A Survey of State-of-the-Art Multi-Authority Attribute Based Encryption Schemes in Cloud Environment

Reetu Gupta[1*], Priyesh Kanungo[1], and Nirmal Dagdee[2]
[1]School of Computer Science and Information Technology,
DAVV, Indore, India.
[e-mail: reetu.gupta0211@gmail.com, priyeshkanungo@gmail.com]
[2]Shivajirao Kadam Institute of Technology and Management,
Indore, India.
[e-mail: nirmaldagdee@gmail.com]
[*]Corresponding author: Reetu Gupta

Received July 12, 2022; revised November 10, 2022; accepted December 21, 2022; published January 31, 2023

Abstract

Cloud computing offers a platform that is both adaptable and scalable, making it ideal for outsourcing data for sharing. Various organizations outsource their data on cloud storage servers for availing management and sharing services. When the organizations outsource the data, they lose direct control on the data. This raises the privacy and security concerns. Cryptographic encryption methods can secure the data from the intruders as well as cloud service providers. Data owners may also specify access control policies such that only the users, who satisfy the policies, can access the data. Attribute based access control techniques are more suitable for the cloud environment as they cover large number of users coming from various domains. Multi-authority attribute-based encryption (MA-ABE) technique is one of the propitious attribute based access control technique, which allows data owner to enforce access policies on encrypted data. The main aim of this paper is to comprehensively survey various state-of-the-art MA-ABE schemes to explore different features such as attribute and key management techniques, access policy structure and its expressiveness, revocation of access rights, policy updating techniques, privacy preservation techniques, fast decryption and computation outsourcing, proxy re-encryption etc. Moreover, the paper presents feature-wise comparison of all the pertinent schemes in the field. Finally, some research challenges and directions are summarized that need to be addressed in near future.

Keywords: Attribute-based Encryption, Multi-authority, Policy Update, Privacy Preservation, Revocation.

1. Introduction

The technological innovations and advancements of ICT are directing the individuals and organizations to put enormous digital data online i.e., to increase their data sharing efforts. Organizations are scattered around the globe and distributed environments like cloud systems can be used to enable data sharing proficiency amongst them. Online data sharing results in various benefits like higher productivity, less time compared to manual exchange of data and retrieval of updated data from anywhere, at any time [1]. Business industries, government sectors, online social and commercial platforms, etc. are the major application domains requiring data sharing among various entities. One of the important application areas is mobile health care system, where the healthcare providers use various types of wearable sensors and mobile devices to access patient's health data and provide proper medical treatment to save their lives in critical conditions. Healthcare organizations may use the cloud to store and distribute electronic medical records, removing the geographical reliance between numerous entities, such as doctors, pharmacy labs, researchers, insurance companies, patients etc. [2]. Though these kind cloud-based data sharing services provide enormous advantages, they also open up a wide range of security and privacy issues [3][4].

As the data owner and organizations outsource their data to cloud, the direct control over the data is lost. The majority of data kept in the cloud is very sensitive, such as medical information, important research investigations etc. Encrypting sensitive data before sending it to the cloud is a natural way to secure it. Because the trust domain of cloud storage servers differs from that of users, the cloud server cannot decide who can access the data or who cannot. Access control techniques are required to ensure that only authorized users will be able to access the encrypted data.

Various techniques of access control have been presented for protecting the data contents and its privacy. Attribute based access control is the most promising technique as the access is granted depending upon the attributes carried by the user. Attribute Based Encryption (ABE) [5] provides an approach for allowing the data owner to specify data access policies inside the encrypted data. The users who possess the desired attributes can only decrypt the encrypted data. There are two types of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE).KP-ABE implements policy in the users' private keys. Hence, once the key is issued, the limited number of users can access the encrypted data. Another form called CP-ABE [6] is a public-key encryption technique, in which the user's private key is specified using a set of attributes and the ciphertext is linked to an access policy. When both of these match, the user is able to decrypt the data. As the access control is based on attributes possessed by the user, CP-ABE schemes cover a large group of users. Attributes are issued to the user by various attribute authorities, which may belong to single or multiple domains. According to this, the schemes are bifurcated in single or multi-authority CP-ABE schemes. Multi-authority CP-ABE schemes are best suited for major applications like e-health, e-government etc., where users get their attributes issued from multiple domain authorities.

1.1 Contribution of this study

Recently, various studies and surveys are made in the field of privacy and security issues in cloud computing. Author in the review paper [4] presented a privacy security framework for cloud computing. The review provided a detailed discussion on access control, ABE schemes, hierarchical ABE schemes, searchable encryption and trust based schemes. Another work [7] [9] analyzed security and privacy challenges in cloud data storage. Some of the features of ABE schemes are discussed in brief. The survey in [8] focused on CP-ABE variations specific

for mobile cloud computing. The majority of the survey papers gave general discussions on cloud security issues and challenges.

