Performance analysis of the proxy-based and collusion-resistant revocable CPABE framework

Shobha Chawla, Neha Gupta
School of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India

Article Info

Article history:

Received Feb 1, 2024
Revised Feb 23, 2024
Accepted Mar 20, 2024

Keywords:

Attribute-level revocation
Ciphertext policy attribute-based encryption
Collusion resistant
Proxy server
User revocation

ABSTRACT

An efficient revocation of access rights in ciphertext policy attribute-based encryption (CPABE) schemes has multiple challenges, particularly for lightweight devices. Thus, extensive research on the existing studies enforcing and governing access control has been conducted. The methodologies used in the existing CPABE (bilinear pairing cryptography based) schemes to revoke users at the system and attribute levels have been focused on in the current study. The existing studies have been examined on the basis of the following parameters for revocation: type of revocation addressed, level of collusion resistance, dynamicity achieved, scalability of revocation, and computational cost incurred. It has been observed in the study that no single scheme achieves all the revocation properties and addresses both types of revocation. The module proposed in proxy-based and collusion-resistant multi-authority revocable CPABE (PCMR-CPABE) efficiently addresses both types of revocation and is fully collusion-resistant, dynamic, and scalable. The present paper extends the study on PCMR-CPABE and presents a performance analysis of the module in terms of functional specifications and computational cost. The presented analysis has compared the performance of the existing cutting-edge schemes with the PCMR-CPABE module and has proved that the proposed module is better in terms of functionality and is computationally inexpensive.

Corresponding Author:

Shobha Chawla
School of Computer Applications, Manav Rachna International Institute of Research and Studies
Faridabad, India
Email: shobha.chawla@gmail.com

1. INTRODUCTION

Ciphertext policy attribute based encryption (CPABE) scheme has enabled one-to-many encryption, fine-grained access control, and secure data transfer in a cloud environment. The scheme suggested access control enforcement by using the attributes of data consumers and allows successful decryption when the secret key of the data user satisfies the conditions of the access policy. The basic CPABE scheme has four entities: the data owner, the data user, the attribute authority, and the cloud service provider. Although the data owner uploads the encrypted data to the cloud, the basic CPABE system suggests that the data owner can still manage and decide who can access the sensitive data. The data owner defines the access policy, which regulates access control and denies access to unauthorized users of the file [1]. The data user has to possess certain attributes satisfying the access policy embedded in the encrypted data for successfully decrypting the ciphertext. Depending on the possessed attributes, the attribute authorities issue a secret key to the data users. The data user won't have access to the ciphertext unless their secret key meets the access policy. CPABE embeds the access policy within ciphertext. This association allows the data owner of the CPABE to determine the authorized user of the encrypted file. The existing schemes have implemented the base CPABE scheme using single or multiple authority frameworks. Under the single-authority framework, a single attribute authority controls the CPABE scheme. In single authority framework, the authority initializes the complete system and generates the secret key for the data users. However, the key-escrow problem under the single-authority CPABE system is a big concern. It causes a security breach of the entire system if it gets compromised. Alternatively, the incorporation of multiple attribute authorities in the CPABE scheme increased its reliability. Furthermore, data user attributes are controlled and managed by distinct authorities in the real world. Therefore, the incorporation of multiple attribute authorities enhanced the practicability of the CPABE scheme.

Among the various issues identified in the base CPABE scheme, the present paper studies the challenges pertaining to dynamic and scalable denial of access to revoked users with full collusion-resistance. The CPABE scheme allows the revocation of users at system and attributes levels. System-level or user revocation takes away the full access rights of the user. On the contrary, the user is revoked at the attribute level when he loses certain attributes but is still part of the system. As a result, upon attribute-level revocation, the user can only access files whose access policy conditions are complied with by the user's remaining attributes. An efficient revocable CPABE scheme should address both types of revocation and revocation should be scalable, dynamic, collusion- resistant and computationally inexpensive. We have proposed the proxy-based revocable CPABE in single-authority and multi-authority CPABE modules (based on bilinear pairing cryptography with LSSS) in [2] and [3], respectively. The key contributions of the present work are summarized as follows:

- The present work has briefly re-discussed the proposed proxy-based revocable CPABE in single-authority and multi-authority CPABE modules presented in [2] and [3], respectively. Both proposed modules are collusion-resistant, scalable, dynamic, computationally inexpensive, and ensure forward and backward secrecy.
- The present work presents the performance analysis of the proxy-based and collusion-resistant multi-authority revocable (PCMR)-CPABE module proposed in [3]. The study compares the computational cost of the proposed proxy-based collusion-resistant multi-authority revocable CPABE module (PCMR-CPABE) with the existing state-of-the-art schemes. The results of the analysis indicate that PCMR-CPABE is computationally inexpensive and efficient. Furthermore, PCMR-CPABE efficiently realizes the revocation at the system and attributes levels.

