Long-Distance Cross-Domain English Online Resources Based on Attribute-Based Encryption

Xiaofeng You

Department of General Education, Luoyang Vocational College of Culture and Tourism, Luoyang, Henan 471000, China
E-mail: youxiaofeng49@126.com

Received 24 March 2026; Accepted 02 May 2026

Abstract

The rapid growth of distributed learning systems and cross-disciplinary digital services development has augmented the pressure on protecting and effective systems of sharing online educational resources. Conventional identity-based access control systems usually do not offer scalable and fine-grained security in heterogeneous systems where users are members of various administrative domains. To overcome these weaknesses, this paper suggests a secure long-distance cross-domain resource sharing model that is founded on a Hybrid Advanced Encryption Standard (AES) and Multi-Authority Key-Policy Attribute-Based Encryption (MA-KP-ABE) scheme of English online learning resources. The offered architecture combines symmetric encryption as the efficient method of data protection with the attribute-based encryption to implement flexible access control policies across various domains. Within the framework, AES is employed in expedited data encryption, MA-KP-ABE is employed in efficient key management, attribute verification by multiple authorities, dynamic policy enforcement as well as the ability to revoke attributes. The system was tested experimentally on some performance measures such as encryption time, decryption time,

Journal of Cyber Security and Mobility, Vol. 15_4, 867–914.
doi: 10.13052/jcsm2245-1439.1544

key generation time, storage overhead, scalability and accuracy of access control. The experimental findings prove that the proposed hybrid framework has an encryption time of 105.2 ms, decryption time of 82.5 ms, and a key generation time of 52.59 ms. The model also has low storage overhead of 6.5% and scalability to cross-domain settings of over 1500 users. Moreover, the system has a high accuracy in access control of 98.60% which means strong authorization and policy enforcement. The innovation of the given work is formed by the combination of AES and multi-authority KP-ABE with dynamic policy management and attributes revocation where it is possible to provide cross-domain access to online educational resources with the required security, scalability, and efficiency.

Keywords: Advanced encryption standard, multi-authority key-policy attribute-based encryption, cross-domain resource sharing, access control security, online learning resources, secure data encryption.

1 Introduction

In the modern digital networked environment, the need to share online resources via secure means across administrative boundaries has become a necessity in the collaborative, federated services, and large distributed applications domain [1]. Conventional identity-based access control is not usually scalable or able to articulate fined grained policies in dynamic across domain environments where users can be of different organizations and have varied privileges. Attribute-Based Encryption (ABE) is an effective cryptographic tool, which binds data access control policies to attributes of users or objects, to provide fine-grained access control without centralized authorities [2]. The capability of ABE to incorporate access policies into encryption makes sure that only users that have the relevant attributes can decrypt sensitive data, enhancing confidentiality and privacy. This feature is especially useful in long-distance cross-domain web platforms, in which there is a greater variation of trust limits, and enforcement may not be possible in a centralized way [3]. ABE enables a single cryptography layer to enable the system to eliminate the reliance on a trusted third party to enforce ABE, and to achieve scalability in distributed systems. The recent developments in ABE research demonstrate its usefulness in cloud computing, IoT and joint data sharing. Nevertheless, there are still major challenges of policy coordination, controlling key management and trust assumptions when adapting ABE to cross-domain long-distance resources [4].

To facilitate the secure cross-domain access based on ABE and such control schemes, several approaches have been suggested. One of them is the decentralized attribute-based access control (D-ABAC) that exchanges attribute information securely across domains through group signatures and minimizes dependence on a central authority although it still faces a synchronization overhead and trust establishment problem [5]. Other classical ciphertext-policy attribute-based encryption (CP-ABE) schemes provide fine-grained access control through the integration of ciphertext policies, but they do not scale well and they cannot effectively revoke attributes in multi-domain environments [6]. Extensions of CP-ABE with hierarchies and traceability are intended to facilitate structured data and accountability, but may be costly to execute key exchange and policy enforcement operations in heterogeneous networks [7]. Moreover, the vast majority of current frameworks presuppose homogeneous network conditions and are unable to effectively address long-distance latency or asynchronous attribute updates, generating performance and usability gaps with real-world deployments [8].

Other interesting methods are proxy re-encryption with ABE, which offers greater flexibility in ciphertext domain-adaptation, but adds complexity to re-encryption key administration, and may bring about trust threats in an environment where proxies are semi-trusted [9]. Quantum-resistant ABE schemes apply access control to post-quantum environments by improving security but, in many cases, they increase the computational cost that restricts their implementation on resource-constrained devices [10]. ABE models with the assistance of blockchain improve their transparency and decentralization, but the models add new consensus and smart contracts overhead, which can adversely affect scalability [11]. Homomorphic or zero-knowledge privacy-preserving ABE can be used to perform confidential attribute checks but may enable inference attack vectors and does not yet have efficient policy reconciliation across domains. Such constraints point to the necessity to develop a single, effective, and scalable framework that would be specific to long-domain cross-domain environments [12].

These limitations are overcome in the proposed framework by adding a cross-domain ABE orchestration layer, which coordinates decentralized attribute authorities with a lightweight cross-domain policy broker, which guarantees real-time policy reconciliation and an efficient distribution of key. The framework reduces the cryptographic overheads and yet offering high levels of security by combining attribute revocation that is aware of policy and adaptive. It has introduced novel contributions such as distributed attribute consensus mechanism, which removes points of trust, latency-conscious

policy enforcement optimized with long-distance links, and a hybrid ABE + blockchain audit trail mechanism, which enforces transparent accountability with no performance penalties. Together, these components favor safe, distinctive as well as privacy-conserving access to web-based resources over heterogeneous administrative divisions. This innovation facilitates the feasible implementation during cloud-native services, federated learning, and collaborative research infrastructures, which cut across the global networks.

Contributions

- Propose a safe long-distance inter-domain resource sharing framework of English online learning platforms is to combine Advanced Encryption Standard (AES) with Multi-Authority Key-Policy attribute-based encryption (MA-KP-ABE) which helps facilitate effective and secure information encryption in the heterogeneous domains.
- Establish a multi-authority attribute management system that allow decentralized attribute checking and flexible generation of keys and, subsequently, offer fine-grained access control to users in different administrative domains.
- Implement a dynamic access/revocation control policy and attribute revocation policy that helps in enhancing the security through the addition of adaptive policy between distributions and the online learning resources.
- Evaluate the efficiency of the proposed framework on the basis of several performance parameters including encryption efficiency, decryption efficiency, key generation overhead, storage consumption, scalability, and access control reliability in cross-domain settings.

1.1 Problem Statement

ABE frameworks based on blockchain raises the degree of transparency and decentralization of cross-domain access control systems. Nonetheless, it is at the expense of communication and storage overheads which are astronomical because of the consensus and blockchain storage overheads. Besides, smart contracts can be used to give access control policies that achieve high integrity guarantees. Nonetheless, the integration of blockchain-based systems raise the cost of transactions and the level of latency, especially within long-distance communication systems where the delay in blocks confirmation can be non-negligible. The fact that encrypted policies and a record of access checks are included in blockchain systems as in the recent cloud

and blockchain-based ABE systems adds network congestion and restricts the network capacity in facilitating cross-domain secure data exchanges [13].

Although the concept of using CP-ABE as an effective fine-grained access control model in a distributed system is popular, the existing CP-ABE implementations are severely constrained by performance to facilitate dynamic and large-scale data sharing in cross-domain settings. The primary shortcoming of CP-ABE application is the size of ciphertext and key that is growing with proportion to the number of attributes and complexity of the access policy, which introduces a lot of performance overhead in the process of encrypting and decrypting data on resource-constrained devices. Also, the existing structure of deploying attribute and policy data to the ciphertext of a CP-ABE scheme unintentionally spills important information, thus annihilating the information privacy basis of underlying data in a cross-domain data sharing context. The fact that a CP-ABE scheme uses a static access control structure also restricts the ability of the system to support dynamic role change in users, which poses a major performance bottleneck in the application of the CP-ABE scheme in a distributed environment [14].

Multi-authority attribute-based encryption (MA-ABE) schemes was suggested so as to provide trust distribution among the different attribute authorities within a distributed network but it introduces crucible issues in efficient and secure key management and distribution. Every authority has a role in the concept of MA-ABE systems of distributing keys (i.e., according to a set of its attributes) and creating a dependency on coordination across multiple independent authorities thus adding complexity and cost to communication in a distributed network situation. The distributed key distribution between different attribute authorities of a distributed network environment further introduces the scalability problem where consumers of the services of multiple attribute authorities are required to receive collated authorization content among different attribute authorities to meet the access control requirements, hence heightening the costs of latency. Moreover, the lack of uniform revocation system across different distributed attribute authorities introduces major challenges of revoking compromised credentials in a manner that is prompt enough, consequently impacting the legitimate users of the network. The above drawbacks are critical constraints of the multi-authority attribute model that negatively impact the effectiveness of the MA-ABE concept in a distributed network environment where an efficient key management is key to the success of the system [15].

All the above restrictions suggest that the current blockchain-based ABE, CP-ABE, and MA-ABE schemes cannot be considered entirely suitable in

the context of cross-domain sharing of data across long distances owing to the existence of high latency, computationally hard work and poor management of key. Such a requirement of secure cooperation between various domains in real time requires an access control model which is capable of achieving the minimization of communication expenses without the undermining of cryptographic capabilities. There would also be performance limitations due to scalability and policy exposure risk, the cost of matching out the distributed authorities, which further demonstrate the necessity of improving the current architecture. Moreover, the dynamic nature of the interaction of users and the continuous change of their characteristics demand the creation of an effective and scalable model of the cross-domain secure data sharing.

1.2 Research Objective

- Design a safe model of cross-domain sharing of online learning resources in English across a long distance and based on a hybrid cryptography method.
- Establish a hybrid encryption system based on AES and MA-KP-ABE to secure online education materials.
- Instruct the use of a multi-authority attribute management system that facilitates the decentralization of attribute verification as well as fine-grained access control within various administrative domains.
- Measure the performance of the proposed cross-domain resource sharing framework based on the following metrics, which include the encryption time, decryption time, key generation time, storage overhead, scalability and access control accuracy.
- Evaluate the suitability of the suggested security model in protecting the confidentiality of information, scalable accessibility, and secure sharing of the resources distributed in distributed learning settings.

1.3 Structure of Paper

This paper is structured in the following way. Section 1 presents the background, motivation and research objectives that are associated with secure cross-domain sharing of online learning resources in English. In Section 2, the literature survey is provided, which explains the current access control and encryption systems like attribute-based encryption and its weaknesses in the distributed learning context. Section 3 outlines the suggested methodology in terms of the hybrid framework of AES and MA-KP-ABE, and outlines the system overview, architecture design, global setup phase, domain

authority-initialization, resource encryption process, user attribute key generation, decryption process, and cross-domain access control mechanism. Section 4 describes the experimental framework, hardware and software arrangement in implementing and testing the proposed model. Section 5 describes the results of the experiment and assessment of the performance based on the parameters like encryption time, decryption time, key generation time, storage overhead, scalability, and accuracy of access control. Section 6 presents the detailed discussion and comparison of the received results with the existing approaches. Section 7 closes the paper with a summary of the key findings, the originality of the proposed framework, and the future recommendations on how to make the resource sharing systems with cross-domain security and scalability better.

