Journal of Autonomous Intelligence (2023) Volume 6 Issue 3
doi: 10.32629/jai.v6i3.748

ORIGINAL RESEARCH ARTICLE

Key management and access control based on combination of cipher text-policy attribute-based encryption with Proxy Re-Encryption for cloud data

R. Mohan Naik[1,*], H. Manoj T. Gadiyar[2], M. Bharathraj Kumar[1], B. K. Jeevitha[3], G. S. Thyagaraju[2], U. J. Ujwal[4], K. Arjun[2], S. M. Manasa[5], S. Avinash[1], J. Anil Kumar[6], T. K. Sowmya[1], K. P. Uma[3], A. R. Ramaprasad[7]

[1] *Department of Electronics and Communication Engineering, Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire 574240, Dakshina Kannada, Karnataka, India*

[2] *Department of Computer Science and Engineering, Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire 574240, Dakshina Kannada, Karnataka, India*

[3] *Department of Computer Science and Engineering, Vivekananda College of Engineering and Technology, Puttur 574203, Dakshina Kannada, Karnataka, India*

[4] *Department of Computer Science and Engineering, KVG College of Engineering, Kurunjibagh, Sullia 574327, Dakshina Kannada, Karnataka, India*

[5] *Department of Computer Science and Engineering, The Oxford College of Engineering, Bengaluru 560068, India*

[6] *Department of Electronics and Communication Engineering, JNN College of Engineering, Navule 577204, Shivamogga, Karnataka, India*

[7] *Vraio Software Solutions Pvt Ltd, Bengaluru 560055, Karnataka, India*

*** Corresponding author:** R. Mohan Naik, mohannaik@sdmit.in

ABSTRACT

In various cloud computing models, the data need to be protected and to access these data in secure manner is important. The cryptographic key which is used to secure these data using both in the encryption as well as in decryption it is mandatory to manage these keys to secure these keys by disclosing in public networks such as any wireless and cloud environment. Utilizing Ciphertext Policy Attribute-based Encryption (CP-ABE), which provides effective data governance and key management, for cloud data encryption. The work based on the combination of Cipher Text-Policy Attribute based Encryption and Proxy Re-Encryption is elaborated in the article (CP-ABE-PRE). The encrypted data should ideally be transformed such that it may be unlocked with new keys, without an intermediate decryption step that would allow the cloud provider to read the plaintext this process is known as data re-encryption. The computational and communication burden on users connecting to the cloud from resource constrained devices can be reduced using the proposed technique. The experimental results show for Cipher Text-Policy Attribute-Based Encryption are compared to the current algorithm (CP-ABE) demonstrate good results in encryption and decryption times. Additionally, the CP-ABE offers crucial distribution and administration options for cloud data. CP-ABE with Proxy Re-Encryption does appear to be highly efficient which proves verifiability and fairness for cloud data users to which also address revocation problem as well as collusion resistant model.

Keywords: key management; Ciphertext Policy Attribute-based Encryption (CP-ABE); Proxy Re-Encryption (PRE)

1. Introduction

The Cloud storage information facilities which provide large storage of information with flexibility of controlling and processing. This information is vulnerable to several attacks that may exist in any cloud storage

ARTICLE INFO

Received: 19 June 2023
Accepted: 21 July 2023
Available online: 4 September 2023

COPYRIGHT

Copyright © 2023 by author(s).
Journal of Autonomous Intelligence is published by Frontier Scientific Publishing. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).
https://creativecommons.org/licenses/by-nc/4.0/

services. So, its mandatory to secure this information by preserving the data without any modification. Every ciphertext in CP-ABE is combined with a policy for access that is based on attributes. These characteristics are connected to a user's personal key. Users won't be able to decipher the encrypted communication unless the private key's attribute completes the access structure connected to the ciphertext. Proxy Re-Encryption is a different method that rapidly gaining popularity to facilitate secure and private data association and sharing in the Cloud. By utilising a re-encryption key and a partially trustworthy proxy, Proxy Re-Encryption makes it possible to convert ciphertexts encrypted with converting the public key of the data owner into ciphertexts that another user's secret key may decrypt. The plaintext won't ever be visible to the proxy. Proxy Re-Encryption has been used by researchers in connection with the Cloud as well as for confidential and secure data sharing and cooperation.

