OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

A Novel Approach for improving the Multiauthority Ciphertext-Policy for Blockchain Based Digital Rights Management Scheme

Dr. Sunil Kumar R M[1], Dr. Mrutyunjaya M S[2] ,Dr. Karthik B U[3], Dr. Murthy D H R[4]

[1.]*Associate professor, Department of CSE, R L Jalappa Institute of Technology.*
[2.]*Associate professor, Department of CSE (Data Science), R L Jalappa Institute of Technology.*
[3.]*Assistant professor, Department of CSE (Data Science), R L Jalappa Institute of Technology.*
[4.]*Associate professor, Department of CSE (Cyber Security), R L Jalappa Institute of Technology.*

Abstract: ***Blockchain based system for managing digital rights that would safeguard the privacy of digital contents, improves the fairness of transactions in digital copyright, and they free up digital copyright owners from administrative and time-consuming burdens. We started creating multi-authority ciphertext policy. The novel Attribute Based Encryption (MACP-ABE) scheme demonstrate it is indistinguishable from plaintext under an adaptively selected plaintext attack (ICPA) while maintaining high performance and security. When the ciphertext access policy need to be updated, the right holder can sell the copyright to multiple users by merging MACP-ABE with proxy reencryption. This agent is barred from accessing any data related to digital content. An Ethereum smart contract is used to perform a meaningful exchange of the decryption keys among the party requesting the rights and the party holding the rights. To further enhance fairness, data on digital rights are stored on another blockchain as a ledge, which significantly reduces public blockchain's storage overhead. Our system can provide ICPA security, thwart collusion attempts, and safeguard user privacy, according to a security study. Performance study demonstrates that our system can offer a plethora of functionality to satisfy a variety of user demands. The simulation results demonstrate how effective our method is in comparison to other existing schemes.***

Key Terms—Blockchain, proxy re-encryption, Digital Rights Management (DRM), multi-authority ciphertext-policy attribute-based encryption (MACP-ABE).

I.INTRODUCTION

The massive growth and novel features of digital content have reignited interest in digital right management (DRM) systems, which utilize a variety of access control methods to limit the use of patented products and works protected by intellectual property [1][2][3][4][5][6][7].Distributed digital rights management (DDRM) and centralized digital rights management (CDRM) are the two primary subcategories of DRM systems. In the CDRM, the client must provide a third-party control over the transfer of digital rights before they may assign digital objects to that party. The CDRM's benefit is that it makes digital rights owners' lives much easier. However, a third party might break the law and engage in criminal activity, such as giving access to digital content to unapproved individuals. The interests of the owner of the digital rights will undoubtedly be harmed. Additionally, when a third party's server is compromised, certain data pertaining to digital material will be exposed. Additionally, all users will be impacted if the third party cannot be accessible. The DDRM allows the owners of the digital rights to distribute or formally transfer their rights. The Digital Distribution Rights Management system provides holders of digital rights with the ability to manage their rights, however, this comes with a significant increase in the amount of time and computing resources required. These new Internet goods, such serial novels or brief movies, are not well suited for the two types of DRM methods.

On the one hand, the authors of serial tales and quick films frequently lack the time to oversee their digital material as well. They often assign one or more platforms to handle their digital materials. On the other side, because short movies may be edited, updated, and disseminated more readily by an untrusted party, artists must utilize more effective methods to safeguard their rights and interests in the event of a disagreement. As a result, the creators could worry that the platform (the third party) would change their works or reveal them to certain unapproved audiences without their permission. The fairness, or if they can obtain the relevant digital materials after making a payment, may be of importance to the audience. They also hope that the platform would protect their privacy. Although a CDRM scheme can accommodate audience requirements, it might not be in the best interests of those who create digital material. Most of the time will be spent on encryption, promotion, sale, permission, etc. if the existing DDRM method is used, which will eventually reduce the amount of high-quality

digital material that can be produced. this is not a long-term solution.This is not beneficial for them.

II. Related Works

DRM scheme was initially proposed Rosenblatt et al. [8] in 2002, A digital rights management scheme (DRM scheme) is a system designed for protecting digital content from unauthorized access or distribution. DRM technology is often employed to enable content owners to control how their digital content is used and distributed, typically by restricting access or limiting certain activities.

DRM schemes may also include other security measures such as encryption, watermarking, digital signatures, and access control. DRM schemes are typically used by content providers to ensure that users abide by the terms of the license agreement, such as paying for the content, not copying it, or using it only within a certain time frame. They delivered comprehensive explanations of media rights, rights models, DRM system concepts, and a variety of commercial solutions. Later on, several researchers adopted different technologies to enhance and optimize the established DRM techniques.

A DRM plan was presented by Yen et al. [9]. The agent receives the data from the rights holder. Through the preview permission, the customer verifies the digital material, and through the agent, they execute the transaction. Through the client, the agent is able to keep track of user permissions.

Ibrahim et al.'s [10] proposal for an enterprise DRM technology that is safe, reliable, and has effective storage. Encryption the data is done by Rights holder using the symmetric key, the entire public key to encrypt the symmetric key, and the distributed share to sign the ciphertext before sending it to the authorization server. The separated ciphertext is sent to the appropriate storage server by the permission server using the information dispersal mechanism. and recovering the symmetric key using the verified distributed threshold decryption mechanism.