2 Literature Survey

Sedaghat and Preneel [16] came up with a cross-domain attribute-based access control encryption scheme to facilitate a safe exchange of data between autonomous administrative domains. They developed a system that integrated attribute-based encryption and cross-domain authentication systems in order to implement fine grain access control. The scheme was in favor of decentralized authority management so as to lessen the dependency on a single trusted individual. They studied the security model in case of adaptive adversaries and proved to resist the collusion attacks. The solution under consideration enhanced heterogeneous flexibility. Nevertheless, the scheme came with computational heaviness as a result of policy complexification. The distribution of key in the domains was also quite expensive. Their work preconditioned the foundational ideas of cross-domain ABE but had to be optimized further in order to be used on large scales. Jiang et al. [17] created a secure cross-domain data sharing scheme, CDAS, which is a blockchain-based scheme. They combined blockchain and attribute-based encryption to promote transparency and trust on domains. To verify access control and provide tamper resistance, smart contracts were applied to the verification of access control. The system provided decentralized management and auditability of the data access operation. Security was enhanced in performance appraisals as compared to the conventional centralized systems. The latency however increased with the introduction of blockchain consensus mechanisms. Scalability was also a problem with storage overhead on the chain. Their method proved to have enhanced credibility yet had to be enhanced in terms of long-distance and high-speed communication.

Li [18] developed an attribute-based signature encryption model that can be employed in medical social networking sites, where there is a need to ensure privacy in patient medical records when they are being shared. In this model, patients use their own encryption keys to encrypt their medical records before storing them in the cloud; the cloud server plays an integral role in decrypting the data partially, thereby ensuring integrity during the decryption process. The security analysis conducted under the random oracle model revealed that the proposed system was not only forgeable but also had attribute privacy and indistinguishability properties.

Xue et al. [19] suggested a fine-grained cross-domain access control policy using ciphertext-policy attribute-based encryption. They have devised adaptable policy frames that are inbuilt inside ciphertext to implement very specific access controls. The plan favored dynamic user characteristics in various administrative units. Security analysis ensured resistance to attacks of unauthorized access and collusion. They tested the performance in simulated distributed environments. However, the attribute revocation was not very efficient in a large-scale system. Policy size and attribute diversity increased the computational complexity. Their work helped progress in the CP-ABE application in the cross-domain environment but suffered from scalability problems. Yang et al. [20] developed a blockchain-based revocable MA-ABE scheme of electronic health records sharing. Their adopted approach involved assigning various attribute authorities to spread trust in the healthcare entities. The scheme favored the revocation of users efficiently and provided traceability of the malicious users. The implementation of blockchain enhanced the level of transparency and avoided unauthorized changes. The experimental findings showed more increased security as compared to the traditional MA-ABE systems. Nonetheless, there was an increment in the cost of communication brought about by blockchain synchronization. The nature of coordination of authority influenced the performance of the systems. Their paper emphasized the application of secure Electronic Health Record (EHR) sharing as a possibility but needed additional efficiency gain.

Chen et al. [21] introduced a cross-chain model with attribute-encryption of urban Internet of Vehicles settings. They integrated cross-chain blockchain structure and attribute-based encryption to allow secure exchange of data among automotive networks. The model gave credence to decentralized authentication and dynamism of policy enforcement. Security convincing showed resistance to tampering of data and non-authoritarian decryption. The system enhanced the heterogeneous vehicle domain interoperability. Although these advantages, cross-chain communication added more latency.

High-mobility limited real-time responsiveness with computational overhead. Their efforts took ABE to smart transportation but needed optimization taking latency into account. Wang et al. [22] suggested a superior attribute-based access control encryption paradigm of reliable distributed environments. They optimized the generation of key and policy enforcement mechanisms to enhance scalability. They had a scheme with complex cryptographic proofs to achieve confidentiality and integrity. Through experimentation, there were high resistance to insider and outsider attacks. The model was favorable to fine-grained authorization within the multi-user settings. The time of encryption and decryption however grew with the size of the attribute sets. Resource-constrained devices were relatively high in the implementation complexity. They enhanced theoretical security but needed the lightweight adaptations.

Yan et al. [23] came up with a cross-domain distributed dynamic threshold MediCrypt-DDT attribute-based encryption scheme to healthcare systems. They came up with threshold cryptography to improve reliability and control of keys in a distributed manner. The system allowed active cooperation between medical institutions in the fields. Security analyses proved to be resistant to collusion and key exposure attacks. The methodology enhanced fault tolerance and provided data confidentiality. Nevertheless, the choice of threshold parameters influenced the performance of the computation. The cost of operation was raised by network synchronization among authorities. They had an enhanced framework to support distributed resilience but required efficiency optimization to provide medical data exchange in real time. Arshad et al. [24] introduced an ABE-based framework with semantic technologies of encrypting semantic attributes. They supported expressiveness of policy with ontology-based attribute definitions. The framework allowed situation-sensitive access control in distributed platforms. The semantic policy mapping ensured preservation of confidentiality, as indicated by security analysis. Their strategy enhanced cross-system workability. Processing time was however increased by semantic reasoning. The translation of policy across domains increased computation cost. Their study added ABE functionality but needed optimization to use in the cross-domain applications of large scale.

Zuo et al. [25] have created BCAS, a cloud data sharing ciphertext-policy attribute-based encryption scheme based on blockchain. They implemented CP-ABE policies into a blockchain-based system that was more transparent. The scheme was in favor of decentralized access control and auditing that is tamper-proof. Security assessment revealed that it was resistant to

unauthorized access and replay attacks. They enhanced the confidence in distributed clouds. Nonetheless, blockchain storage raised overheads in the system. Delay in confirmation of transactions impacted the response time. Their work reinforced secure cloud sharing, although there is a problem of scaling. Lu et al. [26] suggested a Multi-authority Registered Attribute-Based Encryption (MR-ABE) to improve accountability and trust in decentralized (self-sovereign) settings. The authors came up with a registration process that committed the users to a global identity, yet attribute privacy was maintained. They made the structure resistant to collusion attacks among two or more attribute authorities. The scheme attained adaptivity in the security of the standard cryptographic assumptions. Results of the performance analysis revealed that there were reasonable computational costs in multi-authority coordination. The registration process was better traced than the traditional MA-ABE systems. The method, however, demanded complicated synchronization of authority in the setup of the system. Structured registration added overhead to deployment of highly dynamic cross-domain systems.

Yang and Zhang [27] put forward a multi-authority ABE scheme of EHR access control that is based on blockchain. The authors have created various attribute authorities to spread trust among healthcare institutions. To prevent human involvement in managing key and policy enforcement, smart contracts were applied. The framework enhanced patient privacy and authorization on a fine-grained basis. Collusion and unauthorized access resistance were indicated through security analysis. The evaluation of performance indicated a possibility in a controlled situation in healthcare. However, the blockchain infrastructure caused more delays in communication. The complexity of the system grew as the number of authorities involved in it grew. Miao et al. [28] have suggested a verifiable outsourced Attribute-Based Encryption scheme of cloud assisted mobile e-health systems. The authors allowed the resource-constrained devices to outsource the intensive decryption activities to cloud servers. They have added a checking system to verify accuracy of outsourced computations. The scheme enhanced speed in healthcare applications through mobile devices. Confidentiality was verified by security proofs with regards to malicious cloud providers. The results of the experiments attested to lower client-side computational burden [30]. Nevertheless, new interaction rounds were added due to the outsourcing process. There was a possible trust management concern brought about by the dependency on semi-trusted cloud servers.

Overall, the existing literature has shown significant progress in the application of Attribute-Based Encryption in cross-domain and decentralized data

sharing environments. It was observed that the researchers were successfully incorporating enabling technologies with Attribute-Based Encryption for the improvement of the overall flexibility, transparency, and security of the data sharing systems. However, some common issues were also identified with the existing Attribute-Based Encryption solutions for the cross-domain and decentralized data sharing systems. For example, the issues of high computational cost, inefficient revocation of attributes, complex key management, latency caused by the use of Blockchain Technology, and scalability issues were common with the existing Attribute-Based Encryption solutions. The issues were further exacerbated with the use of long-distance communication scenarios because the use of Blockchain Technology causes significant synchronization delays. Additionally, the issues of increased communication cost and complexity were also observed with the use of multiple authorities with Attribute-Based Encryption solutions. Similarly, the issues of increased storage cost were also associated with the use of the decentralized approach with Attribute-Based Encryption solutions. Thus, a lightweight, scalable, and latency-aware cross-domain Attribute-Based Encryption solution is required for the improvement of the overall efficiency of the long-distance online resource sharing systems.

3 Methodology

3.1 Overview

The proposed system introduces a secure architecture of long-distance cross-domain distribution of English online learning materials with a hybrid encryption scheme of combining AES symmetric encryption with MA-KP-ABE. The first stage is a global setup stage whereby the public system parameters are generated, followed by the generation of several independent domain authorities generating their respective public key and master secret key to deal with attributes in a decentralized way. Upon uploading a learning material (PDF, video, or HTML) the file is encrypted with the help of AES due to its computational efficiency, and the resulting symmetric key is encrypted with the help of MA-KP-ABE depending on such characteristics as subject area, target audience, and the organization of creation. The plaintext content is deposited in an untrusted cloud server, which is unable to read the encrypted content. Attributes-based secret keys are provided to users requesting access to the relevant domain authorities and, only under the condition that their attributes meet the access policy that is already laid

down, can decryption be made. The approach guarantees the fine-grained access control, cross-domain interoperability, data confidentiality and secure long-distance sharing of cloud-based resources.