Multi-authority CP-ABE schemes are specially designed to provide access control requirements for large open access environments. The main objective of this work is to aid readers in the field by offering a systematic analysis of multi-authority ABE schemes and their numerous essential features. This paper is different from the existing survey papers in many respects. First, the state-of-the-art access control techniques are examined. Second, many useful features to standard multi-authority CP-ABE schemes that have improved their efficacy and usability are catalogued. These features include attribute and key management techniques, access policy structure and its expressiveness, revocation of access rights, policy updating techniques, privacy preservation techniques, fast decryption and computation outsourcing, proxy re-encryption, delegation of access rights etc. Third, the paper compares and contrasts several MA-CP-ABE schemes with regard to their characteristics and the cost of storage and computation they require. Finally, several research directions are outlined to promote the design of customized ABE techniques in the area.

1.2 Paper organization

The remainder of the document is structured as follows. In section 2, the multi-authority ABE concept is explained with the help of an example of mobile health care system. The system model and syntax for the algorithms are also discussed. Section 3 described the methodology used for systematic literature review (SLR). In section 4, the major functional features presented in current research work are analyzed. In section 5, different schemes are investigated based on various features and a comparison among them is presented. In section 6, research challenges and directions are summarized. Section 7 concludes the paper.

2. Multi-authority CP-ABE scheme

2.1 An example

Online data sharing has become a necessity in today's world. It has immense benefits in many application areas. Let us consider example of an m-health care system, where a patient as the data owner, wants to share his medical records with a doctor, who has specialization in "Cardiology" and has some association in renowned research centers. The patient defines the access policy as ("Cardiologist" AND "Research associate") while doing encryption and then outsources his data in encrypted form on the cloud storage server. Any doctor, who has the attribute "Cardiologist" issued by a hospital and the attribute "Research associate" issued by a university research center, can access his records. In the above example, hospital and university research center are the two attribute issuing authorities.

2.2 System model

Fig. 1 shows a generic system model of multi-authority ABE schemes. The entities of the system are: the central authority called CA, the attribute authorities called AA, the data owner (DO), the cloud service provider (CSP) and the data user (DU). The CA sets up the global public parameters for the system. It also handles registration process of both the AAs and the users. Each AA issues secret key to the users for the attribute set managed by him. Users can apply for secret keys for the corresponding attributes. The data owner encrypts his data with the suitable access policy and sends the ciphertext to the cloud storage provider i.e. CSP. The

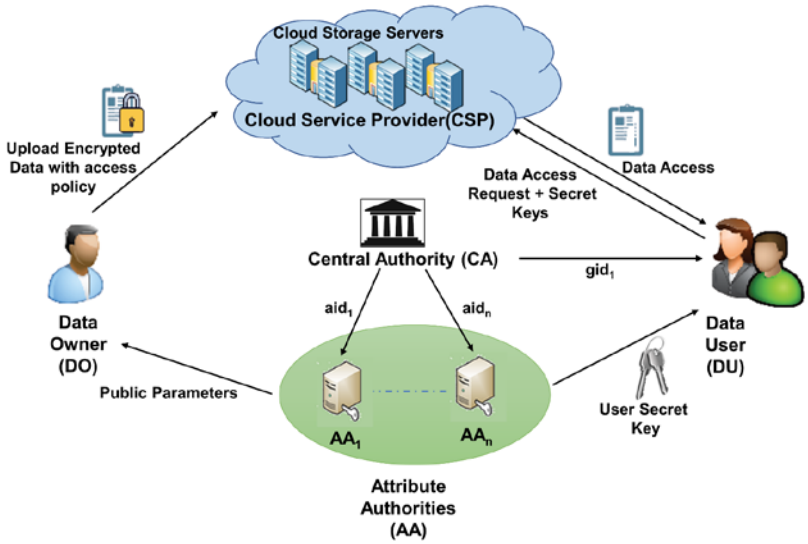


Fig. 1. System model of multi-authority ABE scheme

CSP essentially acts as a resource provider in place of the cloud, replicating that role for the cloud. The data owners use its data storage service and the users send query to the CSP for required data to access it.

2.3 Algorithms

The four fundamental algorithms of a multi-authority CP-ABE system are as follows:

1) System Initialization

GlobalSetup(λ)→GPP: The input to the algorithm is a security parameter, named λ and it returns the global public parameters GPP for the whole system.

CASetup(GPP)→(MPK, MSK): The central authority(CA) runs this algorithm and takes GPP as input. It produces public key MPK and secret key MSK.