Additionally, Proxy Re-Encryption and ABE have combined to boost security and privacy for cloud-based data collaboration and sharing. Several literary works utilise the combined power of the two systems to provide a more trustworthy and guarantee more confidence in the data owner for the cloud-based secure data sharing.

Privacy issues in cloud

Following are some of the privacy issues that may come across in the cloud platform.

Confidentiality Issues: Most of the information related to public which is essential to share with public cloud are vulnerable to various cryptographic attacks. The Hackers or data stealers try to steal these data and possibility to modify or delete the data available in public platform. To secure this confidential information many techniques have been implemented. The data subcontracting facilities such as unlimited cloud storage in these days offers the firms and data owners for treating and storing the massive data amount[1]. Even though, these are the advantages from cloud servers, there is appear in serious issues regarding the confidentiality and data security in the cloud environment[2].

Data Loss Issues: Data loss or data theft is one of the most significant security challenges that cloud providers face. More than 60% of consumers would refuse to use the cloud services offered by a provider if they had previously reported data loss or theft of crucial or susceptible data. Additionally, even if only one storage unit is hacked, it is very simple for an attacker to access several ones. However, they cannot access or regulate for specific stored record or enforce the data which is helpful for security[3].

Multi-Tenancy Security Issues: The term "multi-tenancy" refers to a model whereby several tenants share computing resources, data

storage, applications, and services. The same logical or physical platform is then used to host this in the location of the cloud service provider. By using this strategy, the supplier can maximise earnings at the expense of the customer. Attackers may unfairly use the possibility of having several residences and conduct a variety of attacks against their fellow renters, creating several privacy issues. There is a requirement of key in the proposed research that makes the system secure that overcome the problems of key management and key distribution[4]. So, it is mandatory to secure the content in the cloud without modifying the data[5,6]. The proper encryption algorithm provides the cloud platform to be more secure. And it is also mandatory to manage the cryptographic key needed in the encryption model. There are so many works related to key management has been undertaken. In this paper the model of CP-ABE and Proxy encryption is involved to provide efficient access control system with key management.

2. Literature review

The following part provides a survey of some contemporary approaches, along with information on their benefits and drawbacks.

Lei et al.[7] demonstrated the need for effective key management in a cloud environment. The protocol covers the creation, deletion, retrieval, updating, and actions on key and certificate-containing objects, among other things, as well as properties that are specific to the item in question, including the object identification.

Fathi et al.[8] suggested the LR-AKE Cluster mode protocol for effective key management. To enable communication across several servers, the LR-AKE requires the user to remember a password in addition to preserving a high-entropy secret on the client computer.

Sanka et al.[9] list of suggested capabilities for efficient. Without the data owner's persistent internet connection, key management and data access are possible. The capability list paradigm states that before storing the data in the CSP, the data owner produces a list with entries for each user and their access entitlements.

In the beginning, Goyal et al. proposed attribute-based encryption[10] offers a more flexible and granular access control for data. Using Proxy Re-Encryption, a semi-trusted proxy can convert ciphertexts that were encrypted using the data owner's public key into ciphertexts that can be decoded using another user's secret key. The proxy will never have access to the plaintext.

Using above literature and existing privacy issues in cloud, it is very important to design and implement a model which addresses the revocation problem and collusion free model the which provides with reduced commutation cost with proper access control. The following section elaborates the proposed CP-ABE-PRE model for resource constrained cloud storage devices.

3. Proposed methodology

3.1. Architecture description

Trusted authority (TA) as shown in **Figure 1** produces the required keys such as master secret key and public key. A unique code by considering user list is assigned for the properties, resulting in the creation of a revision key if revocation occurs. In this process the Attributes are used for generating of public and private key. The key generation unit will be used by data owner to secure the file which is uploaded into the cloud server. If the data user possesses the necessary characteristics and complies with the access policy established by the data owner, they will be able to decrypt the file and gain access to it. Some of the public factors are taken into consideration, such as the unique ID that is obtained using the secret key and the authority attribute that was generated in that configuration. The key encryption method will be gathered by CP-ABE in cases where the encrypted user declines the attribute set and where the decrypted user needs to keep the attribute set

to decipher the ciphertext. Different access structures are decrypted for various types of data by various users. This method is useful for preventing unwanted data access and it decreases cloud storage. To enable secure cloud data sharing, the ABE technique and proxy server work together to use the Proxy Re-Encryption strategy. According to the approach, a data owner, let's say Jack, encrypts data with a random key. After that, Jack creates another random value, k_1, and uses an access control policy and ABE to encrypt it. Later, Jack calculates k_2 using functions on k and k_1, i.e., $k_2 = k\ k_1$, and uses his public key to encrypt with Proxy Re-Encryption. The encrypted data and the two keys are then stored in the Cloud (ABE key and proxy key). The proxy key can be obtained by a permitted user, who can then re-encrypt it with his key, if one is discovered using an authorization list. Using this, he computes k, or $k_1\ k_2$, obtains the decrypted file, and then decrypts the ABE key.