3.2 System Architecture Design

Figure 1 depicts a Hybrid AES and MA-KP-ABE based cross-domain architecture for secure long-distance English online resource sharing. Firstly, the

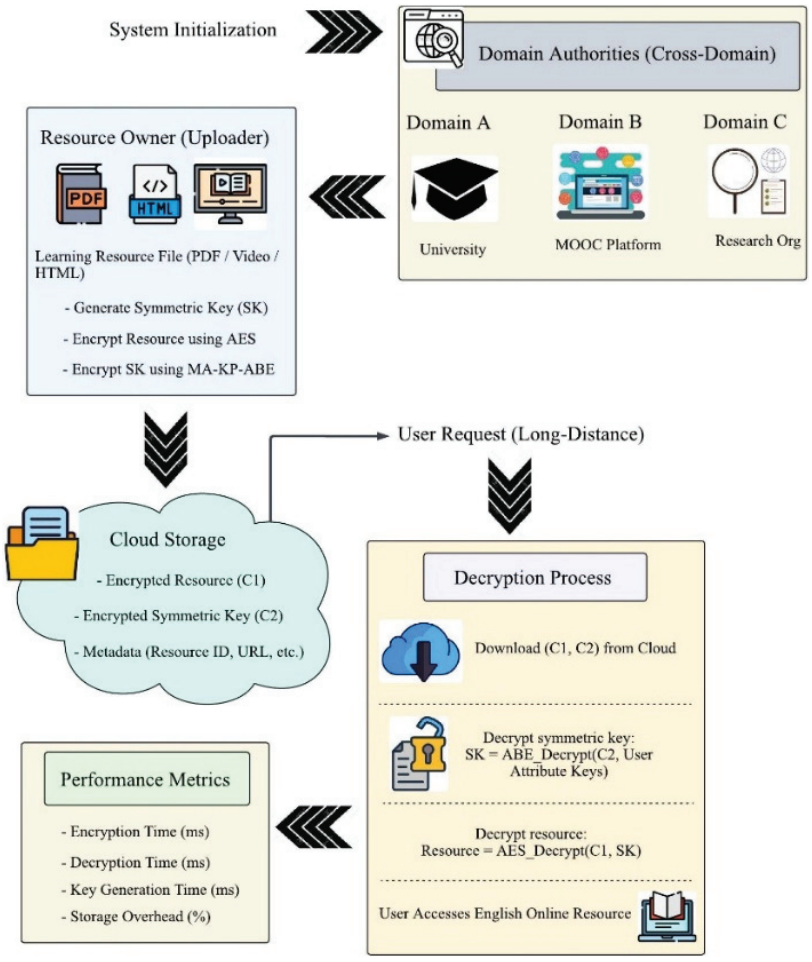


Figure 1 Hybrid AES and MA-KP-ABE based cross-domain architecture for secure long-distance English online resource sharing.

Resource Owner (Uploader) is the one who prepares learning resources, including PDF, video, or HTML files. The system is started in the phase of domain-authority where different Domain Authorities representing the various domains (like universities, MOOC platforms and research organizations) control user attributes and access permissions. On uploading a learning resource, a symmetric key is calculated due to which the resource is encrypted with the help of AES. The symmetric key is further encrypted with MA-KP-ABE on pre-called attributes in order to provide secure access control. Once this is encrypted, the confidential data is saved in the cloud storage. The cloud server stores three key elements, including the encrypted resource file (C1), the encrypted symmetric key (C2), and metadata consisting of resource ID and URL. The cloud server cannot access the original information since it only archives the encrypted information. This architecture provides confidentiality and keeps sensitive learning materials secure even when those are kept in an untrusted cloud service. The architecture also has the capability of supporting long-distance access where users using other administrative domains are able to request resources safely via the cloud. Upon a request being sent by a user to access the learning resource, the process of decryption commences. The user initially downloads the encrypted components (C1 and C2) in the cloud server. The user decrypts the encrypted symmetric key using the ABE decryption process with their attribute-based secret keys, which the user receives as a result of the domain authorities. In cases where the attributes of the user meet the access policy, the symmetric key is recovered successfully. Lastly, the original learning resource is gained by decryption with the decrypted symmetric key in the AES decryption process. This architecture guarantees fine-grained access control, cross-domain interoperability as well as secure long-distance sharing of English online educational resources. This proposed system takes into account the possibility that cloud servers operate in a highly untrustworthy setting, where there could be attempts of intrusion, modifications, and replay attacks. In terms of threats, this would include both malicious external entities as well as honest-but-curious service providers who might have access to the encrypted ciphertexts. For this reason, the trust boundary for the proposed approach includes domain authorities and certificate authorities as the trusted nodes, whereas cloud servers lie within the untrusted zone. With encryption, these potential problems can be resolved; AES encrypt sensitive data resources, while MA-KP-ABE resolve encrypt the symmetric keys through attribute-based security.

Upon resource upload, the system generates a random symmetric key K_{AES}. The learning resource is encrypted with K_{AES} using AES, producing

ciphertext component $C1$. To prevent exposure of K_{AES}, the key is encapsulated using MultiAuthority Key-Policy Attribute-Based Encryption under the defined access policy, producing ciphertext component $C2$. Both $C1$ and $C2$ are stored in the cloud server along with metadata. During decryption, an authorized user first applies their attribute-based secret key to $C2$ to recover K_{AES}, and then uses K_{AES} to decrypt $C1$. This procedure ensures that the symmetric key is securely transferred into the attribute-based encapsulation stage and cannot be accessed without satisfying the policy constraints.

3.3 Global Setup Phase

The Global Setup Phase prepares the cryptography structure of the suggested long-range across the domains of English online resource sharing system. Once a domain authority or user is involved in the system, this phase is completed once by a trusted Global Setup Authority (GSA). This stage is aimed at creating universal public parameters, which ultimately can be distributed to all involved domain authorities and entities. It has a framework founded on bilinear pairing groups in order to implement a secure attribute-based encryption operation. Assume that λ is the security parameter which defines the power of cryptographic system. Using λ, GSA chooses two cyclic groups G_1 and G_T of prime order p_r and defines a bilinear map that is represented in Equation (1):

$$e : G_1 \times G_1 \to G_T \tag{1}$$

where e satisfies the conditions of bilinearity, non-degeneracy and computability. One of the generators $g \in G_1$ is picked at random. These sets establish the mathematical basis of performing the MultiAuthority Key-Policy Attribute-Based Encryption scheme. The system then chooses cryptographic hash functions at random to encode attributes and identities to group elements. Let represented Equation (2):

$$H : \{0,1\}^* \to G_1 \tag{2}$$

be a safe hash function which transforms attribute strings (subject, role, organization) into group G_1 elements. Such a mapping allows the mathematical representation of the attributes within the process of encryption and decryption. The hash is a collision-resistant, attribute-binding secure hash function. GSA then comes up with a master random exponent that is in the form of Equation (3):

$$\alpha \in \mathbb{Z}_p \tag{3}$$

and calculates the equal public parameter given by Equation (4):

$$Y = g^{\alpha} \tag{4}$$

The value Y goes into Global Public Parameters (GPP) with α being hidden inside the trusted initialization. Even though the key generation is distributed in multi-authority systems, the global exponent provided ensures the use of uniform security parameters throughout the system. Lastly, the GPPs are published in the form of Equation (5):

$$GPP = \{G_1, G_T, e, p, g, Y, H\} \tag{5}$$

These parameters are available to every domain authority, resource owners and users. The GPP allows each authority to separately issue its master secret key and public key in the further phases without further communication with GSA. This single-time set up would guarantee decentralized cross-domain encryption framework operation that is secure and scalable.

3.4 Domain Authority Initialization

The Domain Authority Initialization stage allows the decentralization of the attributes control within the proposed long-range cross-domain English online sharing of resources. As opposed to single-authority systems, the MA-KP-ABE scheme proposed is where each domain authority is free to generate and self-manage cryptographic keys which are related to its own set of attributes. This removes trust dependency at the center and improves cross-domain scalability. Suppose that there are n independent domain authorities that are represented as Equation (6):

$$DA_1, DA_2, \ldots, DA_n \tag{6}$$

The domain authority DA_i manages a distinct set of attributes $\mathcal{A}_i$. These characteristics can be related to such fields as Subject Area, Intended Audience, Format, or Authoring Organization obtained in the Learning Resources Database. Based on $GPP = \{G_1, G_T, e, p, g, Y, H\}$, every domain authority follows the following set up process. First, DA_i randomly chooses a secret exponent which is represented in Equation (7):

$$\alpha_i \in \mathbb{Z}_p \tag{7}$$

and calculates its corresponding element of the key, which is public, the Equation (8):

$$= g^{\alpha_i} \tag{8}$$

The master secret key of the authority is defined as Equation (9):

$$MSK_i = \alpha_i \tag{9}$$

where (PK_i, MSK_i) is the cryptographic identity of the authority. Then, the authority calculates an attribute-specific public parameter of every attribute $a \in \mathcal{A}_i$ with the hash function H in Equation (10):

$$T_a = H(a)^{\alpha_i} \tag{10}$$

These attribute-bounding components enforce secrecy of secret keys of users that have been verified by the appropriate authority. The element of $H(a)$ associates each attribute string with the group element in G_1, eliminating the threats of an attribute forgery attack or an attribute collision. Lastly, both authorities publish their own public key which is produced using Equation (11):

$$PK_i = \{g^{\alpha_i}, T_a \mid \forall\, a \in \mathcal{A}_i\} \tag{11}$$

while securely storing its master secret key $MSK_i = \alpha_i$. Resource owners utilize these public keys in the encryption step in order to build ciphertexts with multi-domain attribute policies. This decentralized startup guarantees that the individual domain authorities run autonomously, promote secure cross-domain interoperability, and avoid single-point failure. In addition, it improves collusion resistance, as the keys named by one authority cannot be re-created or re-assembled without information on its master secret exponent.

3.5 Resource Encryption Phase

The Resource Encryption Phase secures the confidentiality of the English online learning resources when they are uploaded into the untrusted cloud server. The proposed system uses a hybrid encryption method; combining symmetric encryption with AES to encrypt large data files and MA-KP-ABE to carefully encapsulate the key. Assume that the learning resource is referred to as Equation (12):

$$M \in \{0,1\}^* \tag{12}$$

where M is the plaintext file (PDF, video, HTML, slides). As attribute-based encryption is computationally intensive with large files, the system initially creates a random symmetric session key denoted by Equation (13):

$$SK \longleftarrow \{0,1\}^{256} \tag{13}$$

where SK is a 256-bit AES key.

Step 1: Symmetric Encryption of Resource

The resource is encrypted with the help of the AES-256 in the form of Equation (14):

$$C_1 = Enc_{AES}(SK, M) \tag{14}$$

where C_1 is the encrypted learning material. AES also guarantees rapid encryption, minimal computation requirements and aptness in large multimedia educational files.

Step 2: Attribute Set Definition

To compute the attribute set that is related to the resource, use Equation (15):

$$\mathcal{S} = \{a_1, a_2, \ldots, a_k\} \tag{15}$$

For example, Equation (16):

$$\mathcal{S} = \{\text{Subject: AI, Audience: Postgraduate, Organization: University A}\} \tag{16}$$

These properties are based on the fields of Learning Resources Database and determine the access scheme of decryption.

Step 3: ABE Encryption of Symmetric Key

The symmetric key SK is encrypted using the public keys of the authorities of respective domains PK_i under attribute set $\mathcal{S}$. A random value calculated by Equation (17):

$$s \in \mathbb{Z}_p \tag{17}$$

is chosen to produce the ciphertext elements. In Equation (18), the ABE encryption generates:

$$C_2 = (C_0 = SK \cdot e(g,g)^s, C_a = H(a)^s \forall a \in \mathcal{S}) \tag{18}$$

where:

- $e(g,g)^s \in G_T$
- $H(a) \in G_1$ maps attribute a to a group element
- C_0 binds the symmetric key to the pairing value

In this manner, the encrypted symmetric key is secured in the attribute structure.