The CPABE schemes that are implemented using bilinear pairing cryptography have been studied in the present paper. An efficient revocation scheme must address revocation at both levels: system and attribute. It should be dynamic, scalable, fully collusion-resistant, computationally inexpensive, and maintain forward and backward secrecy. The present work has studied both levels of revocation handled by the existing single and multi-authority CPABE schemes. System-level revocation revokes all access rights of the user and can also be termed user revocation. A user doing mischievous activities or leaving the organization is a candidate for user revocation. An instant revocation of a user's access rights secures the system from unauthorized access. Several schemes using single or multiple authorities have proposed user revocation modules. They have mainly employed re-encryption of the ciphertext and updating of non-revoked users' keys to avoid revoked users' access. Re-encrypting ciphertext after each revocation in a dynamic environment adds to its size and, as a result, increases storage overhead [4]–[10]. A multi-authority CP-ABE scheme addressing traceability and revocation was proposed by [7] has imposed user-level access control on revoked users by periodically updating the keys of non-revoked users. The scheme proposed by the authors assumed the cloud server as a semi-trusted server and periodically updated ciphertext to deny access to revoked users. Consequently, instant revocation was not possible with this approach. The schemes that have employed proxy servers are either time-based, not scalable or have used access trees as access structures. The access tree-based control scheme makes it secure only under the generic group model. In addition, these schemes are partially resistant to collusion attacks [11]–[19]. Only two studiesm [15] and [12] have discussed the potentiality of the cloud service providers colluding with the revoked users and have also presented solutions to the issue.

When the role of the users changes in the organization, they lose a few of their attributes and access rights. The attribute-level revocation causes the revocation of a few attributes of the user and allows them to access only those resources that can be accessed using the remaining attributes. Existing schemes have updated the attribute group key to revoke users at the attribute level [20]. A few schemes have also proposed proxy re-encryption to achieve attribute-level revocation. The approaches in the existing schemes increase computational costs. In addition, a few schemes have also outsourced partial decryption to cloud service providers. This approach increases the likelihood of revoked users colluding and conspiring with cloud service providers to attack the CPABE system [21]–[30]. A multi-authority access control framework has been proposed as a centralized multi-authority CPABE framework. The proposed framework did not give attention to the possibility of a cloud server turning dishonest and colluding with the revoked user by keeping the older version of ciphertext or key in store [29]. Tu *et al.* [28], presented an instantaneous revocable CPABE scheme. Every time a user attribute is revoked, the multi-authority attribute-based encryption (MA-ABE) system updates the attributes group key. The scheme then updates the ciphertext to restrict access of revoked users. This leads to a computationally expensive approach. In addition, the author has paid little attention on CSP turning dishonest and colluding with the revoked users.

There are a handful of schemes that have presented solutions to both level of revocation [31]–[39]. However, these schemes are computationally expensive, as the key update and ciphertext re-encryption for revocation increase the computation and storage costs of keys and ciphertext. In addition, PIRATTE designed by Jahid and Borisov, and the Hur and Noh scheme are not scalable. The TUR-CPABE scheme implemented dual encryption apart from the re-computation of non-revoked users' keys and ciphertext updates to address the revocation of users. This causes an increase in computation costs. Furthermore, the CTFilter algorithm in the partially hidden access structures (PHAS)-highly efficient key revocation (HEKR)-CPABE scheme increased the computational cost and made it vulnerable to collusion attacks. The approach proposed in [32] updated users' keys and re-encrypted ciphertext to enforce user and attribute-level revocation. All attributes held by the user have been revoked in the proposed approach by the involved attribute authorities to address user revocation. The employed approach is highly computational expensive.

The literature survey has reviewed 36 relevant research articles from 2011 to 2022. From the 36 studied articles, 21 are single-authority revocable CPABE schemes, and 15 have multiple authorities. Out of 36, 16 studies have proposed solutions to only user revocation, 11 authors have addressed only attribute-level revocation, and 9 studies have addressed both levels of revocation issues. In addition, it has been observed all the studies ensure forward and backward secrecy. Collusion attacks can be perpetrated by the users themselves or by revoked users and the cloud service provider. Only four studies have discussed and addressed both types of collusion and are fully collusion-resistant whereas 32 studies did not give any attention to possibility of cloud being dishonest and colluding with revoked users. Furthermore, only 34 studies are dynamic and scalable, and 30 studies have a high computational cost due to key and ciphertext updates with each revocation. The literature study identified the following research gaps:

- Several studied schemes have addressed the revocation problem, either at system-level or attribute-level revocation, but not both.
- The existing cutting-edge schemes have employed either an embedded revocation list or updated the keys of non-revoked users and re-encrypted ciphertext. Such methods increase the size of the ciphertext and the cost of computation.
- Several schemes have also employed a cloud-assisted approach to outsource the computation load. In the existing systems, there hasn't been much consideration given to the potential of dishonest cloud service providers colluding with the revoked users. Thus, they are partially collusion-resistant.
- A few of the studied schemes were not scalable.
- In a dynamic environment, user-level and attribute-level revocation should be instantly addressed. It has been identified in the study of the existing literature that a few studies were not dynamic.

It has been observed in the study that no single scheme has alone achieved all the revocation properties and not also have addressed both types of revocation. Every studied scheme lack some or the other revocation properties. The next section discusses the design and implementation of the proposed proxy based collusion-resistant CPABE framework addressing revocation at both level for single and multi-authorities system.

The present paper is structured in four sections. Section 1 introduces the revocation issue with the CPABE scheme and reviews the existing studies addressing the challenges pertaining to revocation of users in the CPABE schemes. Section 2 briefly explained the algorithms proposed for proxy-based revocable CPABE in single-authority and multi-authority CPABE modules presented in [2] and [3], respectively. Section 3 analyzes the performance of PCMR-CPABE module proposed in [3] by comparing with the existing schemes at functional and computational level. Section 4 concludes the study.

2. METHOD

The proposed CPABE framework aimed to design two modules that could address revocation for users at the system and attribute levels. The design of algorithms of both the modules is briefly explained in this section. The first module presented a proxy-based single-authority CPABE module [2] , and the second module extended the design to multiple authorities [3]. Both modules are based on bilinear pairing cryptography, using LSSS as access policy and fully resist collusion. They ensure scalability and maintain secrecy at both the forward and backward levels. In addition, the modules are computationally efficient while realizing revocation, as they do not update non-revoked users' or attribute group keys and ciphertext to avoid access by unauthorized revoked users.