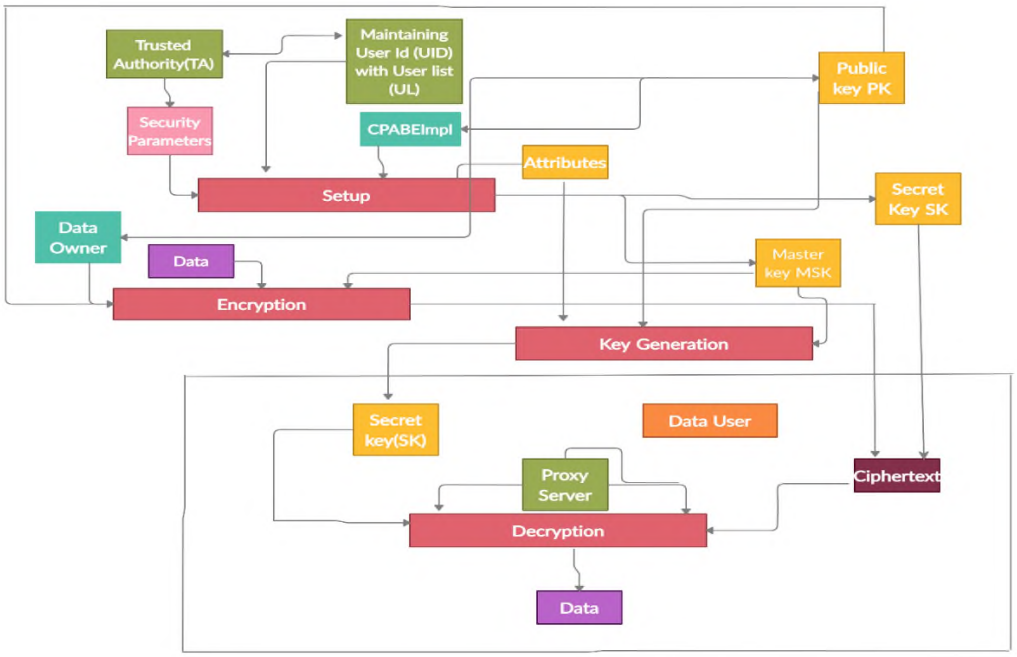

Figure 1. The proposed model using CPABE with proxy server.

3.2. Steps involved in the algorithm (CP-ABE-PRE)

The **Figure 2** elaborates without Proxy Re-Encryption and **Figure 3** describes the steps involved during the CP-ABE-PRE methodology with Proxy Re-Encryption here the user needs to perform initialization step followed by encryption using CP-ABE method where the ciphertext is hidden and the access structure is by using the Linear Secret Sharing Scheme (LSSS) and it is designed for applying highly expressive monotone access structures in CP-ABE schemes. After encryption of the data, it is stored in the cloud. In the decryption process if a set of attribute secret keys owned by a certain user satisfy the access matrix of the ciphertext, the decryption algorithm can successfully recover the data. Here Proxy Re-Encryption for enabling secure and confidential data sharing and collaboration in the Cloud. Proxy Re-Encryption scheme where the data owner's private key is divided into two parts. One half is stored in the data owner's machine while the other is stored in the Cloud as a proxy the user who has access rights can then retrieve the data as the proxy will decrypt the ciphertext with half the user's private key in the proxy and then decrypt again on the user's side to retrieve the full plaintext.