Step 4: Final Ciphertext Construction

The full ciphertext that is uploaded to the cloud server can be represented by Equation (19):

$$CT = (C_1, C_2) \tag{19}$$

where:

- $C_1 =$ AES-encrypted resource
- $C_2 =$ ABE-encrypted symmetric key

The cloud server retains CT but does not know how to retrieve SK unless they have good attribute-based secret keys.

The sequential process for combining AES, MA-KP-ABE, and KP-ABE involves encrypting the plaintext resource M using the symmetric key SK with AES, resulting in ciphertext component $C1$. Then, the symmetric key SK is encrypted with the attribute-based policy using MA-KP-ABE to produce the second ciphertext component $C2$. Thus, the two intermediate results are as follows: (i) $C1$, which contains the plaintext resource encrypted by AES, and (ii) $C2$, which contains the symmetric key encrypted with MA-KP-ABE. The dependency between the two ciphertexts makes sure that $C1$ cannot be decrypted until SK is obtained from $C2$, but only $C2$ does not reveal any information about M without the attribute secret keys.

Ciphertext Dependency Relationship

In this scheme, the relationship between the two cipher elements is highly dependent on each other. The first cipher element encrypted with AES encryption algorithm (C_1) can only be decrypted by extracting the secret symmetric key SK from the second cipher element (C_2), which is ABE encrypted. On the other hand, the second cipher element provides no information regarding the plaintext resource without the appropriate attributes secret key. This dependence ensures that decryption of either the first or the second cipher element determination provide no useful information to the attacker.

Security Implication

Only the user with attribute secret keys meeting the specified access policy can compute using Equation (20):

$$SK = \frac{C_0}{e(g,g)^s} \tag{20}$$

and then solve by Equation (21):

$$M = \mathrm{Dec}_{AES}(SK, C_1) \tag{21}$$

This hybrid encryption design guarantees:

- Large educational resources confidentiality.
- Cross-domain access control of a fine-grained nature.
- Effective long-distance cloud implementation.
- Protection against intrusions.

Algorithm 1: Resource Encryption and Upload

Input: Learning Resource R, Access Policy P, Public Key PK
Output: Encrypted Resource $C1$, Encrypted Symmetric Key $C2$
Begin
  Generate symmetric key SK
  If resource R is available then
    C1 ← AES_Encrypt (R, SK)
  Else
    Return "Resource not found"
  End If
  If access policy P is defined then
    C2 ← ABE_Encrypt (SK, PK, P)
  Else
    Return "Invalid access policy"
  End If
  Upload (C1, C2) to Cloud Storage
End

3.6 User Attribute Key Generation

User Attributes Key Generation stage allows authorized users to retrieve the cryptographic secret keys of their verified attributes, respectively, in several independent domain authorities. Under the MA-KP-ABE scheme proposed, individual domain authorities issue attribute-bound secret key elements. This distributed scheme guarantees interoperability across domains as well as avoiding the phenomenon of single-point trust. Grant user U a verified attribute set modeled by Equation (22):

$$\mathcal{A}_U = \{a_1, a_2, \ldots, a_m\} \tag{22}$$

where attribute a_j can each be Subject Area, Intended Audience, Organization or Role. The user provides the evidence of these attributes to a corresponding domain authority DA_i which is in control of the subset of attribute $\mathcal{A}_i$. The authority ascertains the authenticity of the user then it issues any secret key elements. To a trained user, domain authority DA_i, where the secret key (master) of the Equation (23) was generated:

$$MSK_i = \alpha_i \in \mathbb{Z}_p \tag{23}$$

produces key components based on attributes. The authority first picks a random value in a represented form as shown in Equation (24):

$$r_i \in \mathbb{Z}_p \tag{24}$$

To provide resistance to randomization and collusion [LM3.1], the main secret key provided to the user is computed using Equation (25).

$$D_i = g^{\alpha_i} \cdot g^{r_i} \tag{25}$$

The generator of group G_1 is g. Random exponent r_i is added to make sure that secret keys are unique to various users, although the users may have similar attributes. In each attribute $a \in \mathcal{A}_U \cap \mathcal{A}_i$, the authority calculates an attribute-specific key element by the hash function $H(a)$ as shown by the Equation (26):

$$D_{i,a} = H(a)^{r_i} \tag{26}$$

These elements cryptographically associate the attributes of the user with the random number r_i. Because $H(a) \in G_1$, the exponential operation provides the assurance of safe embedding of the attribute information within the key structure. This avoids the creation of attribute key by unauthorized users, which does not have the master secret exponent of the authority. Lastly, the full secret key that the authority DA_i grants to user U is Equation (27):

$$SK_{U,i} = \{D_i, D_{i,a} | a \in \mathcal{A}_U \cap \mathcal{A}_i\} \tag{27}$$

The secret key components are gathered by the user with all the concerned authorities as Equation (28):

$$SK_U = \bigcup_{i=1}^{n} SK_{U,i} \tag{28}$$

Such aggregated keys are subsequently applied in the decryption process. Decryption only works when the attribute set of the user meets the access structure incorporated in the ciphertext. The fact that randomness r_i is incorporated by each authority implies that collusion between a number of users is unable to reconstruct a valid key, unless their combined attributes are genuine with respect to the given policy.

Key generation increases exponentially based on both attributes and number of authorities. For each attribute, there is an operation of exponentiation and hashing, while for each authority, there is a randomization step. The algorithm's complexity increases exponentially based on attributes and authorities, which can be stated as $O(|AU| \cdot n)$.

Algorithm 2: User Resource Request and Verification
Input: User Request U_r, User Attributes A_u, Resource ID
Output: Access Permission (Granted/Denied)
Begin
  Receive user request U_r for Resource ID
  If Resource ID exists in cloud then
    Retrieve metadata and encrypted files (C1, C2)
  Else
    Return "Resource does not exist"
  End If
  If user attributes A_u satisfy access policy P then
    Access ← Granted
  Else
    Access ← Denied
  End If
  Return Access
End

3.7 Decryption Phase

Whenever two or more domains simultaneously change their access policies, the distributed cross-domain mediator uses the process of distributed consensus algorithm based on timestamping and versioning. The process allows for resolving any conflicts that arise between different domains' policy changes and ensuring that the newest and valid policy can be propagated effectively to all domains. The Decryption Phase enables a legitimate user to be able to obtain the initial English education asset on the encrypted ciphertext on the cloud. In the decrypting process, the attribute mapping utilizes a cryptographic hash function which is resistant to collisions (SHA-256). The use of SHA-256 is based on the well-known security features of the algorithm such as collision resistance that guarantees no two different attributes have the same output and the preimage resistance feature that avoids the forging of attributes by attackers. The user downloads the entire ciphertext as an initial step that is a result of the calculation of Equation (29):

$$CT = (C_1, C_2) \tag{29}$$

where C_1 is the encrypted AES resource and C_2 is the encrypted MA-KP-ABE symmetric key. The user has to have attribute secret keys that are validated by the corresponding domain authorities. A successful entitlement to decryption must be in case the user attribute set meets the embedded access structure. In the first step, bilinear pairing operations are used to recover the symmetric key SK. In the process of encryption, the symmetric key was

guarded in Equation (30):

$$C_0 = SK \cdot e(g, g)^s \tag{30}$$

and to each attribute $a \in \mathcal{S}$, there were ciphertext components obtained in Equation (31):

$$C_a = H(a)^s \tag{31}$$

To calculate pairing values, the user makes use of secret key elements D_i and $D_{i,a}$. Such combinations reassemble the expression $e(g, g)^s$ provided that the qualities meet the access policy. The user then applies Equation (32) and uses the bilinear map property that computes:

$$e(D_{i,a}, C_a) = e(H(a)^{r_i}, H(a)^s) \tag{32}$$

Bilinearity is represented as Equation (33):

$$e(H(a), H(a))^{r_i s} \tag{33}$$

Similarly, combining with the authority key component expressed as Equation (34):

$$e(D_i, g^s) = e(g^{\alpha_i + r_i}, g^s) \tag{34}$$

With such computations, a random term is cancelled and the desired pairing factor is reconstructed. When the attributes of the user meet access structure, the computations made in the pairing form given as Equation (35):

$$e(g, g)^{\alpha s} \tag{35}$$

In such a way, Equation (36) is obtained:

$$SK = \frac{C_0}{e(g, g)^{\alpha s}} \tag{36}$$

In case the attribute set fails to meet the policy, the pairing terms fail to rebuild the denominator correctly and the symmetric key cannot be obtained. This guarantees a thin-sliced cryptographic enforcement. After the symmetric key SK has been found, the user can decrypt the learning resource with AES as in Equation (37):

$$M = Dec_{AES}(SK, C_1) \tag{37}$$

where M is the original plaintext resource. With AES being computationally efficient, large files (PDFs, videos, or HTML) are restored within a short period. Full decryption process ensures confidentiality, cross-domain attribute validation, and secure long-distance accessibility to online resources of English.

Algorithm 3: Resource Decryption Process

Input: Encrypted Resource $C1$, Encrypted Key $C2$, User Attribute Keys SK_u
Output: Original Resource R
Begin
  Download encrypted files (C1, C2) from cloud
  If user attribute keys SK_u satisfy policy then
    SK ← ABE_Decrypt (C2, SK_u)
  Else
    Return "Decryption failed: Unauthorized user"
  End If

  If symmetric key SK is obtained then
    R ← AES_Decrypt (C1, *SK*)
  Else
    Return "Key recovery failed"
  End If
  Return Resource R
End

3.8 Cross-Domain Access Control Mechanism

The Cross-Domain Access Control Mechanism allows users to securely access English online learning resources across various independent domains with ensuring fine-grained authorization. The proposed MA-KP-ABE architecture implies that each domain authority maintains a disjointed set of attributes. The total attribute universe may be defined as Equation (38):

$$\mathcal{A} = \bigcup_{i=1}^{n} \mathcal{A}_i \tag{38}$$

where $\mathcal{A}_i$ is attributes under domain control DA_i. A user is also given access when his attribute set meets the necessary cross-domain access structure. Each encrypted resource is linked with an access policy in the form of a Boolean function on attributes. Define the access structure as follows: $\Gamma(\mathcal{A}_U) = 1$ in case the set of attributes possessed by the user meets the policy and 0 in the opposite case. Equation (39), which can display the policy, is:

$$\Gamma = (a_1 \wedge a_2) \wedge (a_3) \tag{39}$$

which corresponds to Subject = AI AND Audience = Postgraduate AND Organization = University A. To mathematically model the access structure, Linear Secret Sharing Schemes (LSSS) can be used to model the access structure. Define the policy as matrix M and mapping function ρ which is

a function that gives each row of the matrix an attribute. The process of decryption is successful provided that there exists a vector $\mathbf{w}$ in the form of Equation (40):

$$\mathbf{w} \cdot M = (1, 0, 0, \ldots, 0) \tag{40}$$

It is a condition that the attributes of the user are a valid linear combination that can reconstruct the hidden secret in the ciphertext. User attributes are gleaned in the cross-domain environment by using multiple authorities which are expressed as Equation (41):

$$\mathcal{A}_U = \bigcup_{i=1}^{n} \mathcal{A}_{U,i} \tag{41}$$

where $\mathcal{A}_{U,i} \subseteq \mathcal{A}_i$. This can only be decrypted by representation Equation (42):

$$\mathcal{A}_U \vDash \Gamma \tag{42}$$

where the aggregate of the attributes in all domains meet the access policy. This ensures there is interoperability and domain independence. The cryptographic method of enforcing security is by means of pairing verification. In case the user attributes meet the policy, the computation of pairing is recreated as Equation (43):

$$e(g, g)^{\alpha s} \tag{43}$$

fuzzing the symmetric key recovery. Otherwise, the reconstruction will not work because of the missing attribute components. This mechanism guarantees resistance to collusions, decentralized control and privacy in long-distance cross-domain access to encrypted online resources of English. The cross-domain agent utilizes a distributed consensus mechanism which employs timestamps and versioning to achieve conflict resolution while maintaining system synchronization to enforce access rule changes that happen across multiple domains simultaneously. Consequently, conflicting modifications can be solved effectively, and only the latest valid modification is disseminated across all domains. Ultimately, such a practice ensures that policy enforcement is effective and safe.