The proposed framework has employed a proxy server assisted approach. The secret decryption key has two parts: a secret key and a proxy key. A data user requests the secret key from the attribute authority for the set of attributes they own. On receiving the request, the authority computes the unique set of values for the data user and further computes the other four components of the key. The presence of the unique set avoids the possibility of collusion between data users. The proxy key includes a component of the requested ciphertext and a component of the secret key of the data user. All the keys are submitted to the decryption process. If the secret key has authorized attributes then the decryption algorithm by pairing the secret keys, proxy keys, and ciphertext components can recover the plain-text. The proposed approach is storage cost effective as it eliminates the need of re-encryption of ciphertext to enforce revocation. The framework enforces fine-grained access control with the proxy key. In the case of user revocation, the proxy server issues the proxy key, constituting invalid components. The decryption algorithm will fail due to the invalid components of the issued proxy key. Similarly, in the case of attribute-level revocation, the issued proxy key will allow successful decryption if the remaining attributes of the secret key are still part of authorized set. Table 1 shows the implementation specification of the proposed framework.

Table 1. Implementation specification

Parameters	Specification
Elliptic pairing curve group	Singular symmetric (‘SS512’)
Virtual machine platform	Oracle Virtual Box 6.1 running on Windows 11
Operating system	Ubuntu 22.04
Processor	1.20 GHz Intel Core i3 CPU
Memory	8 GB
Programming language	Python 3.7.13
Library	Stanford pairing-based crypto library [40]
Library modules used to implement the framework	Toolbox modules of the charm-crypto framework

2.1. Proxy-based and collusion resistance single-authority revocable CPABE module

The implementation of the first module has been presented in [2]. The proposed module has five entities (the attribute authority, the data owner, the data user, the proxy server, and the cloud service provider) that allow the proposed CPABE module to achieve one-to-many encryptions and efficient revocation. Each entity is responsible for executing an algorithm that contributes to the efficient design of the module. The proposed module has the following phases:

a) Initialization (setup algorithm): in the initial phase, the attribute authority invokes the setup algorithm that generates the master secret key MSK and the master public key MPK for the universe of attributes existing in the system.

b) Encryption (encrypt algorithm): in the encryption phase, the data owner encrypts the message and generates ciphertext components. The algorithm uses LSSS to define access structure $(\mathcal{M}, p)\ of\ p$ rows and q columns as explained in [2]. The data owner transmits the computed ciphertext to the cloud service provider.

c) Key generation (KeyGen algorithm): the secret key and the proxy key are the two segments of the secret decryption key. In this phase, the attribute authority generates a secret key on request from the data user. This secret key is issued once to the user and needs no updating to revoke access.

d) Proxy key generation (ProxyKeyGen algorithm): the proxy server invokes the proxy key generation process. This key enforces access control. This key is invalidated to fail the decryption process in the case of user revocation. Moreover, the algorithm removes the revoked attributes from the proxy key to enforce attribute-level revocation. The updated proxy key and the secret key can decrypt the ciphertext if the remaining attributes fulfill the conditions of the access policy. The proxy key has a time component embedded in it. This component causes the proxy key to expire after a set period. Thus, a revoked user cannot use the earlier-issued proxy key in the decryption process.

e) Decryption (decrypt algorithm): in the decryption phase, the ciphertext can be decrypted with the secret decryption key only if the secret key satisfies the access structure and the proxy key is not expired. In the case of revocation, the proxy server invalidates the proxy key. Thus, the decryption process fails. According to the linear reconstruction property, there exist constants $w_i \in Z_p$ where $i \in I$ and $I = \{ i: \rho(i) \in S\}$. Thus, for valid shares λ_i, $\sum_{i \in I} w_i \lambda_i = s$.

The proxy-based single-authority CPABE module is secure against q-parallel bilinear diffie-hellman exponent (BDHE) assumptions, data confidentiality, and collusion attacks. The security analysis of the module has been performed in [2]. It has been proven in the analysis that the cloud service provider (CSP) cannot acquire the secret key or proxy key. Hence, the CSP cannot conspire with the revoked users to gain unauthorized access. The study has also compared the performance analysis of the proposed module with the existing CPABE schemes and proved that the proposed module is computationally more inexpensive.

2.2. PCMR-CPABE module

The PCMR-CPABE module has been presented in [3]. The module has decentralized and distinct multiple authorities generating secret keys for the data user. PCMR-CPABE aims to propose a proxy-based, collusion-resistant, multi-authority, revocable CPABE module. The PCMR-CPABE module allows instant revocation and denies access to revoked users. In addition, the module can also revoke the partial access of users if only a few attributes of the user are revoked. The PCMR-CPABE module has implemented scalable, dynamic, and collusion-resistant revocation. Furthermore, it also achieved forward and backward secrecy for the system. Figure 1 exhibits the communication, exchange of data, and execution of algorithms by the entities in the proposed module.

