grant or deny access to data is not controlled by an intermediary server or any specific centralized access control mechanism. What is more, access control is achieved in an automatic and direct manner through the very process of data decryption. The success or failure in decrypting the data-encryption key depends entirely on the correspondence between the attributes of the user and the access policy embedded in the ciphertext. Access control is revealed to be an inherent feature of the system’s very cryptographic framework, which reduces the probability of any manipulation by the system’s administration.

2. Independence of Storage from Access Logic: The process also implies that the storage server does not take part in permission evaluation or user authentication. Its sole function is to provide access to the data in its encrypted form upon request. This explicit separation of functions reduces dependency on the trustworthiness of the storage server and reduces the potential for data leakage or abuse in cases where storage infrastructure is compromised. Additionally, it enhances the system’s ability to function in cloud or distributed systems where trust levels vary.

3. Deterministic Prevention of Unauthorized Access: From the experimental results, especially for client (2), it is evident that the system denies access to the data if the access policy conditions are not met, without revealing any additional information regarding the content of the file or the structure of the access policy. This also aligns with the deterministic nature of attribute-based encryption, which mathematically stops the process if decryption is not possible, thus not providing any partial output, thereby improving data confidentiality.

4. Applicability in Realistic Environments: The implemented operational workflow is presented as a model that can be considered practical and representative of actual usage scenarios that are common in contemporary enterprise systems. In this initial phase, the retrieved data from the storage environment are in an encrypted form. At this point,

the authorization process is validated locally on the user's device via an attempted decryption process. This process illustrates that no alterations are necessary to existing storage infrastructures to accommodate the proposed system. Therefore, integration with existing file management systems or cloud computing systems can be achieved in a manner that is both secure and scalable. This phase represents a natural continuation of the preceding sections in which both methodological and conceptual considerations are united in a manner that is both practical and applicable to a workflow environment. The execution of this phase relies on the public parameters and master key that are defined in Section 3. This provides a basis for the entire system's security. Additionally, this phase relies on the attribute-bound user key. This represents an operationalization of the theoretical considerations presented in Section 4. In this phase, user access privileges are based on attributes rather than identities. At the same time, this phase relies on the encrypted data and data encryption key. These are based on an access policy as described in Section 5. In this context, the intersection of both symmetric encryption methodologies and the CP-ABE protocol is both realistic and actualized. This represents a culmination in the execution process of the entire system, from initial cryptography to the culmination of system implementation. This illustrates that no stage in the proposed system is implemented in isolation or in a vacuum. Instead, it is both cohesive with other stages in the system and thus illustrates its feasibility in allowing for stable operation in actual usage scenarios.

7. Discussion of Results

In this section, there will be an analytical discussion of the results of the implementation, with the aim of interpreting the behavior of the system with regard to the previously stated objectives of the research. This will be supported by analytical tables that will show the interaction of the attributes with the access control policies, the results of the decryption process under various access control scenarios, as well as an analysis of the practical limitations of the implementation. This section will also place the results within the context of attribute-based encryption systems, as well as compare it with traditional server-based access control.

8.1 Summary of Scenarios

Table (1) shows the most important scenarios that have been practically implemented during the experiment. This provides a consolidated view of system behavior under different conditions regarding system attributes. These scenarios include authorized access scenarios, unauthorized access scenarios, as well as a dynamic scenario that involves changes to user attributes after issuing keys, aiming to test the system's reaction to organizational changes.

Table (1): Summary of Implemented Access Scenarios

Scenario	Attribute Status	Access Policy Satisfied	Decryption Result	Access Outcome
Client (1)	Complete	Yes	Successful	Access Granted
Client (2)	Incomplete	No	Failed	Access Denied
Client (1) after attribute modification	Insufficient	No	Failed	Access Denied

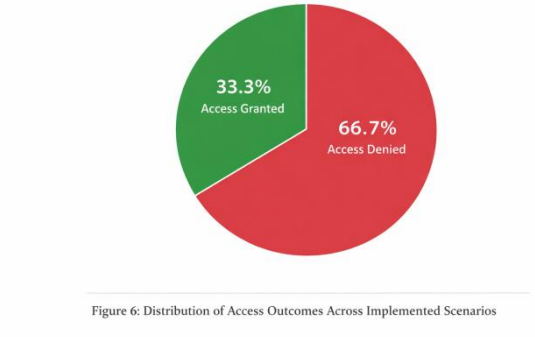

Figure 6: Distribution of Access Outcomes Across Implemented Scenarios

The results clearly show that access decisions depend exclusively on whether the current set of attributes satisfies the access policy embedded within the ciphertext, without reliance on user identity or any external factors. This confirms the dynamic and fine-grained nature of attribute-based access control.