An enhanced corporate DRM approach was put out by Soliman et al. [11]. By utilizing a strategy for dispersing information and distributed storage, this system isolates the data ciphers.

An responsible privacy design for the DRM system was put up by Mishra [12]. The rights holder encrypts each file using a distinct symmetric key, which is then securely sent to the licensing server. The ciphertext is also transmitted to the distributor over this secure channel. When the distributor receives a license request from the customer, they verify the required authorizations and collect the relevant fee. The license is sent to the customer by the licensing server when it has received the distributor's communication.

On a peer-to-peer streaming system, Zhang et al. [13] suggested a unique DRM technique. The key exchange protocol is used by the server and node to authenticate one another. updating the owner list to reflect the authorized user's confirmation, and verifying the watermark in the file to show that the present user is indeed authorized.

A blockchain-based DRM method was created by Wang et al. Using the smart contract mechanism, the appropriate owner uses encryption, stores key, sets price, and controls key usage. Off-chain data ciphertext is obtained by the buyer, who then chooses from the smart contract the necessary permissions and key usage.

On the basis of the Bitcoin system, Zhang & Zhao et al. [15] suggested a unique DRM strategy for P2P networks. The data is encrypted by the proper owner using symmetric key and a public RSA key to encrypt the symmetric key. Peer-to-peer communication is used by the rights requester to receive the data's ciphertext, and the Bitcoin transaction script is used to acquire the accompanying private key.

A highly credible safe DRM method based on blockchain was presented by Ma et al. [16]. The approach uses a trusted third party to store the data in plaintext even though it keeps data index and permission information in blockchain.

A blockchain-based DRM method was presented by Zhang and Zehao [17]. According to their plan, the user must sign up on the blockchain and get a certain virtual money before making a transaction.

Through the investigation of the aforementioned existing schemes, several remarks and declaration of difference comparison of the connected works have been made. The issues with the present DRM methods are briefly summarized as follows.

i. Various users provide the same third party complete control over different types of digital information under the present CDRM methods [9], [12], [16]. Although the user is substantially facilitated by this approach, a third party is aware of the digital message's plaintext content. The user's interests will unquestionably be harmed by any malicious activity on the part of the third party.

ii. The transfer of copyright between the rights owner (RO) and the rights requester (RR) can occur without the involvement of a third party, utilizing current DDRM methods [10], [11], [15]. While this approach offers enhanced privacy protection for digital content, it may also be time-consuming and demand significant effort from the user.

In the current Distributed Digital Rights Management (DDRM) systems that utilize blockchain technology [14], [17], the entire DRM framework is located on the blockchain. The transparency of the blockchain can be used in this way to guarantee the equity of copyright transfers, but it will compromise user privacy too much for all interaction data to be kept there.

III. Proposed method

To address problems with the existing DRM methods, we created a dual-blockchain-based DRM approach that includes proxy re-encryption, multi-authority ciphertext-policy attribute-based encryption (MACP-ABE), and these techniques. We contributed these contributions, to name a few.

i. In order to ensure the flexibility of digital rights management and the privacy of digital assets, an unique MACP-ABE system has been proposed. The digital content is CPABE- encrypted, making it impossible for the agent to access any data because they do not have a

set of keys that match their characteristics. MACP-ABE fine-grained access control strategy allows for greater customization when it comes to distributing and managing digital rights. Furthermore, its multi-authority feature greatly reduces the risk of a single point of failure. Our system may offer adaptively selected plaintext attack (ICPA) security and give in distinguishability of plaintext while also being resistant to collusion attacks. Our system has undergone a thorough simulation, and the results demonstrate that it is quite effective when compared to other MACP-ABE schemes.

ii. The agent is responsible for collaborating with the rights holder to discuss the access policy and reencrypting the original ciphertext to create a new ciphertext with updated access policies. Additionally, they are tasked with educating all audiences about digital rights, which reduces the time and administrative costs for the rights owner.

iii. We established two blockchains to ensure fairness in the DRM transfer. The first blockchain utilizes a smart contract on Ethereum for the decryption key exchange. The second blockchain is responsible for storing digital content abstractions, signatures, and the hash value of the ciphertext. The rights requester formulates a smart contract using their global public key. Once the smart contract is completed, the agent and rights holder receive incentives, while the rights requester obtains access to the partial decryption keys. This mechanism guarantees that if all parties follow the protocol, they will achieve the desired outcome; if any party fails to comply, none will receive anything.

This plan proposes an improved user privacy protection in comparison to existing solutions, owing to the blockchain's storage of only the signature of the rights owner, as well as Ethereum's participant anonymity in smart contracts. Additionally, this plan has the potential to reduce storage costs and heighten blockchain efficiency as opposed to the storage of all digital material on the blockchain. This technique can be utilized in a range of different scenarios. It could reduce the amount of work and oversight needed by musicians by making sure that artists, agents, and fans have equal rights in the purchase of music copyright transactions. Furthermore, members' privacy will be protected as they gain access to the broadcasting rights sharing of popular TV shows.

This paper is organized as follows for the remaining portions. We describe the first stages in Section II. Our strategy's general layout is provided in Section III. The details of our proposed method are detailed in Section IV. The security, usability, and efficacy of the approach are covered in Section V. The conclusion of this paper is Section VI.