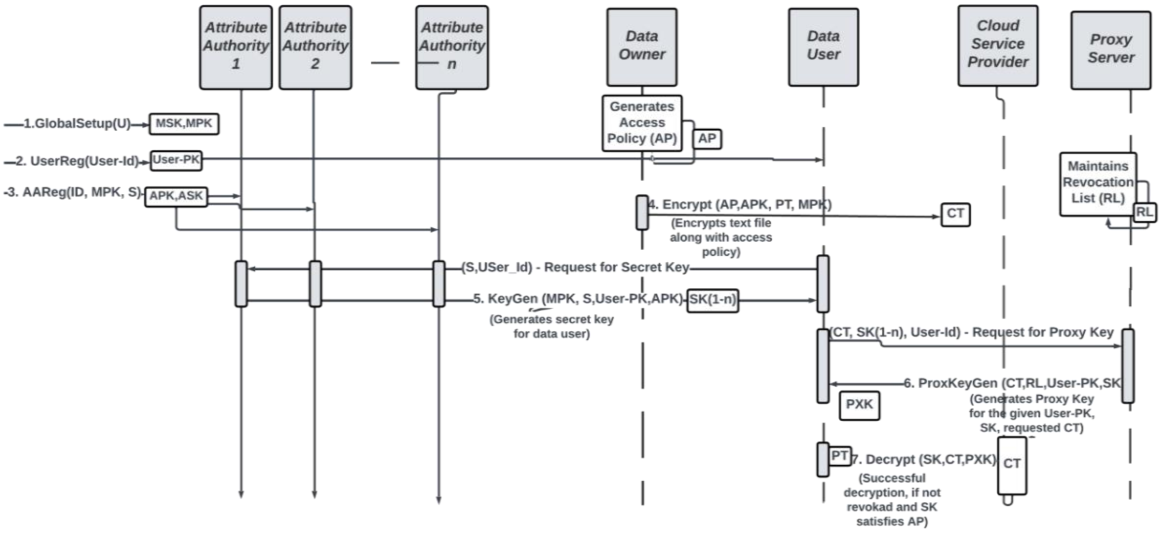
Attribute Authority 1
Attribute Authority 2
Attribute Authority n
Data Owner
Data User
Cloud Service Provider
Proxy Server
1.GlobalSetup(U)
MSK,MPK
2. UserReg(User-Id)
User-PK
3. AAReg(ID, MPK, S)
APK,ASK
Generates Access Policy (AP)
AP
Maintains Revocation List (RL)
RL
4. Encrypt (AP,APK, PT, MPK)
(Encrypts text file along with access policy)
CT
(S,USer_Id) - Request for Secret Key
5. KeyGen (MPK, S,User-PK,APK)
SK(1-n)
(Generates secret key for data user)
(CT, SK(1-n), User-Id) - Request for Proxy Key
6. ProxKeyGen (CT,RL,User-PK,SK
(Generates Proxy Key for the given User-PK, SK, requested CT)
PXK
PT
7. Decrypt (SK,CT,PXK)
(Successful decryption, if not revokad and SK satisfies AP)
CT

Figure 1. Sequence diagram of PCMR-CPABE module

Where: U is universe of attributes, MSK is master secret key, MPK is master public key, S is set of user's attributes, user-PK is user public key, APK is authority public key, ASK is authority secret key, SK is secret key of user, AP is access policy, PT is plain text, CT is ciphertet, PXK is proxy key of user, RL is revocation list.

The following algorithms are executed by the entities in the PCMR-CPABE module:

a) Initialization (global_setup): the initialization phase initializes the base setup parameters. The algorithm outputs the master public key MPK and master secret key MSK. The algorithm chooses a bilinear group G for setting up the parameters.
b) User registration (UserReg): in the user registration phase, the algorithm generates the private key for the data user. The algorithm stores the private key and sends it to the user through a secure channel. The private key issued to the user has been used as the identity component in the module.
c) Attribute authority registration (AAReg): in the attribute authority registration phase, the attribute authorities are registered and issued a public and secret key. The PCMR-CPABE module has assumed that all attribute authorities have distinct sets of attributes.
d) Encryption (encrypt): the encryption algorithm in the encryption phase encrypts the message M and sends the computed ciphertext to the cloud. The ciphertext also includes the embedded access policy based on the linear secret sharing scheme (LSSS). The algorithm uses LSSS to define access structure $(\mathcal{M}, p)\ of\ p$ rows and q columns as explained in [3].
e) Key generation (KeyGen): in this phase, the data user requests the issue of the secret keys to the involved attribute authorities. The attribute authorities of the system manage all the attributes. Each authority has a distinct set of attributes.
f) Proxy key generation (ProxyKeyGen): the proxy server computes the proxy key for the data user. The proxy key allows the PCMR-CPABE module to regulate access control. A decryption process runs successfully if the issued proxy key is valid. A time component has been embedded in the proxy key that

times out after a certain period. Whenever a new proxy key is requested, it is invalidated if the user ID is on the revocation list.

g) Decryption (decrypt): the decryption phase requires all the secret keys of the user (issued by all the authorities), the proxy key, and the ciphertext to compute message M. The message is computed if the proxy key is valid. The decrypt algorithm successfully decrypts the ciphertext if the user ID is not on the revocation list.

The study presented in [3] has also analyzed the strength of the PCMR-CPABE module against the q-parallel BDHE assumption and proved it secure. In addition, the module has also been proven secure against unauthorized access and collusion attacks by cloud service providers and revoked users. The analysis also ensured the maintenance of forward and backward secrecy.

3. RESULTS AND DISCUSSIONS

The performance of the PCMR-CPABE module has been functionally and computationally analyzed in this section. The functional analysis compares the operational-level specifications of the PCMR-CPABE module with those of SEM-ACSIT, MA-ABE, PMTER-ABE, and the Huang scheme and highlights the research gaps identified in these schemes. The comparison exhibits that except for SEM-ACSIT, all other schemes and the proposed module have decentralized multiple attribute authorities.