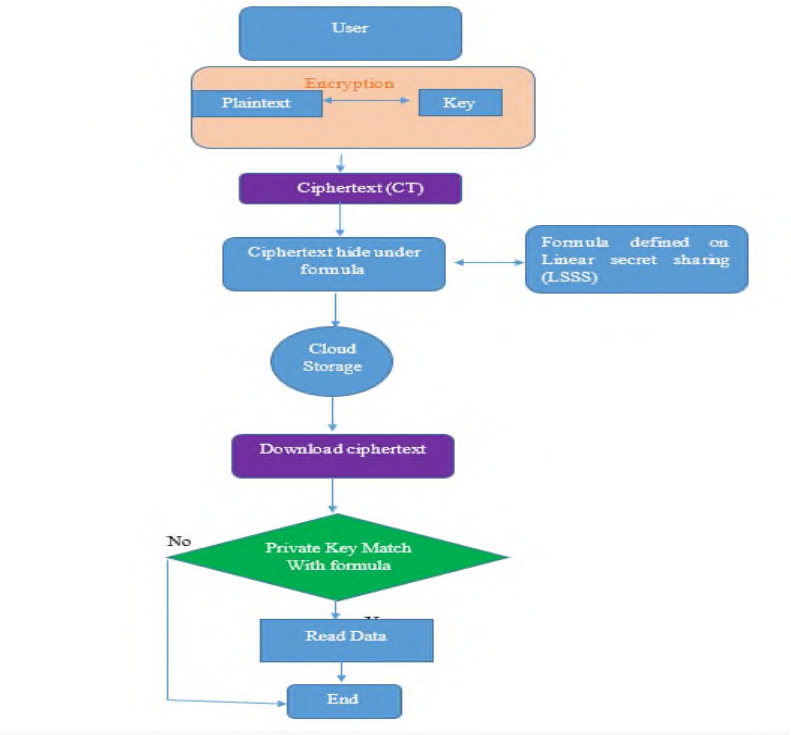

Figure 2. Flow diagram for the proposed algorithm.

The steps followed in the proposed algorithm.

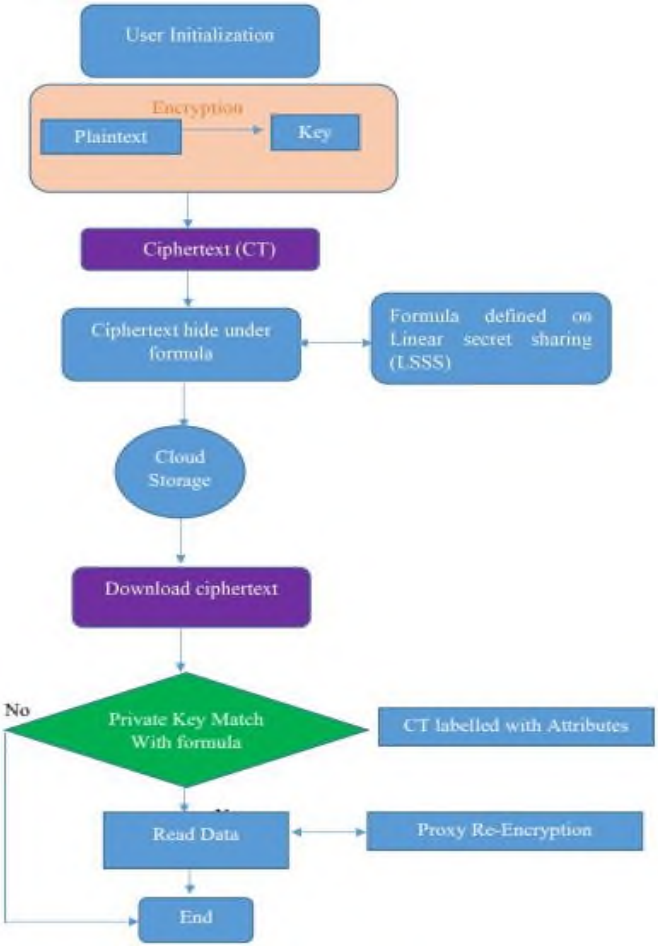

Figure 3. The steps followed in the proposed CP-ABE-PRE.

3.3. Proposed CP-ABE-PRE model

In this section the detailed proposed algorithm is explained using the user setup techniques, TA generates the PK, MSK, and UID numbers. To create their own PK and MSK, which are assigned as a universal attribute set, the TA acquires the security parameters and uses them. The DO receives the MSK after the PK has received the created PK and MSK. The secret key created sends and saves data from the PS, but it cannot decode the data because it will become a part of the user. The following measures were taken:

- **Setup (λ)**

The multiplicative cyclic groups G_0 and G_1 are included in the prime order p.