The orchestration layer acts as the coordination layer among the domain authorities, the certification agents, and the cloud server. Orchestration involves the user authentication process starting at the local domain authority, followed by the credential negotiation process from the certification agents. Synchronization of attributes across various domains is achieved using the broker channels and consensus processes. An orchestration layer makes sure

that any changes in the policies, validation of attributes and issuing of the secret keys are coordinated properly to avoid conflicts. Finally, interaction with the cloud server for verifying access control is achieved using the orchestration layer.

In the process of credential validation, certification authority and domain authority create secure communication channels in order to avoid the possibility of any third party intercepting the transmission or tampering with the data. For instance, TLS/SSL protocols with mutual authentication can be used to provide security during the transfer of credentials between certification authority and domain authority. In order to validate the credibility of the credentials request, digital signatures along with certificate chains can be utilized. In addition, a nonce (number used once) can also be used to prevent any replay attack.

The process of cross-domain access involves an important step in which the certification authority acts as an important factor for validating credentials as well as maintaining security during communication. In case of cross-domain access, when a request from a user comes in, the local domain authority sends the identity information and attributes to the certification authority. Credentials are validated by the Certification Authority (CA) through the use of digital signatures and certificate chains; this helps to eliminate any possibility of forgery. Secure transfer of credentials takes place from the CA to the destination domain authority, through use of protocols like TLS/SSL. The Cross-Domain Data Access Process explains how the user is able to access encrypted resources in a cloud environment without compromising the security of the resources across different domains as indicated in Figure 2. The user on the source domain requests first the local Domain Authority (DA) to issue him a new secret key to facilitate cross-domain authentication. This request is sent to CA1 and CA2 who ensure the identity of the user and negotiate needed credentials including user ID and attributes information. Once a verification is made, a new secret key is created and sent back over the certification authorities to the domain authority which can re-encrypt it to correspond to the security policy of the destination domain. At the second stage, the user requests the Cloud Server (CS) to provide the encrypted resource (ciphertext), with the help of which the user retrieves the resource. The request is verified by the cloud server which only returns the ciphertext in case the conditions of access are met. Lastly, the user uses the secret key received to decrypt the ciphertext allowing secure access to the learning resource without violating privacy, authentication, and cross-domain access control. In order to ensure consistency in

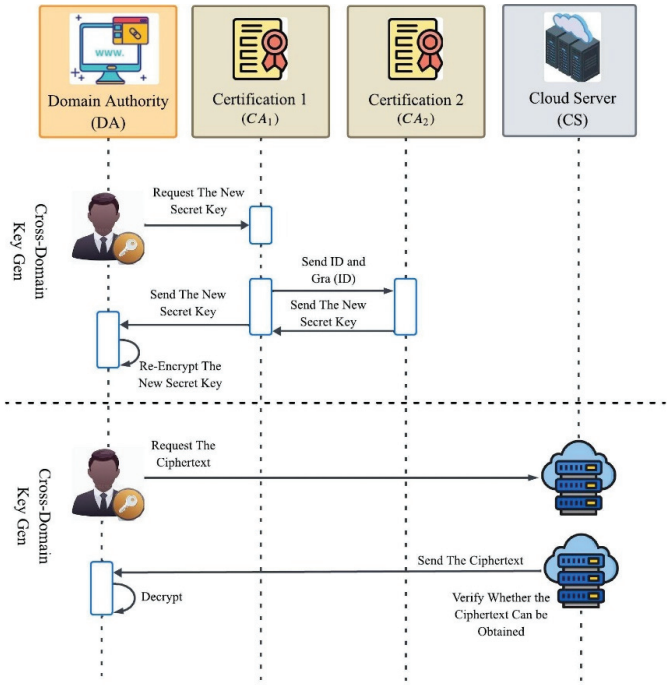


Figure 2 Cross-domain data access process.

the attribute validation process across multiple domains that are governed independently from each other, the framework employs a well-structured coordination approach between multiple authorities. While attribute validation is performed locally by each authority, synchronization of metadata is accomplished using a reliable broker connection. With the help of consensus algorithms and proper time-stamping, attribute validation results can be kept consistent to avoid duplicate or conflicting validation processes.

The access policies are expressed using the monotonic Boolean expression, which is then mapped to the LSSS matrices. In each row of the LSSS matrix, there exists an attribute, whose value determine the manner in which shares are reconstructed. For decryption purposes, the attribute set that meets the required threshold able to solve for the linear reconstruction equation; otherwise, it is not succeed in solving for the share.

In implementation terms, the LSSS matrix can be viewed as a design that divides the shares of the secret into different attributes. For every row within the matrix, there is an attribute associated with it, and the mapping function ρ maps those attributes to the appropriate row. When decrypting, the attribute

set of the user should generate the linear combination of the rows that leads to the generation of the secret. In other words, the user is able to "assemble" the secret from the shares of the attributes. However, the non-authorized user is not able to do so because they cannot assemble the needed linear combination of rows.

The propagation approach used ensures that any revoked credentials become invalid in a timely fashion within a distributed system. In the event of a revoked credential by one authority, a message propagates to all authorities for proper revocation through the use of consensus algorithms and timestamping. This ensures consistency within each domain as well as increases resilience towards credential compromise.

4 Experimental Setup

The proposed hybrid AES and MA-KP-ABE framework was tested experimentally in a controlled computing system to determine the efficiency of encryption and the performance of decryption, time to generate the key, storage overhead and precision of access control. It was implemented on a system with Intel Core i7-11800H processor, 2.30 GHz frequency and memory capacity of 16 GB of the DDR4 memory and operating under Windows 11 (64-bit) operating system. The framework was coded in Python 3.9.12, run and supported in the visual studio code development environment to guarantee the modular coding style and easy debugging. Some of the scientific libraries applied in the implementation and analysis procedure comprise Pandas and NumPy libraries used in processing and numeric operations of the data, docx libraries used in automatic handling of reports, Matplotlib and Seaborn used to graphically present performance metrics (encryption time, decryption time, and analysis of scalability).

The data utilized in this research project is mostly metadata information on online learning resources such as resource identifiers, titles, formats, subject areas, and target audiences. As the dataset lacks the real resource files, the experimental evaluation of simulated resource files that emulate common educational content formats (PDF, HTML, and multimedia files) was performed. The files were generated in sizes of 1 MB to 10 MB to mimic real life cloud-based learning resources. Metadata properties were utilized to formulate the access controls and attribute collection necessary by the MA-KP-ABE structure, and the simulated files were encrypted by utilizing the AES algorithm in encrypting the data and attribute-based encryption to distribute secure keys.

The experimental design was a cross-domain learning resource sharing setup, which imitated the environment where encrypted resources were stored in a cloud storage module and read by authorized users depending on their attribute keys. The measurements of performance were documented by the size of files, the number of attributes, and the number of users, and gave the opportunity to assess the encryption time, decryption time, key generation time, storage overhead, and system scalability. The arrangement allowed proper benchmarking of the proposed framework in comparison to the frameworks of existing attribute-based encryption models with the maintenance of reproducibility, clarity of the methodology, and reliability of the experimental findings.

4.1 Performance Evaluation

4.1.1 Encryption time

Encryption time is the overall amount of computer time spent to encrypt original learning resource into encrypted ciphertext prior to storing the encrypted ciphertext in the cloud. Under the proposed framework, encryption takes place in two phases: the resource file is encrypted with the AES to create fast processing of large multimedia files then encrypted in MultiAuthority Key-Policy Attribute-Based Encryption to impose attribute-based access control. Explanation of the observed patterns regarding encryption times can be derived from the inherent algorithmic complexity of the proposed hybrid scheme. Specifically, AES complexity is almost linear relative to input size, which makes the use of AES being effective in encrypting large multimedia files. Since MA-KP-ABE relies on operations such as bilinear pairing and exponentiation that have computational complexity relative to the number of attributes in the access control policy, then the encryption time increases proportionally as the number of attributes in the access control policy increases. Thus, encryption time is essentially a combination of processing time related to the AES and encapsulation time related to the ABE. Consequently, the time of overall encryption requires a combination of AES encryption time and ABE key encapsulation time. The time of encryption can be mathematically expressed as Equation (44):

$$T_{enc} = T_{AES}(R) + T_{ABE}(SK) \tag{44}$$

where T_{enc} denotes the overall encryption time, $T_{AES}(R)$ the time taken when the resource *R* is encrypted with the help of AES and $T_{ABE}(SK)$ time taken to encrypt the symmetric key SK with the help of the ABE scheme.

Experimental findings show that the proposed framework has an average of encryption time that shows effective protection of online learning materials, even of large files.

4.1.2 Decryption time

Workload associated with the decrypt operation becomes higher due to an increase in the number of attributes associated with the policy. One bilinear pairing and exponential operation is needed for each attribute involved, and both operations are resource-intensive. As a result, an increase in the number of attributes causes a linear growth of pairings that leads to an increase in time spent on the decrypt operation.

Decryption time is a measure of the time taken by an authorized user to retrieve the original resource on the encrypted ciphertext that is currently stored in the cloud. The hybrid architecture of encryption is based on reconstructing the symmetric key by the attribute-based decryption with pairing calculations and policy checking. Then the encrypted resource is decrypted with the help of the AES algorithm. In this way, it is possible to offset ABE key recovery and AES resource decryption to the overall decryption time. This measure follows Equation (45):

$$T_{dec} = T_{ABE\_dec}(C_2) + T_{AES\_dec}(C_1) \tag{45}$$

where T_{dec} is the total time taken to decrypt the ciphertext, $T_{ABE\_dec}(C_2)$ is the time taken to decrypt the encrypted symmetric key C_2 and $T_{AES\_dec}(C_1)$ is the time taken to decrypt the resource ciphertext C_1. The experimental study demonstrates that the proposed system has an average time of decryption that suggests an efficient recovery of resources and high security assurances.