Table 2 shows that only the proposed module fully resists the collusion attacks. In PCMR-CPABE, the cloud service provider has no access to the proxy keys and secret keys of data users. Thus, they cannot conspire with the revoked users. In addition, only the proposed module and the Huang scheme have addressed the revocation issue at both the system and attribute levels. However, the Huang scheme updates the non-revoked users' secret keys and the ciphertext to enforce revocation. Such approaches increase computational overhead. The PCMR-CPABE module is implemented using the proxy server. The proxy server of the module prevents access by revoked or malicious users. The proxy server in the PCMR-CPABE module does not update the ciphertext or the key of non-revoked users to prevent the revoked users from accessing the ciphertext. Consequently, we can state that the PCMR-CPABE module is functionally more efficient than all the other listed schemes in Table 2. Table 3 compares the computational costs of all the schemes.

Table 2. Functionality comparison

Parameters	SEM-ACSIT [29]	MA-ABE [28]	PMTER-ABE [7]	Huang Scheme [32]	PCMR-CPABE proposed module
Approach	Centralized	Centralized	Decentralized	Decentralized	Decentralized
Level of revocation	Attribute-level Revocation	Attribute-level Revocation	user Revocation	User and attribute-level revocation	User and Attribute-level Revocation
Collusion resistance	Partial	Partial	Partial	Partial	Full
Ciphertext update	Yes	Yes	No	Yes	No
Key or attribute-group key update of non-revoked users	Yes	Yes	Yes	Yes	No
Forward and backward secrecy	Yes	Yes	Yes	Yes	Yes

Table 3 compares the computational efficiency of SEM-ACSIT, MA-ABE, PMTER-ABE, the Huang scheme, and the proposed PCMR-CPABE module. The number of pairings, exponential, and multiplication operations are used to calculate the computational expenses of the modules. The comparison of encryption modules shows that the PCMR-CPABE module generates ciphertext more quickly. It uses less exponential and multiplication operations than other stated schemes. The computing cost of the decryption algorithm for the PCMR-CPABE and SEM-ACSIT modules is also equal. Both the modules vary with $\mathrm{N_{ux_k}}$ and $\mathrm{N_k}$. Furthermore, the MA-ABE, PMTER-ABE, and Huang schemes decryption algorithms are computationally more expensive than the decryption algorithms of the PCMR-CPABE and SEM-ACSIT modules. The secret key generation algorithms of PCMR-CPABE and the SEM-ACSIT module vary in terms of A_k and N_{ux_k}. When compared to the SEM-ACSIT module, the proposed PCMR-CPABE module requires more exponential operations, but as the number of user attributes increases, the computational cost for the SEM-ACSIT module's key generation algorithm rises more than that of the proposed PCMR-CPABE module. In addition, the secret key generation algorithms of MA-ABE, PMTER-ABE, and the Huang scheme require more exponential and multiplication operations than the PCMR-CPABE module. The MA-ABE and SEM-ACSIT modules have only addressed attribute-level revocation, and only user revocation has been proposed by PMTER-ABE, while the PCMR-CPABE module and Huang's scheme propose solutions to both levels of revocation. Table 3 also shows that compared to the other specified schemes, the PCMR-CPABE revocation algorithms are computationally more efficient as the proxy server invalidates the proxy key in the case of revocation. The other listed schemes in Table 3 updated ciphertext and secret key and caused increase in the size of them. The proposed module do not cause any increase in the size of ciphertext or secret key while revoking the access rights. Thus, Table 3 shows that the comparison of all algorithms of the PCMR-CPABE with those of the SEM-ACSIT, MA-ABE, PMTER-ABE, and the Huang scheme proves that the PCMR-CPABE's algorithms are all more computationally efficient.

On our testing device, exponentiation takes 1.12 ms to process, multiplication takes 0.004 ms, and pairing operations take 0.94 ms. An average of 20 execution trials was calculated to determine the stable results. These values are used to compute the computation complexity of all the schemes listed in Table 3 to generate the CPU execution time of algorithms. The processing times required by the KeyGen, Encrypt, and Decrypt algorithms of all the compared schemes have been shown in Figures 2 to 4, respectively. As shown in the figures, the processing time of all three algorithms in SEM-ACSIT, MA-ABE, PMTER-ABE, the Huang scheme, and PCMR-CPABE increases linearly. The value of $\mathrm{N_k}$ is kept 4 while calculating the processing time of the schemes. Consequently, it can be stated that, in comparison to all the other schemes, PCMR-CPABE has the lowest execution time and is more feasible for resource-constrained devices.