IV.PRELIMINARIES

Bilinear Pairing

Bilinear pairing is a mathematical pairing between two groups of points. The pairing is a bijection between the two groups, meaning that every point in one group is mapped to one and only one point in the other group. It is also bilinear, meaning that the pairing satisfies a certain mathematical property, which is that the pairing of two points in the first group multiplied by the pairing of two points in the second group is equal to the pairing of the product of the two points in the first group with the product of the two points in the second group. Bilinear pairings are used in cryptography and are an important part of the development of secure communication protocols.

The basis of pairing-based encryption is the discrete logarithm problem. The following are the three properties of bilinear pairing: bilinearity, nondegeneracy, and computeability.

Assume G1, G2, and GT are the 3 multiplicative cyclic groups. The map is described as e: G1, G2, GT which meets the three criteria listed below.

1.Bilinear first Equation:

e(g1a, g2b) = e(g1, g2)ab is valid for g1 G1, g2 G2, a, b Zp.

2.Nondegenerate:

e(g1, g2) = 1, GT exists for g1 G1, g2 G2.

3.Calculable:

For the case where g1 G1, and g2 G2, there is always a suitable procedure to compute e(g1, g2).

Linear Secret Sharing Scheme (LSSS)

It is a type of secret sharing scheme in which a secret is divided into multiple parts and distributed among different participants. This scheme is used to protect secrets from unauthorized access or manipulation by unauthorized parties. In this scheme, a part of the secret is shared with each participant and the entire secret can only be reconstructed when all the participants combine their parts. This scheme is an important tool for secure communication and data storage. It provides an effective way to protect sensitive data from external threats and unauthorized access.

Each participant receives a unique portion of the secret thanks to a method of encryption known as Shamir's secret sharing [18]. When it is necessary to extract the secret, you merely need to collect enough bits to utilize the decryption process to calculate the shared secret.

Shamir's secret sharing system is generalized as LSSS. The following is a typical description of LSSS:

1. Generation of a random polynomial: Choose a random polynomial of degree k-1, where k is the minimum number of participants that must be present to reconstruct the secret. The polynomial should have a constant term which is equal to the secret that is to be shared.
2. Choose the participants: Select the participants that will be involved in the scheme.
3. Assign a unique number to each participant: Assign a unique number to each participant that will be used to compute their share of the secret.

4. Compute the secret shares: Compute the secret shares for each participant by plugging their unique number into the polynomial and computing the output.
5. Distribute the secret shares: Distribute the secret shares to each participant.
6. .Reconstruct the secret: When the minimum number of participants are present, they can reconstruct the secret by computing the polynomial with their unique numbers and the secret shares they received.

Assumption of Complexity

The Bilinear Diffie-Hellman exponent decisional parallel assumption (BDH-DP) is an assumption used in cryptography that is believed to be computationally difficult to solve. The assumption states that given a bilinear group G of prime order p, two random elements g, g' ∈ G, and an element h ∈ G, it is hard to decide whether there exists an element x ∈ Z_p such that h = g^x = g'^x. The complexity assumption for BDH-DP is that it is computationally infeasible for an adversary to solve the decisional problem in polynomial time. It is believed that the problem can be solved in exponential time using the best known algorithms.

Access Tree Diagram

Access Tree Structure: In the ABE scheme system, access control policy is represented by a common structure called an access tree structure

1. Establish a secure channel for user authentication and authorization.
2. Use an access control policy to determine which users have access to which resources.
3. Use an encryption algorithm to protect data stored in the system.
4. Use a trusted third party or an attestation service to verify user identities and to establish secure transmission of data.
5. Use an access control list to determine which users have access to which resources.
6. Log all access attempts and maintain activity logs to detect any misuse of the system.
7. Use an access control matrix to determine which users have access to which resources.
8. Implement an audit trail system to track user activities and ensure accountability.
9. Implement an access control policy to define user rights and responsibilities.
10. Establish a secure communications channel for users to access resources.The access tree structure for the three functions is defined as follows: parent(x) returns the parent of a leaf node x; att(x) indicates the attribute associated with leaf node x; and index(x) returns the serial number of a node x from 1 to num, in order of its subnodes.

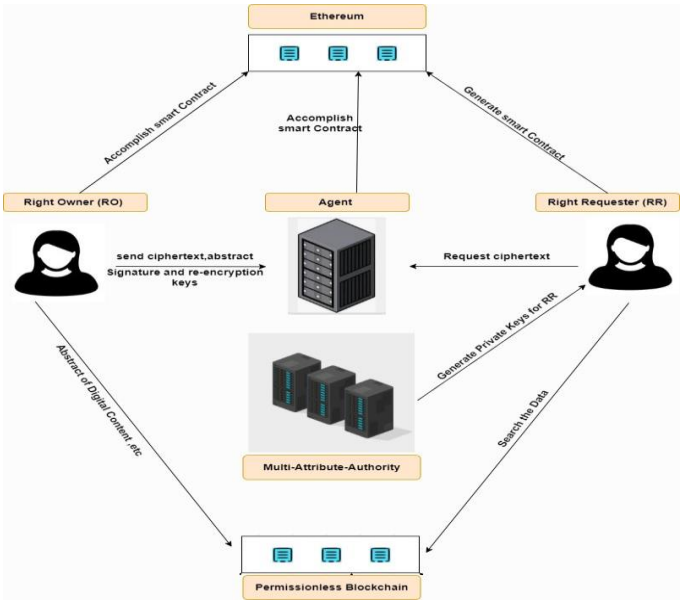

Fig 1 : Overview of proposed work

V.Proposed Scheme

a.System Model

As shown in Fig. 1, our system consists of six different entities: In our system, we presume that agent and RO are honest, and they will fill the smart contract with the proper decryption keys.