8.2 Analysis of Fine-Grained Access Control Effectiveness

In this sub-section, we will look at the direct relationship between attribute sets and access decisions as shown in Table (2), to emphasize the determinative aspects of the system that have been implemented. Determinism is said to be the characteristic that the result of the decryption is completely determined by the attribute state without any intermediate decisions.

Table (2): Impact of Attributes on Access Decisions

Attribute Set	Policy Satisfied	Implementation Observation
All required attributes	Yes	Data fully recovered
One missing attribute	No	Process stopped at data key decryption
Partially shared attributes	No	No additional privileges granted

The above results show that the system is secure from privilege accumulation and policy circumvention even if the user has some of the required attributes. Any kind of breach in the access policy will result in the process being terminated at an early stage.

8.3 Separation of Storage from Access Control (Applied Analysis)

Table (3) illustrates the functional contribution of the system's components during real execution, with particular emphasis placed upon the dichotomy between the storage of data and access control logic. The dichotomy is a reflection of a design goal of the proposed system that reduces reliance upon trusted intermediary infrastructure.

Table (3): Roles of System Components During Execution

Component	Effective Role During Execution	Decryption Capability
Storage Server	Storing ciphertexts	No
Attribute Authority	Issuing keys	No
Authorized User	Performing decryption	Yes
Unauthorized User	Attempting decryption	No

From this analysis, it can be determined that access control within the system does not occur at the infrastructure level, but rather using specific cryptographic keys and attributes. Therefore, the system manages to sustain its resilience even if the storage servers are compromised or abused.

8.4 Analysis of Practical Limitations Observed During Implementation

Despite the positive results, several practical limitations were encountered during deployment that could be related to the intrinsic characteristics of attribute-based encryption schemes, rather than to the design or implementation of the system. Table 4 summarizes the encountered limitations.

Table (4): Practical Limitations Observed During Implementation

Limitation	Practical Description	Impact on the System
Attribute management	Need for precise attribute definition	Requires organizational governance
Revocation	Not instantaneous without key updates	Temporarily limited impact
Policy complexity	Increased complexity raises computational cost	Affects performance
Key management	Reliance on an attribute authority	Central trust point

These restrictions are like those found in related literature and demonstrate the trade-offs that are inevitably made in security, efficiency, and manageability. They also highlight the importance of organizational structures in facilitating effective attribute and policy management.

8.5 Implementation-Oriented Comparison with Traditional Access Control

Table (5) presents a practical comparison between the implemented system and traditional server-based access control mechanisms, based on observations from the experimental deployment.

Table (5): Practical Comparison with Traditional Access Control Mechanisms

Criterion	Traditional Access Control	Implemented System
Location of access decision	Server	Encryption layer
Trust in server	High	Low
Resistance to compromise	Limited	High
Adaptation to changes	Administrative	Cryptographic

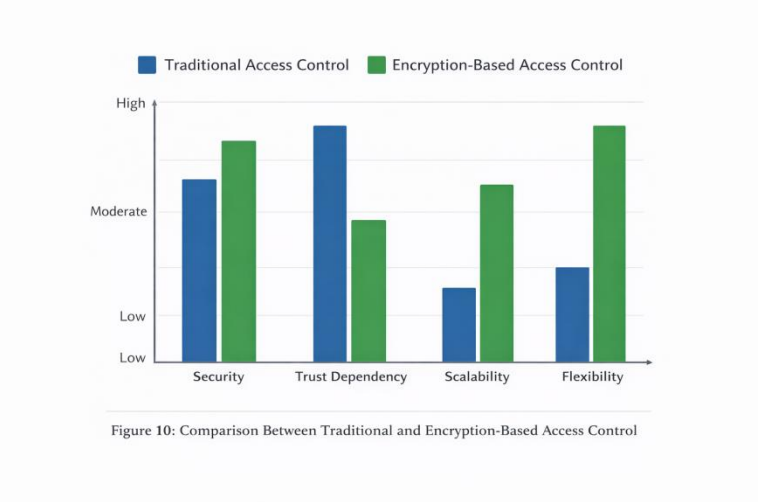

Figure 10: Comparison Between Traditional and Encryption-Based Access Control

This comparison highlights the practical value of the implemented system, particularly in cloud and distributed environments where full trust in storage servers cannot be assumed. It demonstrates that shifting access control logic to the encryption layer achieves higher security and autonomy while reducing dependence on centralized administrative enforcement.