Table 3. Comparison of computational cost

Modules	SEM-ACSIT	MA-ABE	PMTER-ABE	Huang Scheme	PCMR-CPABE Proposed Module
Encryption	$N_k\|P\| + (1 + 5N_{cx_k})\|E\| + 2N_{cx_k}\|M\|$	$(1+2N_{cx_k})\|P\| + (6N_{cx_k})\|E\| + 2N_{cx_k}\|M\|$	$(1+2N_{cx_k})\|P\| + (6N_{cx_k})\|E\| + 2N_{cx_k}\|M\|$	$(1+2N_{cx_k})\|P\| + (6N_{cx_k})\|E\| + 2N_{cx_k}\|M\|$	$\|P\| + (1+5N_{cx_k})\|E\| + N_{cx_k}\|M\|$
Decryption	$(N_k + 4N_{ux_k})\|P\| + (2 + 3N_{ux_k})\|M\| +(N_{ux_k} + 1)\|E\|$	$3N_{ux_k}\|P\| + (3N_{ux_k} + 1)\|M\| + (4N_{ux_k} + 5N_{cx_k} + 1)\|E\|$	$4N_{ux_k}\|P\| + 4N_{ux_k}\|\mathrm{M}\| + 4N_{ux_k}\|E\|$	$3N_{ux_k}\|P\| + (2 + 6N_{ux_k})\|M\| + 5N_{ux_k}\|E\|$	$(N_k + 4N_{ux_k})\|P\| + (2 + 3N_{ux_k})\|M\| + (N_{ux_k} + 1)\|E\|$
Key Generation	$(2N_k + 2N_{ux_k})\|E\| + (N_k + N_{ux_k})\|M\|$	$(4N_{ux_k})\|E\| + (2N_{ux_k})\|M\|$	$(5N_{ux_k})\|E\| + (2N_{ux_k})\|M\|$	$(5N_{ux_k})\|E\| + (2N_{ux_k})\|M\|$	$(5N_k + N_{ux_k})\|E\| + (N_k + N_{ux_k})\|M\|$
Revocation	Attribute-level Revocation 1. Ciphertext Update- $N_{cy_k}(\|E\| + 2\|M\|)$ Key Update- $2\|E\| + (N_{uy_k} + 1)\|M\|$	Attribute-level Revocation Ciphertext Update- $(1+2N_{cx_k})\|P\| + (6N_{cx_k})\|E\| + 2N_{cx_k}\|M\|$	User Revocation 1. Ciphertext update- $(1+2N_{cx_k})\|P\| + (6N_{cx_k})\|E\| + (1+8N_{cx_k})\|M\|$ 2. UpdateKeyGen- $4N_{nr_k}\|E\| + N_{nr_k}\|M\|$	User and Attribute-level Revocation- 1. UpdateKey- $N_{nr_a}\|E\| + N_{nr_a}\|M\|$ 2. CiphertextRe-encrypt – $N_{cx_a}\|E\| + N_{cx_a}\|M\|$	Proxy Key Generation 1. No Revocation- $(1 + N_{cx_k})\|E\|$ 2. User Revocation- $(1 + N_{cx_k})\|E\|$ Attribute-level Revocation- $(1 + N_{cx_k})\|E\|$

N_{cx_k}: number of attributes in an access policy owned by authority k. N_k: number of attribute authorities. N_{ux_k}: number of attributes held by a user. N_{cy_k}: number of ciphertext containing revoked attribute $\mathrm{y_k}$. $\mathrm{N_{uy_k}}$: number of non- revoked users holding revoked attribute $\mathrm{y_k}$. $\mathrm{N_{nr_k}}$: number of non-revoked users for attribute authority k. $\mathrm{N_{nr_a}}$: number of non-revoked users holding revoked attribute a. $\mathrm{N_{cx_a}}$: number of revoked attributes. |P|: number of pairing operations. |E|: number of exponential operations. |M|: number of multiplication operation.

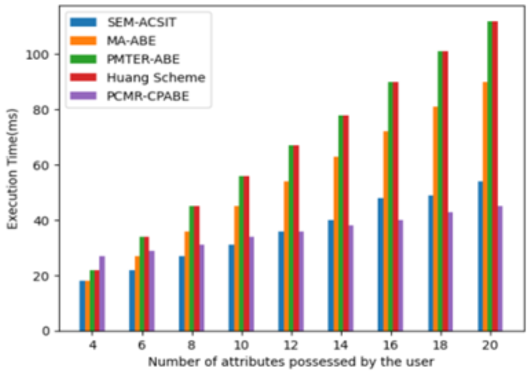

Figure 2. Comparison of KeyGen algorithm

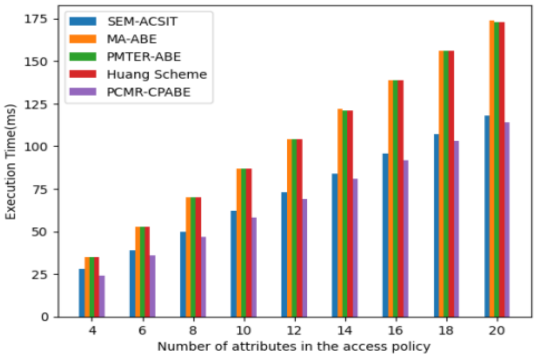

Figure 3. Comparison of encrypt algorithm

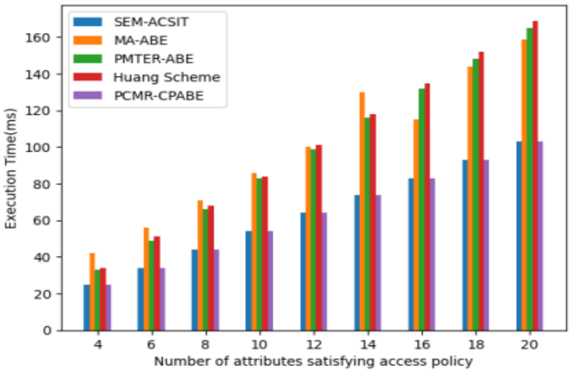

Figure 4. Comparison of decrypt algorithm

4. CONCLUSION

An algorithm becomes more feasible for resource-constrained devices when it has a low computing cost. The present study analyzed the performance of the multi-authority module (PCMR-CPABE) in terms of functional and computational. The analysis compares the functional attributes and the computational cost of PCMR-CPABE with the SEM-ACSIT, MA-ABE, PMTER-ABE, and the Huang's revocable CPABE scheme. The computational cost of key generation, encryption, and decryption algorithms of the PCMR-CPABE has also been compared with the schemes. The computational cost of algorithms has been calculated in terms of the number of pairings, the exponential, and the multiplication operations. The comparison shows that the proposed PCMR-CPABE module is computationally more inexpensive than the existing schemes. The comparison of the functional specification's states that PCMR-CPABE module has realized dynamicity, scalability, and full collusion-resistance. It also ensures forward and backward secrecy. The PCMR-CPABE module need for key updating or ciphertext re-encryption to enforce access control or revoke the access rights of users. Thus, it is also storage cost effective. The study concludes that PCMR-CPABE is practically implementable due to its cost effectiveness. PCMR-CPABE is based on bilinear pairing cryptography and is only secure against classical attacks but not quantum attacks. Our future research work will extend the PCMR-CPABE to lattice-based cryptography to prevent quantum attacks.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 321–334, 2007, doi: 10.1109/SP.2007.11.