Let g be given as a generator of G_0 with the bilinear map e defined as in the Equation (1).

$$e: G_0 \times G_1 \rightarrow G_T \tag{1}$$

Select uniform values for α and β randomly from $Z_p', \alpha, \beta \epsilon_R Z_p'$

The *PK* is reported in accordance with Equation (2),

$$PK = (G_0, g, g_1, g_2, f_1) \tag{2}$$

where

$$g_1 = g^{\beta}$$
$$g_2 = e(g, g)^{\alpha}$$
$$f_1 = g^{\frac{1}{\beta}}$$

where *MK* is defined as (b, g^{α}).

- **Encryption**

The input of an encryption algorithm produces a cypher text CT that is specified by the term "encrypt", and the method produces a message denoted by the symbol *M* and an access matrix denoted by the symbol (A); that contains the public keys for the attributes used in the access policy (*PK*, *M*, *T*).

Two components make up the cipher text.

- **First part**

Each data is encrypted using the symmetric encryption algorithm *E(m,k)*, which is represented by Equation (3).

$$CTs = EM \parallel CT \tag{3}$$
$$EM = \{\varepsilon(m_i, k_i)\}_{i=1}^{l} \tag{4}$$

where

$$k_i = H_2(a_i \parallel a_0)$$

- **Second part**

This situation demonstrates how ABE functions. The complete Cipher Text (CT) is displayed as in the Equation (5).

$$CT = (B_0, C_0, B_1, C_1, \{B_{N_i}, C_{N_i}\}_{i=2}^{l}, \{E_{N_i}, E_{N_i}{}'\}_{n_{i \in Node}}) \tag{5}$$

where

$$\left.\begin{aligned} B_0 = a_0 e(g, g)^{\alpha S_0}, C_0 = g^{\beta S_0} \\ B_1 = a_1 e(g, g)^{\alpha S_1}, C_1 = g^{\beta S_1} \end{aligned}\right\} \tag{6}$$

So in general it is defined as

$$B_{N_i} = a_i e(g, g)^{\alpha f_{N_i}(0)} a_i = H_2(k_{j+1} \parallel j), C_{N_i} = g^{\beta f_{N_i}(0)}$$

$$E_{n_i} = g^{f_{N_i}(0)}, E_{N_i}{}' = H_1(attn(n_i))^{f_{n_i}(0)}$$

$H_1(')$ is the collision resistant hash function.

$H_1: \{0,1\}^* \rightarrow Z_P'$

- **Key generation**

At this point, the Authority Setup algorithms are being executed with respect to the inputs as a result of the outputs from the System Setup.

The Generation method creates an output and distributes it to qualified users with the attribute secret key corresponding to a GID.

$$KeyGen(MK, SK) \tag{7}$$

We assume that the function $r\epsilon_R Z_p'$ uniform, however they were chosen using a random function Z_p'.

The randomly chosen values becomes as

$$r_j \epsilon_R Z_p', \forall_j \in S \tag{8}$$

The *SK* is represented as $SK = (D, \{D_j, D_j'\}_{j \in S})$, where

$$D = g^{\frac{(\alpha + r)}{\beta}} \tag{9}$$

$D_j = g^r H_1(j)^{r_j}$ and $D_j' = g^{r_j}$.

- **Decryption**

The primary function of the decryption method is to recover the message M and set the secret key attributes that belong to a certain user while satisfying the ciphertext's access matrix. The decoding algorithm would then fail.

To ascertain if the access policy having the tree satisfies the set of attributes *S.*

If *T*: $T(S) = T_o(S)$ and $T_1\ (S)$ (When $T(S) = 1$)

Go to step 2

Else

Return.

The proposed CP-ABE-PRE achieves the better privacy with access control that possesses less storage ahead and stores the part of *SK* in the *PS*. The proposed CP-ABE-PRE reduces the system complexity in the DO thereby delegates the CT update to PS which reduces the DU complexity that delegates the SK to PS during revocation which is collusion resistant.

4. Quantitative result analysis

We steered a series of experiments to assess the performance of the CP-ABE-PRE model in practice. The model was executed on a Windows 11 PC platform with a 2.2 GHz Intel Core i5 CPU and 8 GB RAM. The bilinear cryptographic operations were performed using the JAVA programming language. Tysowski and Hasan[11] gave an easy method to perform user revocation operation by combining CP-ABE with re-encryption. In their scheme, each user belongs to a group and holds a group secret key issued by the group. However, their scheme does not resist collusion attack performed by revoked users cooperating with existing users. Li et al.[12] has demonstrated that the suggested technique is secure under the Diffie-Hellman assumption of divisible computation, and local devices can calculate with relatively little expense offer a ciphertext-policy attribute-based encryption (CP-ABE) scheme with effective user revocation as elaborated in Ramachandra et al.[13].