AASetup(GPP, k, U_k)→(APK_k, ASK_k): Each authority AA_k runs this algorithm with GPP and with its attribute domain called U_k. No two authorities have common attribute domain, means for i ≠ j, $U_i \cap U_j = \emptyset$. This algorithm produces public key APK_k and secret key ASK_k fir the AAs.

2) Encryption

Encrypt(K, ψ, GPP, $\cup APK_k$) →(CT): This algorithm takes as input the system parameters GPP, a symmetric key K by which data is encrypted , an access structure ψ and the set of public keys of relevant authorities. It outputs the ciphertext CT.

3) User Key Generation

CAKeyGen(GPP,gid)→($CAPK_{gid}$,$CASK_{gid}$): This algorithm takes GPP and the user's gid as input. It produces gid related identity-key $CASK_{gid}$, which is used by the user and public key $CAPK_{gid}$, which is used by the AAs for generating attribute-related keys.

AAKeyGen($S_{gid,k}$, GPP, MPK, $CAPK_{gid}$, ASK_k)→($ASK_{S,gid,k}$): When a user requests k^{th} authority for generating keys for attribute set $S_{gid,k}$, AA_k runs this algorithm with inputs as $S_{gid,k}$, GPP, MPK, $CAPK_{gid}$ and ASK_k.

If $CAPK_{gid}$is invalid, then it returns $\perp$, else it returns corresponding attribute-related keys $ASK_{S,gid,k}$ for attribute set $S_{gid,k}$.

4) Decryption

Decrypt(CT,GPP,FK_{gid})→(K): The decryption algorithm takes inputs as the public parameter, the ciphertext CT and the set of final secret keys FK_{gid}. The decryption will be successful if and only if the user's attributes satisfy the access structure.

3. Methodology

To date, there has been a plethora of research papers written about multi-authority ABE schemes and their different features. To the best of our knowledge, there is no solitary research paper that comprehensively compares and contrasts the aspects of different multi-authority ABE schemes. A systematic review of the literature on multi-authority ABE schemes is conducted. The methodology adopted for SLR included following steps [45]: a) Formulate the research questions b) Decide inclusion criteria c) Search the current literature d) Extract data and assess quality e) Categorize and analyze the data.

a) Formulate the research questions: This survey is targeted to find the answers of following questions:

1. What features should the multi-authority ABE scheme contain to make it suitable for large open access environments?
2. Can MA-ABE schemes be customized to meet the security objectives of different applications?

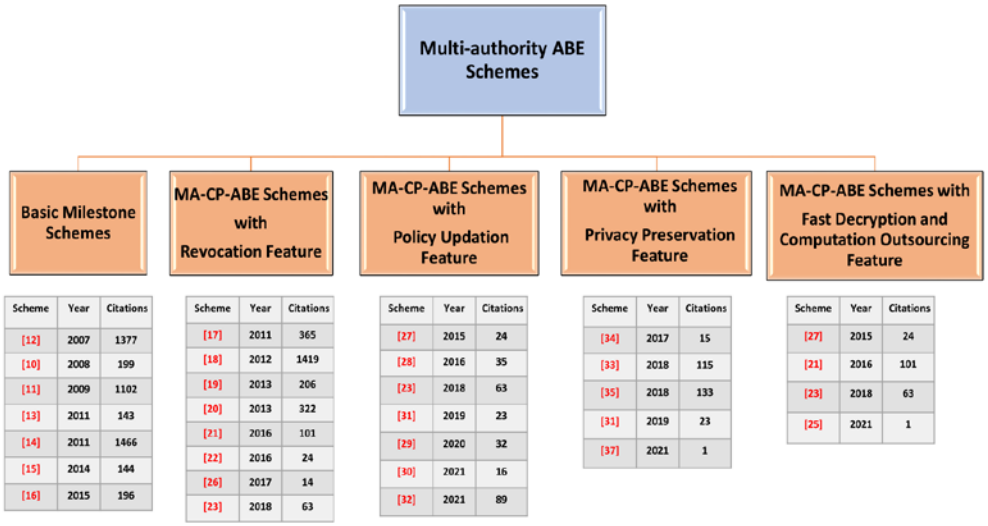
b) Decide inclusion criteria: The inclusion criteria considers following parameters:

1. The first step in doing a high-quality literature review is to include articles that have been published in peer-reviewed journals or presented at respected academic conferences.
2. The listed research papers should have been subjected to peer assessment.
3. There should be a large number of citations for the included papers.
4. Recent papers should be added to see the most recent updates and findings.

c) Search the current literature: As the survey targeted to review multi-authority ABE schemes, the search string included terms such as "Multi-authority", "Access Control Techniques", "Cloud-based data storage", "Dynamic and efficient access control". After examining the search results and survey papers discovered during the initial search, additional focused search queries were run to obtain more recent studies.

d) Extract data and assess quality: The research papers found based on the search criteria were then placed in an Excel spreadsheet for additional review based on the inclusion criteria. Initially, 130 papers were entered in the Excel sheet. After analyzing their publication information and number of citations, they were reduced to 44 papers.

e) Categorize and analyze the data: After reading and summarizing each of the 44 articles, they were categorized according to their respective features and characteristics. **Fig. 2** depicts the classification, relevant referenced article, and citation count for each category.