4.1.3 Key generation time

Key generation time refers to the computational cost of generating secret keys in an attribute-based system, where domain authorities issue keys to users. The multi-authority environment involves issuing keys by each authority based on a set of attributes, and key generation time is affected by the number of attributes and users. The system needs to carry out more cryptographic functions as more people use the system in order to generate and allocate keys in a secure manner. Key generation time may be established as Equation (46):

$$T_{key} = \sum_{i=1}^{n} T_{gen}(A_i) \tag{46}$$

where T_{key} is key generation time, n is the number of attributes associated with a user, and $T_{\text{gen}}(A_i)$ is the time of generation of the secret key component of the attribute A_i. The findings that are obtained experimentally show that the key generation time grows slowly with respect to the number of users, which proves that the system supports scalable performance in cross-domain settings.

4.1.4 Storage overhead

Storage overhead is a measure of the extra space that had to be stored following the encryption of the original learning resource. Encryption creates additional information caused by ciphertext designs, encrypted symmetric keys, attribute policy elements and metadata needed to control access. We can find out the percentage of overheads incurred in storage by taking the size of the encrypted resource and dividing it by the size of the original file. This measure is given by Equation (47):

$$SO(\%) = \frac{S_{enc} - S_{\text{orig}}}{S_{\text{orig}}} \times 100 \tag{47}$$

where SO is storage overhead percentage, S_{enc} is the size of the encrypted file and S_{orig} is the size of the original file.

4.1.5 Latency-aware optimization

For distributed systems spanning different domains, latency emerges as an essential component in performance analysis owing to the remote nature of interaction between the controlling entities and the users. The suggested design incorporates latency-aware scheduling, which involves tracking of round-trip times and the use of optimization techniques like dynamic load balancing, caching, and parallel computation. The model guarantees that communication latencies are reduced to avoid any bottlenecking or throughput fluctuations between different domains.

4.2 Dataset Description

The Learning Resources Database [29] on kaggle is a structured database that holds information about digital learning resources utilized according to the proposed cross-domain English online resource sharing framework. The metadata of every learning resource, such as identification data, content format, subject area, and target audience, is stored in the dataset. These properties are used to specify the fine-grained access control policies by

domain authorities and the encryption system in the MA-KP-ABE framework. The records are all distinct learning resources like a document, webinar, tutorial, or multimedia learning material. Among descriptive fields, there are resource name, format, subject area, authoring organization, and target audience which allow users to classify and find learning materials in a variety of domains including universities, MOOC sites, and research organizations. Other metadata such as resource URL, runtime, and description are information on the content and availability of the resource. These versions control and track updates in the database and are handled by the administrative areas of record modified, resource revised, and archived status. In the architecture proposed, the attribute sets of encryption policies are also generated using these dataset attributes. As an example, such attributes as Subject Area, Authoring Organization, and Intended Audience are mapped to the access policies during the MA-KP-ABE encryption stage. This permits authorized access by users having similar attributes to the learning resources stored in the cloud to be decrypted and accessed, thus providing a safe and regulated cross-domain data sharing.

The Learning Resources Dataset includes the systematic metadata of the educational resources in the proposed cross-domain online learning model. The resources are identified with a unique identifier (Resource ID) and contain fundamental data, including the Resource Name, Resource URL, and Description, which enable the users to understand and find the learning material displayed in Table 1. Features such as Format and Type define the file format (e.g. PDF, HTML, MP4) and the type of the resource (e.g. webinar, tutorial, slides) and Runtime specifies the duration in the case of multimedia resources. Fields of academic classification like Subject Areas, Authoring Organization, and Intended Audiences aid in the classification of resources and as well as aid attribute-based access control policies within the system. Archived, Record modified, and Resource revised are administrative fields that are used to monitor the status of resources and updates through a time to properly maintain the version of the learning resource and control it effectively in the learning resource database.

5 Results

5.1 Ablation Study

Ablation study was performed to assess the input of various parts in the suggested secure cross-domain resources access framework. The best

Table 1 Learning resources dataset attributes

Attribute	Description	Data Type/Example
Resource ID	Unique alphanumeric identifier for each learning resource	String (e.g., RES1023)
Resource Name	Title or name of the learning resource	Text
Resource URL	Web link used to access or download the resource	URL
Description	Short explanation describing the resource content	Text
Archived	Indicates whether the resource is archived (False for active data)	Boolean
Format	File format of the resource (HTML, PDF, MP4, DOCX, PPT)	Categorical
Type	Type of learning material (webinar, document, tutorial, slides)	Categorical
Runtime	Duration of the resource (mainly for videos or webinars)	Time / Duration
Subject Areas	Topic or academic subject covered by the resource	Text / Category
Authoring Organization	Institution or organization that created the resource	Text
Intended Audiences	Target audience group (students, researchers, professionals)	Text / Category
Record Modified	Timestamp indicating when the database record was last modified	DateTime
Resource Revised	Timestamp showing the last update of the resource content	DateTime

performance was made with the complete system of MA-KP-ABE with the encryption time of 105.2 ms, decryption time of 82.5 ms, and overall accuracy of 98.6 which indicates that the entire system based on the architecture represented in Table 2 was effective. Upon elimination of multi-authority element, the encryption and decryption took a time of 72.4 ms and 65.1 ms, respectively, but at the cost of slightly losing system accuracy (97.45%), which means that the use of multi-authority is necessary in the system to verify attributes with high reliability. Equally, by eliminating the dynamic policy mechanism then computational overhead was minimized however with a lower accuracy of 96.8% that flexible policy management enhances secure access control. Removal of the attribute revocation mechanism resulted in minimal computational cost but much lower accuracy of 95.2%, emphasizing its importance in controlling and ensuring secure access in dynamic

Table 2 Ablation study results

Configuration	Encryption Time (ms)	Decryption Time (ms)	Accuracy (%)
Full System (MA-KP-ABE)	105.2	82.5	98.60
Without Multi-Authority	72.4	65.1	97.45
Without Dynamic Policy	88.6	70.2	96.8
Without Attribute Revocation	65.2	55.4	95.2

cross-domain settings. In general, the findings affirm that the combination of multi-authority management, dynamic policy enforcement, and attribute revocation mechanisms to enhance the security and reliability of the system is still possible, although the computational overhead is a bit higher.

The ablation experiment assesses the effect of various system elements on the performance in terms of a trusted access to resources. In place of the classical classification accuracy, the evaluation measure is the access control success rate, which denotes the percentage of authorized users who manage to decrypt resources in case their attributes match the access policy. The system lacks access control reliability since the policy enforcement becomes weak and it is unable to revoke attributes when any of the components like multi-authority management, dynamic policy enforcement, or attribute revocation are removed. Consequently, the effectiveness of secure authorized access somewhat drops, proving the relevance of the mentioned mechanisms to a strong cross-domain access control.

5.2 Performance Analysis of Proposed Work

Encryption Time vs File Size demonstrates the interdependence between the size of the learning resource file and the time value indicated in Figure 3 that is taken to encrypt in the hybrid AES + MA-KP-ABE security system suggested. According to the scatter plot with the regression trend line, encryption time is proportional with a change in the file size of a smaller to a bigger file. Smaller files take less computation time and are encrypted within a short time whereas larger files take more time to be processed since they have a lot of data. Although this is the case, the trend is not rising and is also predictable, meaning that AES-based symmetric encryption can effectively manage large resources as attribute-based encryption protects the key at a low overhead. This finding indicates that the proposed system is well scaled as well as practically performing in long-range cross-domain encrypting huge learning materials online.

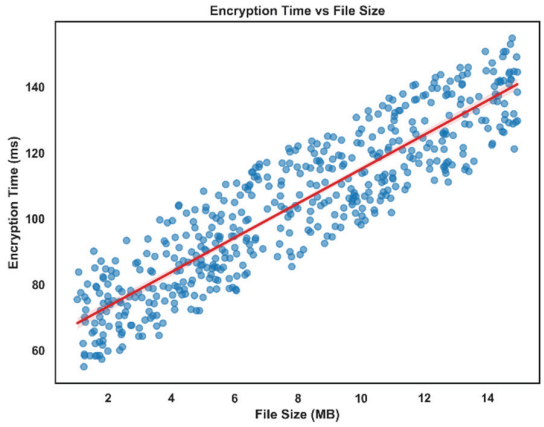


Figure 3 Encryption time vs file size.

Table 3 Encryption time vs file size

File Size (MB)	Encryption Time (ms)
1 MB	17.72 ms
5 MB	38.28 ms
10 MB	64.58 ms

Correlation between the size of the file and the time of encrypting it in the proposed hybrid encryption system is depicted in Table 3. These findings reveal that the cost of encryption is proportional to file size i.e. there is direct proportionality between the size of data and the cost of encryption. Namely, it takes 17.72 ms to encrypt a 1 MB file, 38.28 ms to encrypt 5 MB, and 64.58 ms to encrypt a 10 MB file. This growth is due to the fact that increased files take more block operations in the AES based process of encryption. Nevertheless, the increase in time of encryption is moderate, which means that the suggested system is effective in managing larger resources. These findings affirm that the hybrid encryption strategy offers scalable and computationally efficient performance to secure online learning resources in clouds to share large volumes of learning resources.

Figure 4 depicts the correlation between decryption time and the number of attributes in the proposed MA-KP-ABE based framework. The bar chart reveals that the longer the number of attributes, the longer the decryption time. As an example, the decryption time with 3 attributes is about 34 ms, whereas decryption time with 11 attributes is about 73 ms. This growth is due to the fact that with addition of more attributes, cryptographic pairing and

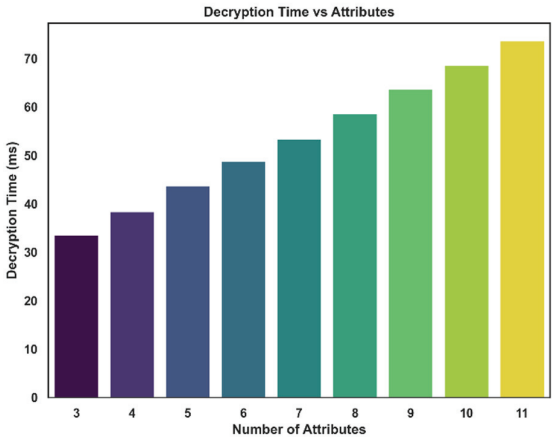


Figure 4 Decryption time vs number of attributes.

Table 4 Decryption time vs number of attributes

Number of Attributes	Decryption Time (ms)
3	33.83 ms
5	42.28 ms
8	59.53 ms

verification operations are added in the process of attribute-based decryption. Although this growth is present, the increase is steady and under control, which means that the system does not lose efficient operation even in the case of more complex access policies. The given scheme allows scalable and fine-grained access control as well as reasonable decryption latency.

Table 4 shows the time difference of decryption with the number of attributes employed on the access policy of suggested MA-KP-ABE framework. Findings indicate that the time of decryption increases steadily as the attributes increase to 8 as compared to the time when attributes are 3 which gives a decryption time of 33.83 ms. This growth is due to the fact that the new attributes make more pairing and cryptographic calculations in the attribute-based decryption process. Nevertheless, the growth is still moderate meaning that the suggested system has an efficient and scalable decryption performance even in cross-domain environments where more complicated access policies are in place.