To use resource constraint devices, the proposed algorithm is much convenient to perform good results with key lengths variations. The **Table 1** provides an evaluation of the proposed CP-ABE-performance PRE's in terms of different cloud datasets which is having a file size of 7 KB and 15 KB and the performance analysis is done by using encryption time, decryption time, and completion time for keys with lengths of 8, 16, 32, 64, 128, and 256 bits for 7 KB and 15 KB data file as demonstrated in **Figure 4**. The encryption, decryption, and completion time all decrease as the key length rises, demonstrating increased self-checking, error-detection, and error-correction. The accompanying table shows that the criteria consider validating the efficacy of the suggested strategy. Here the statistical significance is obtained using real data parameters which significantly improved in the decryption time even if the key size increased. The CP-ABE-PRE model significantly lower the time cost to decrypt ABE ciphertexts by introducing the re-encryption method. Additionally, the time used in decrypting a re-encrypted ciphertext is independent of the number of attributes and thus much less than that of decryption for an ABE ciphertext. Comparing to Li et al.[12] the decryption time is slightly greater, and we prove our model is efficient for resource constrained cloud storage devices with fine grained access control.

Table 1. Performance analysis of proposed method for 7 KB and 15 KB data file respectively.

Key length in bits	Encryption time (ms) for 7 KB data	Encryption time (ms) for 15 KB data	Decryption time (ms) for 7 KB data	Decryption time (ms) for 15 KB data	Completion time (ms) for 7 KB data	Completion time (ms) for 15 KB data
8	19,456	26,578	17,544	22,223	47,123	49,378
16	17,197	18,209	10,233	11,874	29,344	30,815
32	8216	9131	4355	5066	13,663	14,797
64	4201	4465	2301	2547	5923	7607
128	2132	2251	1123	1378	2854	4194
256	967	1017	674	824	2102	2373

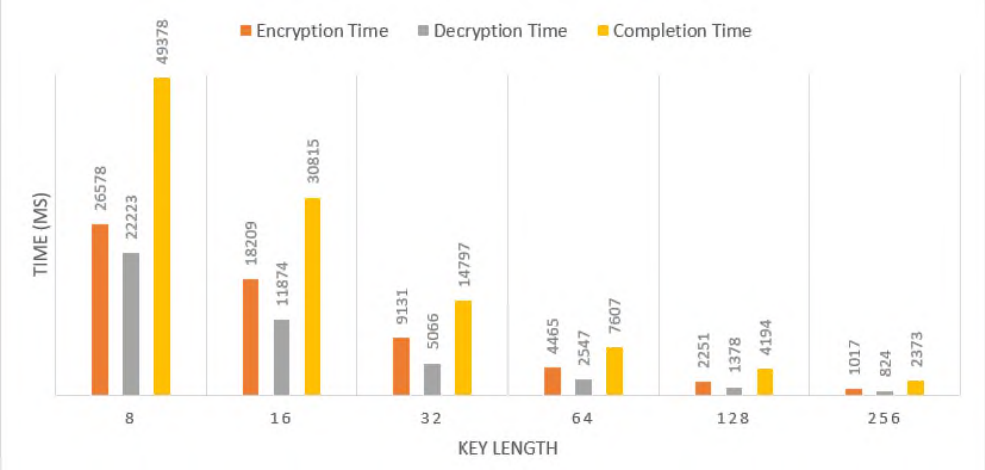

Figure 4. Graphical representation for the proposed CP-ABE-PRE scheme.