i. Rights Owner: The Right Owner (RO) may employ an agent to facilitate the sale of rights for the digital content with reduced effort and cost. The RO first generates a ciphertext, its signature, and an abstract of the digital content which are then securely transmitted to the agent. Subsequently, the ciphertext, its hash value, and the abstract of the digital content are published to the blockchain, while the RO creates corresponding partial decryption keys. Upon initiation of a smart contract by the Requestor of Rights (RR) on Ethereum for obtaining said rights, the smart contract is completed with the insertion of the respective decryption keys and signature of the RO.

ii. Rights Requester (RR): The RR uses blockchain ledger to identify digital rights. He creates a smart contract on Ethereum's blockchain, utilizing his global public key, which enables him to buy partial decryption keys from the RO and agent. These decryption keys are then used by the RR to decrypt encrypted digital content, granting them access.

iii. Multiattribute-Authority: Our scheme now incorporates multi-authorities. Each of them operates independently and generates public and private keys for each user, as well as a decryption key. One of these authorities is AAK. This technology could reduce the risk of a single-authority attack disabling the entire digital rights system. However, it could also make managing attributes and distributing keys more straightforward. Moreover, it is

feasible to meet the requirement for a distributed system in reality.

iv. Agent : The agent will coordinate with the RO to establish a process for granting access and re-encrypting the data with a new encryption key. They will then produce partial decryption keys, which they will connect to an Ethereum smart contract developed by the RR as well as affix their signature.

v. Ethereum: Here a smart contract on the Ethereum network is used to securely exchange partial decryption keys. To ensure that the data in the smart contract is linked to that on a separate blockchain, we provide the signature of the abstract. This safeguards the buyer's rights by allowing us to compare their purchase records with the relevant digital content, and it ensures that the result of the copyright purchase transaction is consistent with the digital material.

vi. For keeping track of details about digital content, such as the hash value of the ciphertext and the signature, a blockchain that saves data is utilized as a ledger. The permissionless blockchain is a fantastic option for maintaining specific digital material data that are publicly viewable, making it easy for anybody in the world to search for and locate what they're searching for.

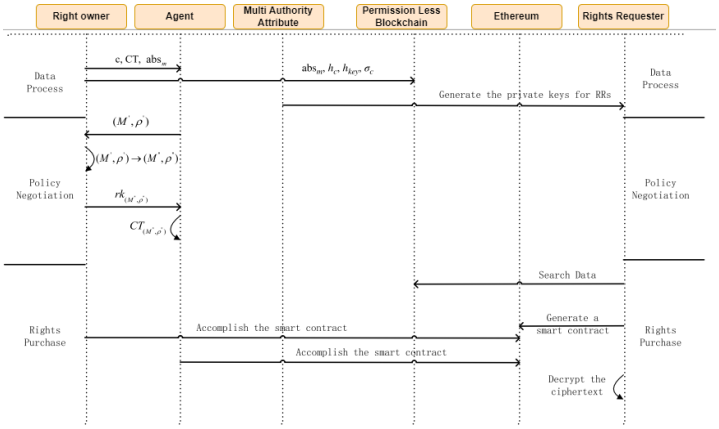

Fig 2: Proposed method

Our method is broken down into the three steps of data processing, policy negotiation, and right purchase (Fig. 2).

Data processing: We build up our system and assign authority throughout this step. The RO creates an abstract that belongs to the digital material and encrypts it. The RO also signs the signature for the ciphertext of the digital content.

The RO then transmits to the agent the ciphertext, signature, and abstract. The RO then publishes the ciphertext, symmetric key hash values, and abstract on the blockchain.

Policy Negotation: The RO incorporates some of the attributes they manage into the access policy the agent has supplied, resulting in a new access policy. Once the new access policy is in place, the RO will generate the corresponding re-encryption keys and pass them on to the agent. The agent can then take the initial ciphertext and re-encrypt it using the new re-encryption keys to produce the re-encrypted ciphertext.

Rights Purchase : In this procedure, the Requester searches for digital content on the blockchain, creates a smart contract using their global public key, generates partial decryption keys with the Resource Owner and Agent, fulfills the smart contract with signatures and keys, receives payment from both parties, obtains a symmetric key by decrypting ciphertext, and restores digital data by decrypting ciphertext encrypted with the symmetric key.

b.Threat Model

Our model presumes that the agent is both sincere and curious. We do not trust any other entities, so we assume that the agent will carry out the rights sale accurately and update access policies accordingly. However, since the agent is curious, they may be interested in acquiring digital content for their own benefit. Therefore, our threat models must take into account what knowledge the agent can acquire about how to obtain such material.