[2] S. Chawla and N. Gupta, "A cloud based enhanced CPABE framework for efficient user and attribute-level revocation," *International Journal of Computers and Applications*, pp. 1–11, Aug. 2023, doi: 10.1080/1206212X.2023.2250149.

[3] S. Chawla and N. Gupta, "A proxy-based and collusion resistant multi-authority revocable CPABE framework with efficient user and attribute-level revocation (PCMR-CPABE)," *International journal of Safety and Security Engineering*, vol. 13, no. 3, pp. 527–538, 2023.

[4] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage," *Soft Computing*, vol. 22, no. 1, pp. 243–251, 2018, doi: 10.1007/s00500-016-2330-8.

[5] Z. Wu, Y. Zhang, and E. Xu, "Multi-authority revocable access control method based on CP-ABE in NDN," *Future Internet*, vol. 12, no. 1, pp. 15–28, 2020.

[6] N. Vaanchig, H. Xiong, W. Chen, and Z. Qin, “Achieving collaborative cloud data storage by scheme with dual-revocation,” *International Journal of Network Security*, vol. 20, no. 1, pp. 95–109, 2018, doi: 10.6633/IJNS.201801.20(1).11.

[7] K. Sethi, A. Pradhan, and P. Bera, “PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems,” *Cluster Computing*, vol. 24, no. 2, pp. 1525–1550, 2021, doi: 10.1007/s10586-020-03202-2.

[8] X. Zhang, Y. Chen, X. Yan, and H. Jia, “Multi-authority attribute-based encryption with user revocation and outsourcing decryption,” *Journal of Physics: Conference Series*, vol. 1302, no. 2, 2019, doi: 10.1088/1742-6596/1302/2/022026.

[9] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, “Revocable, decentralized multi-authority access control system,” *Proceedings - 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC Companion 2018*, no. Dec, pp. 220–225, 2018, doi: 10.1109/UCC-Companion.2018.00088.

[10] X. Zhang, F. Wu, W. Yao, Z. Wang, and W. Wang, “Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation,” *Concurrency and Computation: Practice and Experience*, vol. 31, no. 21, pp. 4678–4686, 2019, doi: 10.1002/cpe.4678.

[11] J. K. Liu, T. H. Yuen, P. Zhang, and K. Liang, “Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list,” *In 16th International Conference on Applied Cryptography and Network Security*, no. July, pp. 516–534, 2018, doi: 10.1007/978-3-319-93387-0_27.

[12] D. Sethia, H. Saran, and D. Gupta, “CP-ABE for selective access with scalable revocation : a case study for mobile-based healthfolder,” *International Journal of Network Security*, vol. 20, no. 4, pp. 689–701, 2018, doi: 10.6633/IJNS.201807.

[13] Z. Liu, S. Duan, P. Zhou, and B. Wang, “Traceable-then-revocable ciphertext-policy attribute-based encryption scheme,” *Future Generation Computer Systems*, vol. 93, pp. 903–913, 2019, doi: 10.1016/j.future.2017.09.045.

[14] Z. Liu, F. Wang, K. Chen, and F. Tang, “A new user revocable ciphertext-policy attribute-based encryption with ciphertext update,” *Security and Communication Networks*, vol. 2020, pp. 1–11, 2020, doi: 10.1155/2020/8856592.

[15] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, “Access privilege elevation and revocation in collusion-resistant cloud access control,” *Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2018*, no. Oct, pp. 209–214, 2018, doi: 10.1109/WorldS4.2018.8611568.

[16] D. Han, N. Pan, and K. C. Li, “A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 316–327, 2022, doi: 10.1109/TDSC.2020.2977646.

[17] Y. Wu, W. Zhang, H. Xiong, Z. Qin, and K. H. Yeh, “Efficient access control with traceability and user revocation in IoT,” *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 31487–31508, 2021, doi: 10.1007/s11042-021-11286-0.

[18] Z. Liu, Y. Ding, M. Yuan, and B. Wang, “Collusion resistance CP-ABE scheme with accountability , revocation and privacy preserving for cloud-based e-health system,” *International Journal of Network Security*, vol. 24, no. 4, pp. 597–611, 2022, doi: 10.6633/IJNS.202207.

[19] S. Xu, G. Yang, Y. Mu, and X. Liu, “A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance,” *Future Generation Computer Systems*, vol. 97, pp. 284–294, 2019, doi: 10.1016/j.future.2019.02.051.

[20] L. Y. Yeh, P. Y. Chiang, Y. L. Tsai, and J. L. Huang, “Cloud-based fine-grained health information access control framework for lightweightiot devices with dynamic auditing andattribute revocation,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 532–544, 2018, doi: 10.1109/TCC.2015.2485199.

[21] H. Lian, Q. Wang, and G. Wang, “Large universe ciphertext-policy attribute-based encryption with attribute level user revocation in cloud storage,” *International Arab Journal of Information Technology*, vol. 17, no. 1, pp. 107–117, 2020, doi: 10.34028/iajit/17/1/13.