9. Conclusions

This study offers a thorough examination and analysis of Attribute-Based Encryption (ABE) as a complex and powerful solution to access control in cloud computing and distributed computing infrastructures where full trust in the infrastructure is not guaranteed. The rationale behind this study stems from the basic fact that traditional access control models in server infrastructures are deemed inadequate in terms of security and flexibility in handling critical information under the administration of intermediary parties. The study develops a solid foundation in Attribute-Based Encryption (ABE) and its models, with emphasis on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) due to its huge potential in empowering data owners to set specific policies independently of users. The theoretical foundation is combined with a complete practical implementation, which includes the setup of the cryptographic infrastructure, the creation of attribute-bound user keys, encryption of the data encryption key with specific access policies, and evaluation of the access and decryption processes with real-world scenarios.

From the results of the implementation, it has been observed that the proposed system provides fine-grained access control at the level of encryption itself without depending on a trusted server or a centralized access control system. The experimental results have confirmed that access control decisions are made deterministically during the process of decryption based solely on the matching of the attributes of the user with the access policy embedded during the process of encryption. This ensures that there is no unauthorized access, even if the ciphertexts are compromised or the storage environment itself has been compromised. From the point of view of its application, the research has proven the applicability of Attribute-Based Encryption systems in real-world enterprise environments without making fundamental changes to the existing infrastructure of the system, while at the same time maintaining an acceptable level of performance. At the same time, the research has also revealed the limitations of Attribute-Based Encryption

systems, which are a part of this category of systems. These limitations have been observed from the point of view of their application, which have resulted from the intrinsic properties of Attribute-Based Encryption systems. The research has thus drawn a conclusion that Attribute-Based Encryption, especially CP-ABE, is a viable solution for enforcing access control at the level of data without compromising security, especially in a partially untrusted environment. At the same time, the research has attempted to bridge the gap between theory and practice by presenting an integrated framework for its application, which has proven its viability as an effective alternative or complementary solution to access control systems currently being employed by enterprise systems.