Known Ciphertext Model : The ciphertext-only attack corresponds to this threat model. The agent only has access to the ciphertext, abstract, and signature provided by the RR; nevertheless, in order to maximize advantages, he or she may attempt to decipher the ciphertext. By attempting to decipher ciphertext collected by the agent, the RR may also get privileges.

Collusion Attack Model : In this threat model, there are two cases. The first is that the RR conspires with one another to try to acquire rights that they do not already own. The agent and RR conspire to gain the rights in the second scenario.

c. Security requirements:

If an adversary A executes up to polynomial-time queries within a time period T, our method provides ICPA security with a negligible advantage AdvIND-CPA A over the interactive game. Our system is designed to be resistant to collusion attacks, even if all attribute authorities have been compromised and the malicious attribute authority is unable to decrypt the ciphertext. This is achieved by implementing a secure encryption scheme with a non- malleable encryption and authentication scheme to protect the ciphertext from being decrypted, modified, or replaced.

Here, we suggest a new MACP-ABE that would allow users to transfer their digital rights via an agent. And we'll go into depth about each of the three stages of our plan as follows:

Multi-authority Ciphertext-Policy Attribute-Based Encryption (MACP-ABE) is a type of encryption scheme that enables multiple authorities to securely encrypt and decrypt data in a distributed network. This encryption scheme is especially useful for distributed systems where different authorities control different parts of the system. MACP-ABE allows each authority to manage its own set of user attributes and access policies, while still allowing users to access resources controlled by other authorities. MACP-ABE uses a hierarchical

structure to organize the multiple authorities. At the top of the hierarchy is a global authority, which is responsible for managing the public key and the global access policy. Below the global authority are multiple subordinate authorities, each of which is responsible for managing its own set of user attributes and access policies. When data is encrypted using MACP-ABE, it is encrypted using a combination of the global public key and the public keys of each of the subordinate authorities. To decrypt the data, each

subordinate authority must provide its own decryption key, which is only accessible to it. This ensures that each authority only has access to the data that it is responsible for. MACP-ABE also allows for the creation of policies that restrict which users can access certain resources. These policies can be defined using a combination of attributes associated with each authority. For example, a policy might allow only certain users with a certain set of attributes to access a particular resource. MACP-ABE is a powerful encryption scheme that provides a secure way to share data between multiple authorities. By allowing each authority to manage its own set of user attributes and access policies, MACP-ABE ensures that only authorized users can access the data they need.

1. Setup Phase: a. Each authority generates a public/private key pair (sk_A, pk_A) using a key generation algorithm. b. Each authority publishes its public key (pk_A) to a central server.
2. Key Generation Phase: a. The user generates a secret key (sk_U) using a key generation algorithm. b. The user creates a ciphertext policy (CP) representing the set of attributes required to decrypt the ciphertext. c. The user generates a private key (sk_CPABE) associated with the CP using a key generation algorithm.
3. 3.Encryption Phase: a. The user encrypts the data using the CP and the public keys of the authorities. b. The ciphertext is generated using an encryption algorithm.
4. Decryption Phase: a. The user presents her secret key (sk_U) and the ciphertext to the authorities. b. The authorities use their private keys (sk_A) to decrypt the ciphertext. c. If the user's attributes match the CP, the
5. authorities enable the user to access the plaintext.

	Serve Load	RO Overhead	Agent Knows Plaintext	RO can monitor transactions	RO can deny	Distribute Scheme	Licensing Convenience	Protect the privacy of RP
[9]	High	Low	√	X	X	X	Hard	X
[10]	High	Low	√	X	X	X	Easy	X
[11]	High	Low	√	X	X	X	Easy	X
[12]	High	Low	√	X	X	X	Hard	X
[13]	High	high	N/A	√	√	√	Hard	X
[14]	High	Low	N/A	√	X	√	Easy	X
[15]	Low	High	N/A	√	X	√	Easy	√
[16]	High	Middle	√	√	X	X	Hard	X
[17]	Low	Low	N/A	√	X	√	Easy	X
Proposed	Low	Low	X	√	X	√	Easy	√

Table 1: Performance comparison

In Table 1, the comparison is shown. In contrast to previous schemes, [9]–[12] do not contain distributed schemes. The permission list and ciphertexts are stored on the server in the scheme in [13].

In [14] and [17], distributed digital rights management systems are created using blockchain technology and smart contracts. The method described in [15] combines Bitcoin with a peer-to-peer network to lighten the server's workload. It processes data through attribute encryption, allowing rights to be sold to multiple customers, which reduces the processing time and costs for the rights owner (RO). Access is granted to users via attribute private keys, protecting their true identities and making licensing more convenient while ensuring user privacy. A proxy re-encryption mechanism is utilized to provide the agent with authorization for sales without revealing any details about the data. Furthermore, copyright purchase records are stored on a blockchain to prevent the rights owner from denying the transactions.

Effectiveness Analysis

The most time-consuming step in the MACP-ABE system is the AASetup phase, even after expanding the attribute space from 10 to 40 attributes. The time required for this step increases with the size of the attribute space; however, the total processing time will not exceed 0.7642 seconds when there are 40 attributes. If the AASetup stage is omitted, the total processing time drops to 0.1892 seconds, which is acceptable. While increasing the number of attributes in the attribute space extends the AASetup phase, it has a minimal effect on the performance of subsequent stages.