[22] J. Zhao, P. Zeng, and K. K. R. Choo, “An efficient access control scheme with outsourcing and attribute revocation for fog-enabled e-health,” *IEEE Access*, vol. 9, pp. 13789–13799, 2021, doi: 10.1109/ACCESS.2021.3052247.

[23] G. Wang and J. Wang, “Research on ciphertext-policy attribute-based encryption with attribute level user revocation in cloud storage,” *Mathematical Problems in Engineering*, vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/4070616.

[24] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collusion avoidance CP-ABE with Efficient attribute revocation for cloud storage,” *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767–1777, 2017, doi: 10.1109/JSYST.2017.2667679.

[25] T. Naruse, M. Mohri, and Y. Shiraishi, “Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating,” *Human-centric Computing and Information Sciences*, vol. 5, no. 1, pp. 1–13, 2015, doi: 10.1186/s13673-015-0027-0.

[26] L. Touati and Y. Challal, “Batch-based CP-ABE with attribute revocation mechanism for the Internet of Things,” *2015 International Conference on Computing, Networking and Communications, ICNC 2015*, pp. 1044–1049, 2015, doi: 10.1109/ICCNC.2015.7069492.

[27] V. H., D. Goyal, and S. Singla, “An efficient and secure solution for attribute revocation problem utilizing CP-ABE scheme in mobile cloud computing,” *International Journal of Computer Applications*, vol. 129, no. 1, pp. 16–21, 2015, doi: 10.5120/ijca2015906807.

[28] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. Haq, “A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing,” *Computer Networks*, vol. 195, no. May, pp. 108196–108204, 2021, doi: 10.1016/j.comnet.2021.108196.

[29] S. Xiong, Q. Ni, L. Wang, and Q. Wang, “SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2914–2927, 2020, doi: 10.1109/JIOT.2020.2963899.

[30] Z. Liu, Z. L. Jiang, X. Wang, and S. M. Yiu, “Practical attribute-based encryption: outsourcing decryption, attribute revocation and policy updating,” *Journal of Network and Computer Applications*, vol. 108, no. January, pp. 112–123, 2018, doi: 10.1016/j.jnca.2018.01.016.

[31] L. Li, Z. Wang, and N. A. Li, “Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT,” *IEEE Access*, vol. 8, pp. 176738–176749, 2020, doi: 10.1109/ACCESS.2020.3025140.

[32] K. Huang, “Accountable and revocable large universe decentralized multi-authority attribute-based encryption for cloud-aided IoT,” *IEEE Access*, vol. 9, pp. 123786–123804, 2021, doi: 10.1109/ACCESS.2021.3110824.

[33] N. Abodoma, E. Shaaban, and A. Mostafa, “Adaptive time-bound access control for internet of things in fog computing architecture,” *International Journal of Computers and Applications*, vol. 44, no. 8, 2021, doi: 10.1080/1206212X.2021.1935653.

[34] W. Zhang, Z. Zhang, H. Xiong, and Z. Qin, “PHAS-HEKR-CP-ABE: partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 613–627, 2022, doi: 10.1007/s12652-021-02922-6.

[35] Z. Zhang, W. Zhang, and Z. Qin, “Multi-authority CP-ABE with dynamical revocation in space-air-ground integrated network,” in *Proceedings - 2020 International Conference on Space-Air-Ground Computing, SAGC 2020*, 2020, pp. 76–81, doi: 10.1109/SAGC50777.2020.00026.

[36] S. Wang, K. Guo, and Y. Zhang, “Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage,” *PLoS ONE*, vol. 13, no. 9, pp. 1–23, 2018, doi: 10.1371/journal.pone.0203225.

[37] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011, doi: 10.1109/TPDS.2010.203.

[38] S. Jahid and N. Borisov, “PIRATTE: Proxy-based immediate revocation of attribute-based encryption,” *arXiv preprint arXiv:1208.4877*, pp. 1–14, 2012.

[39] G. Ramu, B. E. Reddy, A. Jayanthi, and L. V. N. Prasad, “Fine-grained access control of EHRs in cloud using CP-ABE with user revocation,” *Health and Technology*, vol. 9, no. 4, pp. 487–496, 2019, doi: 10.1007/s12553-019-00304-9.

[40] J. A. Akinyele *et al.*, “Charm: A framework for rapidly prototyping cryptosystems,” *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013, doi: 10.1007/s13389-013-0057-3.

BIOGRAPHIES OF AUTHORS

Shobha Chawla is pursuing Ph.D. (Computer Application) from Manav Rachna International Institute of Research Studies and has total of 10+ year of experience in teaching and 8+ year of experience in research. She has authored research papers in Scopus/peer reviewed journal and IEEE conference proceedings in the area of cloud computing. Her research interests are cloud computing, cryptography and data mining. She can be contacted at email: shobha.chawla@gmail.com.

Neha Gupta has completed her Ph.D. from Manav Rachna International University and has total of 16+ year of experience in teaching and research. She is a Life Member of ACM CSTA, Tech Republic and Professional Member of IEEE. She has authored and coauthored 70 research papers in SCI/Scopus/peer reviewed journals (Scopus indexed) and IEEE/IET conference proceedings in areas of web content mining, mobile computing, and cloud computing. She has published books with publishers like Springer, Taylor and Francis IGI Global and Pacific Book International and has also authored book chapters with Elsevier, Springer, CRC Press, and IGI global USA. She can be contacted at email: nehag2012@gmail.com.