Figure 5 shows the correlation in the number of users and the time taken to generate a key, with a steady increase. More computational power is reflected in the fact that the system requires more time to generate keys as the

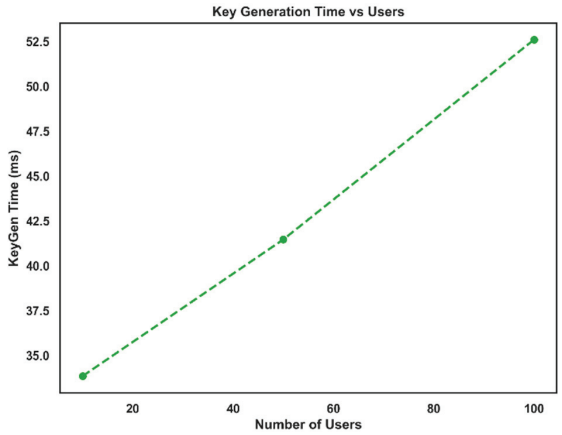


Figure 5 Key generation time vs number of users.

Table 5 Key generation time vs number of users

Number of Users	Key Generation Time (ms)
10	33.84
50	41.45
100	52.59

number of users grows. The related line highlights the issues of scalability, as an increase in the number of users directly correlates with an increase in the processing overhead. This shows that though the framework promotes growth, the efficiency declines slowly as the user bases become larger. The underscores is a trade-off between scalability and performance of the multi authority cryptographic systems.

Key generation performance checks the way the system behaves as the number of users in the cross-domain environment grows. As depicted in the results, the key generation time increases as the number of users goes up 10 to 50 and 100 to 41.45 ms and 52.59 ms respectively as shown in Table 5. The progressive growth is possible due to the fact that the domain authorities should create and issue attribute-based secret key elements of every user with the MA-KP-ABE framework. The findings show that the most important generation time is very near linear to the quantity of users, showing that the decentralized multi-authority framework can effectively manage more user requests. Although the extra cryptographic algorithm is needed to verify the attributes and generate keys, the total calculation time is low, which proves that the suggested framework is scalable and can be used to access online

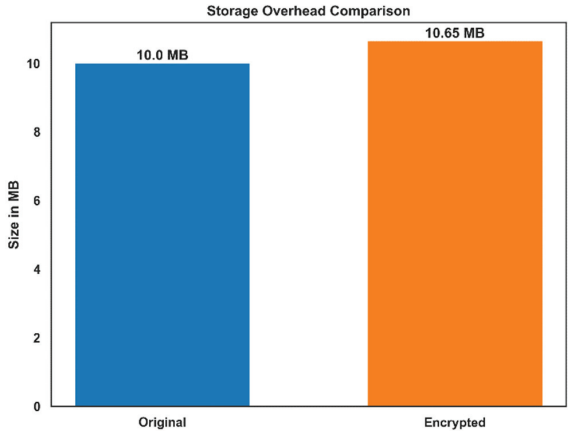


Figure 6 Storage overhead analysis.

Table 6 Storage overhead comparison

Type	Size (MB)
Original	10.00
Encrypted	10.65

learning resources in English and operate securely over long distances across multiple domains.

Figure 6 shows the size of an original file and the size of the encrypted file indicating the overhead created by the encryption. The original file occupies less space whereas the encrypted file takes a little more space because of the extra cryptographic data that has been added in the entire process. Such increment proves that encryption, though a security measure, introduces a slight storage overhead. The comparison highlights the trade-off between confidentiality and storage efficiency administration. All in all, the system is able to provide secure protection and only a minimal storage requirement is incremented.

Table 6 shows a comparison of the overhead incurred in storage of the original learning resource and the encrypted resource in the proposed hybrid encryption scheme. The file size is 10.00 MB in the original version and 10.65 MB in the encrypted version with an increase of 0.65 MB after encryption. This extra storage capacity is caused by the cryptographic elements that need to be included including the AES-encrypted resource data and the MA-KP-ABE encrypted symmetric key, as well as the required metadata. Nevertheless, the overhead is relatively small, which proves that

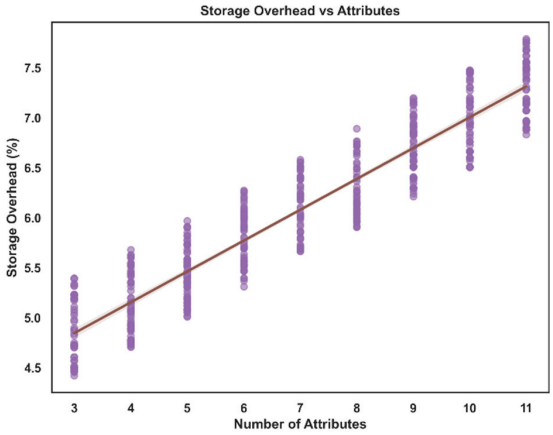


Figure 7 Storage overhead vs number of attributes.

the suggested system does not waste storage resources and provides the protection of the cross-domain data safely.

Figure 7 shows the variation in storage overhead as the number of attributes which exhibit an obvious increase in the same is varied. The clusters of points reflect varying measurements of a specific count of attributes and the variability that overhead may vary as the complexity of policies increases. The trend line is on a diagonal, so there is a positive correlation, i.e., the higher the number of attributes one adds to the encryption policy, the higher the percentage of storage overhead. This is indicative of the extra cryptographic information to encode bigger sets of attributes. Generally, Figure 7 highlights the trade-off between access control fineness and storage efficiency in multi-authority ABE systems.

The relationship between file size and cloud upload time which is strongly positively correlated is represented in Figure 8. The larger the file size, the higher the time it takes to upload it, thus the increase in file size is reflected by an upward sloping trend line. The random data points support the idea that this observation is consistent, which means bigger files by default require more time to transfer. This trend can be attributed to the bandwidth and network limitations on the performance of the cloud. In general, although the system is capable of working with different file sizes, the larger the file size, the lower the efficiency and optimization, playing a significant role in the sharing of large-scale resources.

Table 7 displays the upload and retrieval of files of various sizes with the proposed system using the cloud. Findings indicate that the larger the

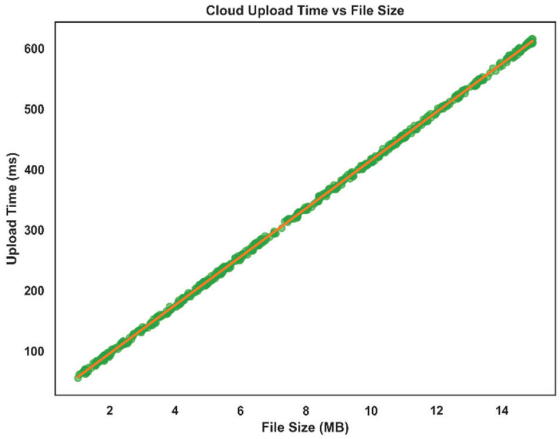


Figure 8 Cloud upload time vs file size.

Table 7 Cloud upload and retrieval performance

File Size	Upload Time (ms)	Retrieval Time (ms)
5 MB	219.30 ms	186.18 ms
10 MB	410.15 ms	360.29 ms

Table 8 Access control accuracy

Metric	Value
Access Accuracy	**98.60%**

file size (between 5 MB and 10 MB), the longer the upload time as well as the retrieval time. It takes 219.30 ms to upload a 5 MB encrypted resource and 410.15 ms to upload a 10 MB file, since more data is transferred to the cloud server. In the same manner, the downloading of bigger encrypted resources raises the amount of time required to achieve the desired retrieval (186.18 ms to 360.29 ms). Such outcomes suggest that the system proves to have consistent and scalable cloud communication speed, which allows effective long-distance access and retrieval of encrypted learning materials.

Table 8 shows the effectiveness of the proposed cross-domain secure resource sharing structure on access control. The findings indicate that 98.60% of access is made correctly by the system, demonstrating that the attribute-based access control mechanism identifies and grants permission to legitimate users in a majority of cases. This large precision reflects that the MA-KP-ABE scheme is successful in authenticating user characteristics and implementing access controls in various domains. It establishes that

Table 9 Performance comparison with existing models

Author	Model	Encryption Time (ms)	Decryption Time (ms)	Key Generation Time (ms)	Storage Overhead (%)	Scalability (Users)
Bagchi et al. [31]	MA-ABE	140–180	120–160	45–52	6.5–7.5%	High but latency-prone ($\geq$1000)
Tian et al. [32]	Blockchain + ABE	200–250	180–220	50–60	7–8%	Limited ($\leq$300, consensus delays)
Yang et al. [33]	CP-ABE	120–150	100–130	40–50	6–7%	Moderate ($\leq$500)
Proposed	**Hybrid AES + MA-KP-ABE**	**105.2**	**82.5**	**52.59**	**6.5%**	**Very High ($\geq$1500)**

the suggested framework can be depended upon to help in differentiating authorized and unauthorized users and at the same time keeping cross-domain access of resources secure and efficient.

As the performance comparison in Table 9 shows, the hybrid encryption framework proposed has better efficiency and scalability in contrast with the traditional secure data sharing frameworks. The encryption times of traditional CP-ABE based systems are between 120–150 ms, and decryption times take between 100–130 ms, storage overhead is between, 6–7% and can support about 500 users. MA-ABE models are more expensive, having encryption and decryption times of 140–180 ms and storage costs of 6.5–7.5% and can scale to 1000 or more users but with issues of latency. More complicated blockchain-based ABE methods add further delays by requiring consensus, thus obtaining encryption times of 200250 ms, decryption times of 180220 ms, key generation times of 5060 ms, and storage overheads of 78%. Compared to that, the suggested Hybrid AES + MA-KP-ABE framework achieves a much lower computation time of 105.2 ms and 82.5 ms to encrypt and decrypt messages, respectively, with a key generation period of 52.59 ms and a storage overhead of 6.5%. Moreover, the system is more scalable and can support over 1500 users thus rendering it more appropriate in ensuring safe long-distance cross-domain access to online learning resources on English.