Given the data we possess, we can assume that an increase in the

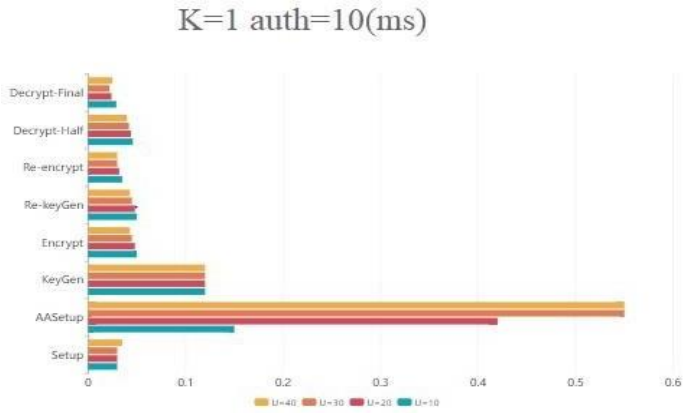

Fig .4 . Efficiency of MA-CPBE in the SCHEME

number of attributes connected to encryption and decryption will cause a delay in the system's start-up time. Nevertheless, the user will only experience a limited impact on the encryption and decryption time.

We can also conclude that even if the system has hundreds or thousands of features, the effects will only be present in the beginning and will not affect the user. Additionally, by relocating the majority of the bilinear maps to the decrypt-half section, which can be managed by external sources like cloud servers without compromising data security, we can tell from the decrypt-final stage's time overhead that the calculations required for the user's

decrypting process are exceedingly short. This will dramatically enhance the user experience. Evidence of this can be seen in Fig. 5(a) and Fig. 5(b), where we altered the number of characteristics linked to decryption, as well as the depth of the access tree. After the alteration of the access tree to k, a substantial increase in the time taken to decrypt-final was observed, while the times taken for encrypt, re-encrypt, and decrypt-half remained the same.

This shows that the jump from 5 to 10 decryption-related attributes had a major effect on the time it took to decrypt-final.

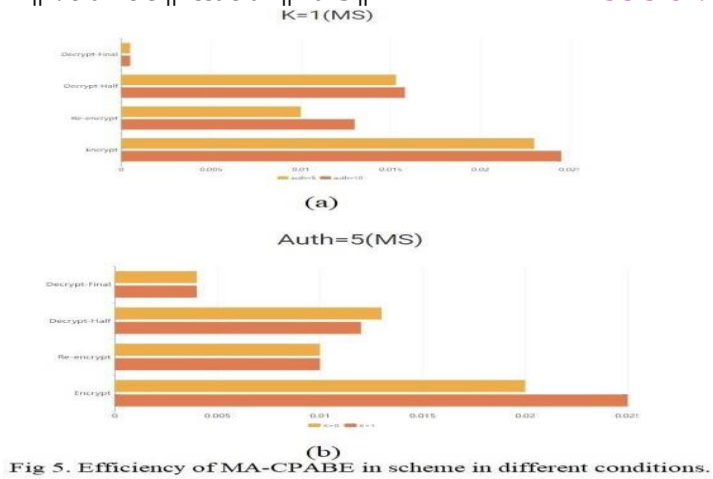

Fig 5. Efficiency of MA-CPABE in scheme in different conditions.

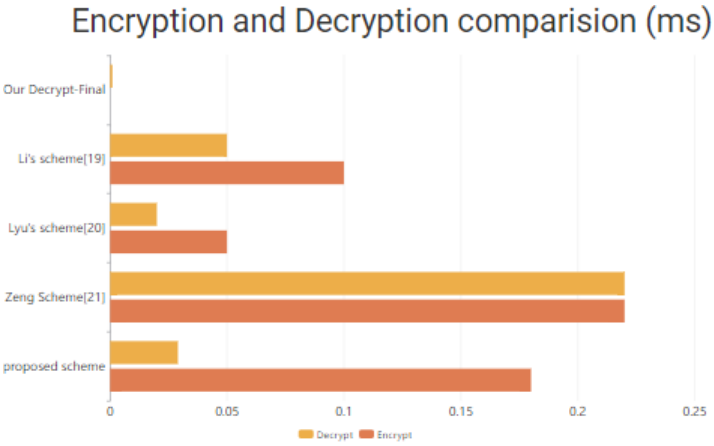

Fig. 6. Efficiency comparison with [19]–[21].

This indicates that we can manage users more effectively in real-world applications by utilizing a more complex access tree with increased depth. The rise in time and cost related to encryption and decryption with greater tree depth is minimal, so we don't need to be overly concerned about its impact on customers.

We also conducted a comparison of our approach with those proposed by Li [19], Lyu [20], and Zheng [21]. In our analysis, each Attribute Authority (AA) is assigned 10 attributes, while the number of attributes associated with decryption is set at 20. Additionally, the total number of attributes in the attribute space is also maintained at 20.