5. Conclusion

The proposed Key Management and Access control model for Cloud Data based on Cipher Text-Policy Attribute-Based Encryption and Proxy-Re Encryption (CP-ABE-PRE). The experimental results demonstrate how CP-ABE is used in proper key management with access control system and decrypting a re-encrypted ciphertext which is independent of the number of attributes which is done with proxy-re encryption scheme. For designing cryptographic protocols, key management deals with the storage, usage, and replacement of keys at the user level. The proposed CP-ABE-findings PRE's at key length 256 (bits) demonstrate decrease in completion time. The findings revealed that as key length rose, encryption, decryption, and completion times

all dropped, indicating a decrease in time consumption and an improvement in the security of the data. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. Our experiment results show computation cost for local devices is relatively low and can be constant. The proposed model is appropriate for resource constrained devices. The existing ABE-PRE[14] schemes do not support a mechanism to achieve verifiability and fairness. The verifiability enables a shared user to verify whether the re-encrypted ciphertext reverted by the server is correct and the fairness guarantees a cloud server escape from malicious accusation if it has truly conducted the re-encryption operation fairly. In this paper, the proposed CP-ABE-PRE model proves a novel verifiability and fair attribute-based Proxy Re-Encryption remarkably, our model can withstand collusion attack performed by revoked users cooperating with existing users. In future the datasets can be changed with different image data to observe good results in CP-ABE-PRE with increase in key size.

Author contributions

Conceptualization, RMN; methodology, HMTG; software, MBK; validation, BKJ, and UJU; formal analysis, KA; investigation, SMM; resources, SA and JAK; data curation, TKS; writing—original draft preparation, RMN; visualization, KPU; supervision, ARR; project administration, GST. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Premkamal PK, Pasupuleti SK, Alphonse P. Dynamic traceable CP‐ABE with revocation for outsourced big data in cloud storage. *International Journal of Communication Systems* 2020; 34(2): e4351. doi: 10.1002/dac.4351
2. Xue K, Gai N, Hong J, et al. Efficient and secure attribute-based access control with identical sub-policies frequently used in cloud storage. *IEEE Transactions on Dependable and Secure Computing* 2020; 19(1): 653–646. doi: 10.1109/TDSC.2020.2987903
3. Zhao Y, Ren M, Jiang S, et al. An efficient and revocable storage CP-ABE scheme in the cloud computing. *Computing* 2019; 101(8): 1041–1065. doi: 10.1007/s00607-018-0637-2
4. Wang S, Wang X, Zhang Y. A secure cloud storage framework with access control based on blockchain. *IEEE Access* 2019; 7: 112713–112725. doi: 10.1109/ACCESS.2019.2929205
5. Rath M. Resource provision and QoS support with added security for client side applications in cloud computing. *International Journal of Information Technology* 2019; 11(2): 357–364. doi: 10.1007/s41870-017-0059-y
6. Singh A. Security concerns and countermeasures in cloud computing: A qualitative analysis. *International Journal of Information Technology* 2019; 11(4): 683–690. doi: 10.1007/s41870-018-0108-1
7. Lei S, Zishan D, Jindi G. Research on key management infrastructure in cloud computing environment. In: 2010 Ninth International Conference on Grid and Cloud Computing; 1–5 November 2010; Nanjing, China. pp. 404–407.
8. Fathi H, Shin S, Kobara K, et al. LR-AKE-based AAA for network mobility (NEMO) over wireless links. *IEEE Journal on Selected Areas in Communications* 2006; 24(9): 1725–1737. doi: 10.1109/JSAC.2006.875111
9. Sanka S, Hota C, Rajarajan M. Secure data access in cloud computing. In: 2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application; 15–17 December 2010; Bangalore, India. pp. 1–6.
10. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security (CCS ’06); 30 October–3 November 2006; Alexandria Virginia USA. pp. 89–98.
11. Tysowski P, Hasan MA. Hybrid attribute-based encryption and re-encryption for scalable mobile applications in clouds. *IEEE Transactions on Cloud Computing* 2013; 1(2): 172–186. doi: 10.1109/TCC.2013.11
12. Li J, Yao W, Zhang Y, et al. Flexible and fine-grained attribute-based data storage in cloud computing. *IEEE Transactions on Services Computing* 2017; 10(5): 785–796. doi: 10.1109/TSC.2016.2520932
13. Ramachandra MN, Gadiyar HMT, Bharathrajkumar M, et al. Enhanced cipher text-policy attribute-based encryption and serialization on media cloud data. *International Journal of Pervasive Computing and Communications* 2022; doi: 10.1108/IJPCC-06-2022-0223

14. Ge C, Susilo W, Baek J, et al. A verifiable and fair attribute-based Proxy Re-Encryption scheme for data sharing in clouds. *IEEE Transactions on Dependable and Secure Computing* 2021; 19(5): 2907–2919. doi: 10.1109/TDSC.2021.3076580