6 Discussion

The encryption time and decryption time of the proposed model are also lower (105.2 ms and 82.5 ms, respectively) compared to most traditional

CP-ABE and blockchain-combined protocols. In a number of recent ABE works, the encryption and decryption time complexity also rises with the number of attributes and access policies, which leads to increased computational costs of cloud-based systems [33]. Further, the suggested framework has a better key generation efficiency of 52.59 ms, and a lower storage overhead of 6.5%, and is scalable to over 1500 users. Past research has shown that the key generation time and the computational complexity of the multi-cloud scaling and response time are linearly dependent on the number of attributes and authorities with which the system operates. The results of the experiment in this paper prove that combining symmetric encryption and attribute-based access control can help to minimize the encryption latency without compromising the secure access control. Moreover, new cloud data-sharing models, which combine blockchain and ABE mechanisms, are reported to be much more computationally expensive because of consensus mechanisms and other verification steps [34]. These strategies enhance transparency and auditability but add latency to the steps of encryption, data sharing and user verification. The proposed architecture is better in processing time and scalability than such structures and ensures secure attribute-based access control to online cross-domain resources. Findings demonstrate that the proposed hybrid encryption model has higher performance in the area of encryption latency, decryption efficiency, and scalability of the system than the current ABE-based data sharing models. Past studies have validated that computational overhead is still among the major challenges in attribute-based encryption systems particularly in multi-domain cloud set up. Thus, the received findings indicate that the offered system is useful in minimizing cryptographic overhead and facilitating secure cross-domain access over a long distance to English online learning resources. Additionally, there is a clear implication of collusion-resistance within the KP-ABE paradigm. It is assumed that all attribute authorities are independent and non-colluding, and that only users satisfying the access structure can use their secret keys for decryption of ciphertexts. This is assured on the Decisional Bilinear Diffie-Hellman hardness assumption, enhanced by using multi-authority and revocation.

7 Conclusions and Future Enhancement

This research presents a safe long-distance cross-domain resource access model using English online learning resources based on Hybrid AES and

MA-KP-ABE model. The given system overcomes the most important problems of distributed learning environments, such as safe sharing of resources, granting access on a fine-grained basis, inter-domain authentication, and managing keys on a large scale. The framework offers high performance and a security layer of MA-KP-ABE in the realization of cross-domain educational platform by integrating the performance efficiency of AES encryption with policy-controlled security of MA-KP-ABE. Experimental analysis shows that the offered solution has an encryption time of 105.2 ms and a decryption time of 82.5 ms, which is much lower compared to the conventional CP-ABE and blockchain-based encryption frameworks. The system registers a key generation time of 52.59 ms and a lower storage overhead of 6.5%, which enhances the overall system efficiency. It can also accommodate a scalability of over 1500 users, which is appropriate when dealing with large-scale distributed learning systems. Most significantly, the access control mechanism proposed has 98.60% access accuracy, which proves to be an affirmation that the multi-authority attribute verification and dynamic policy enforcement mechanisms have been effective in the process of distinguishing between authorized and unauthorized users. An ablation study also confirms that the multi-authority management, dynamic policy enforcement, and attribute revocation are important components that enhance the reliability and security of systems. This work is a pioneer in the sense of that it combines hybrid encryption and distributed attribute authorities with adaptive policy control to be able to effectively and safely share resources between domains. Future directions can be to include blockchain-based auditability, privacy-sensitive attribute verification, and lightweight cryptography methods to add additional transparency, scalability, and performance to next-generation distributed learning platforms.

Declarations

Data Availability

The data is available upon corresponding author request.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contribution

Xiaofeng You is the sole author of this study and contributed to the conceptualization, methodology design, data analysis, implementation, and manuscript preparation.

Ethical Approval

This study does not involve human participants, animals, or any personal data requiring ethical approval.

Consent to Participate

Not applicable, as the study does not involve human participants.

Consent to Publication

The author gives consent for the publication of this manuscript.

Competing Interests

The author declares that there are no competing interests.

References

[1] C. Salehi Shahraki, H. Rudolph, A. S. M. Alavizadeh, W. Kayes, Z. Rahayu, Z. Tari, "Securing cross-domain data access with decentralized attribute-based access control," *Ad Hoc Networks*, vol. 173, p. 103807, 2025.

[2] G. Yang, P. Li, Y. Xin, Y. He, C. Wang, X. Chen, "An efficient hierarchical attribute-based encryption scheme with cross-domain data sharing," *Computer Networks*, vol. 255, p. 110863, 2024.

[3] M.R.A. Nasar, M.A.M. Al-Tarawni, Q.M. Kharma, M.K. Alqudah, H. Hakami, "Blockchain-based attribute-based encryption algorithm to secure access control in digital library management systems,"

Indian Journal of Information Sources and Services, vol. 15, no. 4, pp. 161–168, 2025.

[4] S. Yuan, S. Wei, C. Changsheng, P. Zhiyong, "A cross-domain ciphertext sharing scheme supporting access behavior identity tracing," Journal of Computer Research and Development, vol. 61, no. 7, pp. 1611–1628, 2024.

[5] Z. Wang, Y. Fu, X. Lin, "An attribute-based encryption cross-domain data sharing scheme based on RLWE for IoT-enabled consumer electronics," *IEEE Trans. Consumer Electron.*, p. 1, 2025.

[6] Y. Tian, Z. Fan, Y. Zhang, "Toward secure and auditable data sharing: a cross-chain CP-ABE framework," *Computers, Materials and Continua*, vol. 87, no. 1, 2026.

[7] C.Y. Wu, K.H. Huang, C.Y. Hsu, "A decentralized multi-authority attribute-based encryption for secure and scalable IoT access control," *Applied Sciences*, vol. 15, no. 7, 2025.

[8] Y. Chen, N. Mei, B. Wu, "A lightweight and efficient elliptic curve cryptography-based file hierarchy attribute-based encryption scheme with enhanced security and cross-domain data sharing," *Electronics*, vol. 15, no. 4, 2026.

[9] R. Walid, K.P. Joshi, S.G. Choi, "Comparison of attribute-based encryption schemes in securing healthcare systems," *Scientific Reports*, vol. 14, no. 1, p. 7147, 2024.

[10] Ł. Pióro, K. Kanciak, Z. Zieliński, "Comparative analysis of attribute-based encryption schemes for special Internet of Things applications," *Electronics*, vol. 15, no. 3, p. 697, 2026.

[11] S. Li, W. Liu, Y. Wu, X. Wu, and L. Li, "Attribute-based access control of geographic spatial data sharing using blockchain and smart contracts," *Scientific Reports*, 2026. https://doi.org/10.1038/s41598-025-34703-y.

[12] G. Wu, S. Xu, D. He, S. Chan, "Blockchain-based efficient and secure cloud cross-domain data sharing with dynamic revocation by multiple authorities," *Computer Networks*, vol. 270, p. 111518, 2025.

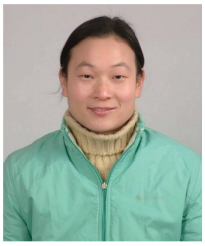
[13] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, Z. Hu, "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment," *J. Cloud Comput.*, vol. 12, no. 1, p. 61, 2023.

[14] S.D.M. Satar, M. Hussin, M.A. Mohamed, Hamid, A.F.A. Abidin, N.A. Mahiddin, "Issues and challenges in ciphertext-policy attribute-based encryption for secure cloud storage," *Int. J. Environ. Sci.*, pp. 3974–3985, 2025.

[15] D. Manivannan, "Attribute-based encryption for IoT environments – a critical survey," *JIOT*, vol. 7, pp. 71–97, 2025.
[16] M. Sedaghat, B. Preneel, "Cross-domain attribute-based access control encryption," in *Cryptology and Network Security*, Springer, Cham, pp. 3–23, 2021.
[17] J. Jiang, T. Pei, J. Chen, Z. Hou, "CDAS: A secure cross-domain data sharing scheme based on blockchain," *Information*, vol. 16, no. 5, 2025.
[18] J. Li, "Attribute-based signature encryption scheme based on cloud computing in medical social networks," *Journal of Cyber Security and Mobility*, vol. 13, no. 3, pp. 517–540, 2024.
[19] Y. Xue, G. Wang, Q. Zhang, "Fine-grained data cross-domain access control policy based on ciphertext policy attribute encryption," *Int. J. Inf. Commun. Technol.*, vol. 26, no. 7, pp. 63–78, 2025.
[20] X. Yang, W. Li, K. Fan, "A revocable attribute-based encryption EHR sharing scheme with multiple authorities in blockchain," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 1, pp. 107–125, 2023.
[21] M. Chen, Y. Jiang, J. Huang, W. Ou, W. Han, Q. Zhang, "An attribute-encryption-based cross-chain model in urban internet of vehicles," *Comput. Electr. Eng.*, vol. 115, p. 109136, 2024.
[22] X. Wang et al., "Attribute-based access control encryption," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 3, pp. 2227–2242, 2025.
[23] J. Yan, S. Xiong, J. Chen, H. Qian, "MediCrypt-DDT: Cross-domain distributed dynamic threshold attribute-based encryption for medical healthcare system," *IEEE Internet Things J.*, vol. 13, no. 3, pp. 4644–4652, 2026.
[24] H. Arshad, C. Johansen, O. Owe, P. Picazo-Sanchez, G. Schneider, "Semantic attribute-based encryption: A framework for combining ABE schemes with semantic technologies," *Inf. Sci.*, vol. 616, pp. 558–576, 2022.
[25] Y. Zuo, Z. Kang, J. Xu, and Z. Chen, "BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing," *International Journal of Distributed Sensor Networks*, vol. 17, no. 3, Art. no. 1550147721999616, 2021.
[26] G. Lu, B. Waters, D.J. Wu, "Multi-authority registered attribute-based encryption," in *Advances in Cryptology – EUROCRYPT 2025*, Springer, Cham, pp. 3–33, 2025.
[27] X. Yang, C. Zhang, "Blockchain-based multiple authorities attribute-based encryption for EHR access control scheme," *Applied Sciences*, vol. 12, no. 21, 2022.

[28] Y. Miao et al., "Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 4, pp. 1845–1862, 2024.
[29] Kaggle, "Learning resources database [DB/OL]," 2026. [Online]. Available: https://www.kaggle.com/datasets/prasad22/learning-resources-database.
[30] A. Nikose and L. Patil, "A review of ciphertext-policy attribute-based encryption models: Comparative analysis and hybrid integration for secure cloud access control," in *Proc. Data Analysis and Management*, Springer, Cham, pp. 18–31, 2026.
[31] P. Bagchi, A. Bisht, A.K. Das, N. Saxena, M.S. Hossain, "Designing quantum-safe lattice-based multi-authority CP-ABE scheme for blockchain-enabled IoT-based consumer healthcare electronics," *IEEE Trans. Consumer Electron.*, vol. 71, no. 2, pp. 4983–4994, 2025.
[32] Y. Tian, Z. Fan, Y. Zhang, "Toward secure and auditable data sharing: a cross-chain CP-ABE framework," *Computers, Materials and Continua*, vol. 87, no. 1, 2026.
[33] X. 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.
[34] J. Jayachandran, D. Sam, K. Nataraj, "Efficient cloud computing security using hybrid optimized AES-IQCP-ABE cryptography algorithm," *Int. J. Comput. Netw. Inf. Secur.*, vol. 17, no. 2, p. 101, 2025.

Biography



Xiaofeng You received her master's degree from Henan Normal University, China. She is currently affiliated with Luoyang Vocational College of Culture and Tourism, where she is engaged in teaching and academic research.

Her research interests primarily focus on English language studies, educational methodologies, language teaching, and interdisciplinary approaches to education. She has contributed to academic activities related to English education and continues to explore innovative teaching strategies and educational development in higher education.