The comparative results illustrated in Fig. 6 demonstrate that our strategy offers a faster encryption time than Zheng's scheme, indicating an improvement in efficiency. However, it is important to note that our encryption time is somewhat less favorable when compared to the schemes developed by Lyu and Li. This suggests that while our approach has certain advantages, there are still areas for potential enhancement in encryption performance relative to these other methodologies. Overall, this comparison provides valuable insights into the strengths and weaknesses of our approach in the context of existing solutions

Case-1(Data processing)		Case-2 (policy negotiate)		Case-3(Rights Purchase)	
KeyGen	Encrypt	Re-KeyGen	Re-Encrypt	Semi-Decrypt	Final-Decrypt
(3s+1)E	(1+5)E+H+P	(10+l')E+2H+P	l'+2nP	nE+(3n)P	2E+H

Table 2: Calculation costs in proposed scheme.

Our scheme's decryption time is faster than Zheng's, Li's, and Ryu's, but slower than both of theirs. However, there are two elements to the decryption in our approach. In actuality, the user just has to complete the decrypt-final step, which takes less time than the first two techniques. The user might contract out to a cloud service provider for the stage of decryption-half. The user's global private key is required for the cloud service to retrieve any pertinent data.

In order to validate the running times, a comparison was conducted between the MACP-ABE approaches in the cited references [22]-[26]. For a case where ten authorities handled two attributes each, the encryption time in [22] was 5104 ms and decryption time was 2.5104 ms. Similarly, for the scenario involving four authorities maintaining seven characteristics each, the encryption time in [23] was 135 ms and the decryption time was 83 ms. Finally, for an instance with two authorities managing ten characteristics, the encryption time in [24] was 150 ms and the decryption time was 110 ms.

The encryption and decryption times of [25] and [26] are significantly slower than our own strategy, with [25] taking 1240 ms for encryption and 810 ms for decryption when four features are connected, and [26] taking 480 ms for encryption and 1400 ms for decryption when five features are kept by each authority and six authorities are involved.

In our approach, we also consider the computational costs involved. To facilitate a clear understanding of the associated notations used in the cost calculation for our proposed scheme, we define the following terms:

- Group G refers to the mathematical structure utilized in our calculations.
- E represents the symbol for the exponential operation within the group GT.
- P denotes the bilinear pairing operation.
- H signifies the operations performed by the hash function.
- s indicates the number of attributes that are assigned to the user.
- l refers to the number of attributes in the previous access policy (IA) that correspond to the Attribute Authority Key (AAK).
- n represents the total number of attributes in the decryption key that comply with the access policy.

By incorporating these definitions, we aim to provide a comprehensive framework for evaluating the computational expenses associated with our scheme, ensuring that all relevant factors are taken into account. This thorough analysis not only highlights the efficiency of our approach but also facilitates comparisons with existing methods, allowing us to identify areas for improvement and optimization in future iterations.

The computation costs of the proposed strategy are presented in Table 2 with particular emphasis being placed on the costs incurred by the agents. It can be seen that the semi- decryption operation has a greater computational cost than the encryption operation in data processing, as demonstrated in table 2. Nevertheless, this process is delegated to a cloud server, meaning that the cloud handles the more complicated computations and the decryption load of the RR is relieved quickly.

VI. CONCLUSION

We integrate MACP-ABE and proxy re-encryption technologies to secure digital rights while reducing the time and computational burden on the rights holder. This enables users to trade digital rights through intermediaries without the concern of the mediator accessing the digital content or disclosing related information. As

a result, our proposal effectively protects the privacy of digital content. To ensure fair transactions, the rights owner (RO) and the intermediary share the decryption keys generated via Ethereum's smart contract. For ease of user acquisition and public verifiability, a summary of the digital content, along with the hash value, the signature of the symmetric key, and the ciphertext, are all recorded on a separate blockchain.

We have conducted a comprehensive assessment of the recommended scheme. Our system has the capability to provide ICPA security, prevent collusive attacks, and protect user privacy, as evidenced by a security analysis. Moreover, our plan incorporates an Ethereum smart contract to guarantee equity. Our findings demonstrate that our scheme has more functionalities to meet the varying needs of users when compared to the methods discussed in [9]–[17]. Furthermore, the simulation results demonstrate that our plan is highly effective in actual conditions.

VII.REFERENCES

[1]N. Kashmar et al., "Smart-AC: A new framework concept for modeling access control policy," Procedia Comput. Sci., vol. 155, pp. 417–424, 2019.

[2]S. Ramamoorthy and B. Baranidharan, "CloudBC—A secure cloud data access management system," in Proc. IEEE 3rd Int. Conf. Comput. Commun. Technol., pp. 217–220, 2019.

[3]A. Ouaddah et al. "Access control in the internet of things: Big challenges and new opportunities," Comput. Net., vol. 112, pp. 237–262, 2017.

[4]A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in Proc. Europe MENA Cooperation Advances Inf. Commun. Technologies, pp. 523–533,2017.

[5]Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[6]S. Kirrane, A. Mileo, and S. Decker, "Access control and the resource description framework: A survey," Semantic Web, vol. 8, no. 2, pp. 311–352, 2017.

[7]D. Servos and S. L. Osborn, "Current research and open problems in attribute-based access control," ACM Comput. Surveys, vol. 49, no. 4, pp. 65:1–65:45, 2017.

[8]B. Rosenblatt, B. Trippe, and S. Mooney, "Digital rights management: Business and technology," M&T Press, New York, NY, 2001.