REFERENSI

[1]. T. Ganesan, "Dynamic Secure Data Management with Attribute-Based Encryption for Mobile Financial Clouds," International Journal of Applied Science Engineering and Management, vol. 17, no. 2, 2023.
[2]. M. Rasori, M. La Manna, P. Perazzo, and G. Dini, "A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8269–8290, 2022.
[3]. Z. B. Jemihin, S. F. Tan, and G. C. Chung, "Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey," Cryptography, vol. 6, no. 3, p. 40, 2022.
[4]. T. Khoachev, "A Brief Review on Attribute-Based Encryption Approaches," SSRN Electronic Journal, 2023.
[5]. R. Walid, K. P. Joshi, and S. G. Choi, "Comparison of Attribute-Based Encryption Schemes in Securing Healthcare Systems," Scientific Reports, vol. 14, p. 7147, 2024.
[6]. Y. Jiang, X. Xu, and F. Xiao, "Attribute-Based Encryption with Blockchain Protection Scheme for Electronic Health Records," IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3884–3895, 2022.
[7]. X. Xiang and X. Zhao, "Blockchain-Assisted Searchable Attribute-Based Encryption for E-Health Systems," Journal of Systems Architecture, vol. 124, p. 102417, 2022.
[8]. X. Yang and C. Zhang, "Blockchain-Based Multiple Authorities Attribute-Based Encryption for EHR Access Control Scheme," Applied Sciences, vol. 12, no. 21, p. 10812, 2022.
[9]. Z. Yang et al., "An Attribute-Based Access Control Scheme Using Blockchain Technology for IoT Data Protection," High-Confidence Computing, vol. 4, no. 3, p. 100199, 2024.
[10]. S. Hohenberger, G. Lu, B. Waters, and D. J. Wu, "Registered Attribute-Based Encryption," in Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2023, pp. 511–542.
[11]. T. Wang, Y. Zhou, H. Ma, and R. Zhang, "Enhanced Dual-Policy Attribute-Based Encryption for Secure Data Sharing in the Cloud," Security and Communication Networks, vol. 2022, Art. no. 1867584, 2022.
[12]. F. Luo, H. Wang, X. Yan, and J. Wu, "Key-Policy Attribute-Based Encryption with Switchable Attributes for Fine-Grained Access Control of Encrypted Data," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 7245–7258, 2024.
[13]. A. Sasikumar et al., "Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things," IEEE Access, vol. 12, pp. 12586–12601, 2024.
[14]. S. Chen, J. Li, Y. Zhang, and J. Han, "Efficient Revocable Attribute-Based Encryption with Verifiable Data Integrity," IEEE Internet of Things Journal, vol. 11, no. 6, pp. 10441–10451, 2023.
[15]. G. Yang et al., "An Efficient Attribute-Based Encryption Scheme with Data Security Classification in the Multi-Cloud Environment," Electronics, vol. 12, no. 20, p. 4237, 2023.
[16]. L. Pioro, J. Sychowiec, K. Kanciak, and Z. Zielinski, "Application of Attribute-Based Encryption in Military Internet of Things Environment," Sensors, vol. 24, no. 18, p. 5863, 2024.
[17]. Y. Dai et al., "Blockchain Empowered Access Control for Digital Twin System with Attribute-Based Encryption," Future Generation Computer Systems, vol. 160, pp. 564–576, 2024.
[18]. M. Almasian and A. Shafieinejad, "Secure Cloud File Sharing Scheme Using Blockchain and Attribute-Based Encryption," Computer Standards & Interfaces, vol. 87, p. 103745, 2024.
[19]. C. K. Ejeofobiri et al., "Securing Cloud Databases Using AI and Attribute-Based Encryption," International Journal for Multidisciplinary Research, pp. 39–47, 2025.
[20]. S. Rani and G. Srivastava, "Secure Hierarchical Fog Computing-Based Architecture for Industry 5.0 Using an Attribute-Based Encryption Scheme," Expert Systems with Applications, vol. 235, p. 121180, 2024.
[21]. W. Huang et al., "ZT-Access: Combining Zero Trust Access Control with Attribute-Based Encryption Against Compromised Devices in Power IoT Environments," Ad Hoc Networks, vol. 145, p. 103161, 2023.
[22]. M. Venema, G. Alpar, and J. H. Hoepman, "Systematizing Core Properties of Pairing-Based Attribute-Based Encryption to Uncover Remaining Challenges in Enforcing Access Control in Practice," Designs, Codes and Cryptography, vol. 91, no. 1, pp. 165–220, 2023.
[23]. V. E. Arasi, K. I. Gandhi, and K. Kulothungan, "Auditable Attribute-Based Data Access Control Using Blockchain in Cloud Storage," The Journal of Supercomputing, vol. 78, no. 8, pp. 10772–10798, 2022.
[24]. K. Routray and P. Bera, "Privacy Preserving Spatio-Temporal Attribute-Based Encryption for Cloud Applications," Cluster Computing, vol. 28, no. 1, p. 34, 2025.
[25]. H. Wu, Y. Liu, K. Zhu, and L. Zhang, "Data-Sharing System with Attribute-Based Encryption in Blockchain

and Privacy Computing," Symmetry, vol. 16, no. 11, p. 1550, 2024.
[26]. X. Yang, A. Chen, Z. Wang, and S. Li, "Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption," Security and Communication Networks, vol. 2022, Art. no. 2204832, 2022.
[27]. K. K. Singamaneni, G. Muhammad, and Z. Ali, "A Novel Quantum Hash-Based Attribute-Based Encryption Approach for Secure Data Integrity and Access Control in Mobile Edge Computing-Enabled Customer Behavior Analysis," IEEE Access, vol. 12, pp. 37378–37397, 2024.
[28]. A. Saidi, O. Nouali, and A. Amira, "SHARE-ABE: An Efficient and Secure Data Sharing Framework Based on Ciphertext-Policy Attribute-Based Encryption and Fog Computing," Cluster Computing, vol. 25, no. 1, pp. 167–185, 2022.
[29]. X. Wang et al., "Attribute-Based Access Control Encryption," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 3, pp. 2227–2242, 2024.
[30]. J. Y. Deshmukh, S. K. Yadav, and G. M. Bhandari, "Attribute-Based Encryption Mechanism with Privacy-Preserving Approach in Cloud Computing," Materials Today: Proceedings, vol. 80, pp. 1786–1791, 2023.