[9]C. T. Yen, H. T. Liaw, and N. W. Lo, "Digital rights management system with user privacy, usage transparency, and superdistribution support," Int. J. Commun. Syst., vol. 27, no. 10, pp. 1714–1730, 2014.

[10]M. H. Ibrahim "Secure and robust enterprise digital rights management protocol with efficient storage," Int. J. Inf., vol. 18, no. 2, pp. 625–640, 2015.

[11]A. H. Soliman, M. H. Ibrahim, and A. E. El-Hennawy, "Improving security and efficiency of enterprise digital rights management," in Proc. IEEE 6th Int. Conf. Comput., Commun. Netw. Technol., pp. 1–7, 2015.

[12]D. Mishra, "An accountable privacy architecture for digital rights management system," in Proc. 6th Int. Conf. Comput. Commun. Technol., pp. 328–332, 2015.

[13]J. Zhang, J. Cai, and Z. Zhang, "A novel digital rights management mechanism on peer-to-peer streaming system," in Proc. Advances Intell. Inf. Hiding Multimedia Signal Process., Springer, pp. 243–250 , 2017.

[14]D. Wang et al. "A novel digital rights management in P2P networks based on bitcoin system," in Proc. Int. Conf. Front. Cyber Secur., pp. 227– 240, 2018.

[15]Z. Zhang and L. A. Zhao, "Design of digital rights management mechanism based on blockchain technology," in Proc. Int. Conf. Blockchain, pp. 32–46,2018.

[16]Z. Ma, W. Huang, and H. Gao, "Secure DRM scheme based on blockchain with high credibility," Chin. J. Electron., 27, no. 5, pp. 1025–1036, 2018.

[17]Z. Zhang and L. A. Zhao, "Design of digital rights management mechanism based on blockchain technology," in Proc. Int. Conf. Blockchain, pp. 32–46, 2018,

[18]A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[19]X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, "Two-factor data access control with efficient revocation for multi-authority cloud storage systems,"IEEE Access, vol. 5, pp. 393–405, 2017.

[20]M. Lyu, X. Li, and H. Li, "Efficient, verifiable and privacy preserving decentralized attribute-based encryption for mobile cloud computing," in Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace, pp. 195–204, 2017.

[21]H. Zheng et al., "Modified ciphertext-policy attribute-based encryption scheme with efficient revocation for phr system," Math. Problems Eng., vol. 2017, Art. no. 6808190, pp. 1–10, 2017.

[22]Q. Li et al., "Secure, efficient and revocable multi-authority access control system in cloud storage," Comput. Secur., vol. 59, pp. 45–59, 2016.

[23]H. S. Gardiyawasam Pussewalageand V. A. Oleshchuk, "A distributed multi-authority attribute based encryption scheme for secure sharing of personal health records," in Proc. 22nd ACM Symp. Access Control Models Technol., pp. 255–262 , 2017.

[24]W. Luo and W. Ma, "Efficient and secure access control scheme in the standard model for vehicular cloud computing," IEEE Access, vol. 6, pp. 40420–40428, 2018.

[25]C. Pisa, T. Dargahi, A. Caponi, G. Bianchi, and N. Blefari-Melazzi, "On the feasibility of attribute-based encryption for WLAN access control," in Proc. IEEE 13th Int. Conf. Wireless Mobile Comput., Netw. Commun., pp. 1–8, 2017.

[26]Q. Li and H. Zhu, "Multi-authority attribute-based access control scheme in mhealth cloud with unbounded attribute universe and decryption outsourcing,"in Proc. IEEE 9th Int. Conf. Wireless Commun. Signal Process., pp. 1–7, 2017.

[27]B. Waters, "Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Workshop Public Key Cryptography, pp. 53–70, 2011.

[28]Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute-based encryption", in Proc. IEEE Symp. Secur. Privacy, pp. 321–334, 2007.

[29]M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. 16th ACM Conf. Comput.. Secur., pp. 121–130, 2009.

[30]J. Li et al., "Multi-authority fine-grained access control with accountability and its application in cloud," J. Netw. Comput. Appl., 2018, vol. 112, pp. 89–96, 2018.

[31]H. Zhong et al., "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage,"Soft Comput., vol. 22, no. 1, pp. 243–251, 2018.

[32]G. Yu et al. "Accountable multi-authority ciphertext-policy attribute-based encryption without key escrow and key abuse,"in Proc. Int. Symp. Cyberspace Saf. Secur., pp. 337–351, 2017.

[33]K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A Ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in Proc. IEEE 5th Int. Conf. Intell. Netw. Collaborative Syst., pp. 552– 559, 2013.

[34]Y. Zhang et al. "Anonymous attribute-based proxy re-

encryption for access control in cloud computing," Secur. Commun. Netw., vol. 9, no. 14, pp. 2397–2411, 2016.
[35]H. Li and L. Pang, "Efficient and adaptively secure attribute-based proxy reencryption scheme," Int. J. Distrib. Sensor Netw., Art. no. 5235714, vol. 12, no. 5, 2016.
[36]X. Zhang and Y. Yin, "Research on digital copyright management system based on blockchain technology," in Proc. IEEE 3rd Inf. Technology, Networking, Electron. Autom. Control Conf., pp. 2093–2097, 2019.