Scheme	Year	Citations
[12]	2007	1377
[10]	2008	199
[11]	2009	1102
[13]	2011	143
[14]	2011	1466
[15]	2014	144
[16]	2015	196

Scheme	Year	Citations
[17]	2011	365
[18]	2012	1419
[19]	2013	206
[20]	2013	322
[21]	2016	101
[22]	2016	24
[26]	2017	14
[23]	2018	63

Scheme	Year	Citations
[27]	2015	24
[28]	2016	35
[23]	2018	63
[31]	2019	23
[29]	2020	32
[30]	2021	16
[32]	2021	89

Scheme	Year	Citations
[34]	2017	15
[33]	2018	115
[35]	2018	133
[31]	2019	23
[37]	2021	1

Scheme	Year	Citations
[27]	2015	24
[21]	2016	101
[23]	2018	63
[25]	2021	1

Fig. 2. Classification of multi-authority ABE schemes

4. Understanding major functional features of multi-authority CP-ABE schemes

Prior to implementing multi-authority ABE in cloud-based data sharing systems, a number of practical challenges need to be resolved. As shown in systematic literature review, following functional features and characteristics of existing approaches are highlighted.

4.1 Attribute and key management:

In single authority ABE schemes, there is a single trust domain and only one authority issues all private keys. In multi-authority ABE schemes, multiple parties play the role of authority and manage multiple trust domains. There are two categories of managing attribute universe in ABE schemes -large universe and small universe. In large universe ABE constructions, any string can be used as an attribute, and the attributes are not necessarily enumerated at system setup. On the other hand, in small universe ABE constructions, the attributes are fixed and enumerated at the system setup. Any change or even addition of a single attribute will result in rebuilding the system and possibly re-encrypting all the data. Large universe MA-ABE schemes are considered as promising schemes.

4.2 Access policy structure and its expressiveness:

The granularity of access control system is determined by the expressiveness of its access policy in the ABE scheme. In the literature, various access structures are employed. These include the threshold policy, the tree policy, the linear secret sharing scheme (LSSS), and the ordered binary decision diagram (OBDD). The schemes using LSSS structure are comparatively more expressive and efficient.

4.3 Revocation of access rights:

Revocation of access rights can be categorized in three types: attribute revocation, user revocation and key revocation. In attribute revocation schemes, an attribute is removed from the system, and all the users who have been granted the attribute, will lose it. In user revocation schemes, if a user is removed from the system, then she/he loses all her/his attributes. In key

revocation schemes, the revoked user only loses one or more attributes, and she/he can access the data as long as her/his remaining attributes satisfy the access policy. In the above example of m-health system, if the doctor resigns from his post of “Research associate”, then in that case, he should not be able to decrypt previously shared data anymore. Key revocation techniques are preferred in real life applications.

4.4 Policy updating techniques:

Data owners may require changing their access policy for various reasons, e.g., the patient may suffer from diabetes when he is being treated for heart disease. In that case, he needs to update his access policy to allow endocrinologist doctors. In this case, the new policy will be [(“Cardiologist” AND “Research associate”) OR “Endocrinologist”]. Policy updating allows data owners to manage their access policy with flexibility.

4.5 Policy privacy preservation:

In normal attribute-based encryption schemes, the access policy is shared publicly along with the ciphertext. This exposure of policy may disclose sensitive information about the encrypting and decrypting parties, e.g., in the policy [(Patient = “INP201” AND Hospital = “Apollo”) OR (Doctor = “Cardiologist” AND Hospital = “Apollo”)], it is revealed that the patient is being treated by the doctor in ‘Apollo’ hospital and suffering from heart disease. The attribute values contain more sensitive information. ABE schemes with partially hidden policies only consist of the attribute names in access policy, not their value. Like, if the attribute values are made hidden, the above policy becomes [(Patient = “*” AND Hospital = “*”) OR (Doctor = “*” AND Hospital = “*”)]. Some fully policy-hidden approaches are also proposed in literature, but partially policy hiding approaches are more usable.

4.6 Fast decryption and computation outsourcing:

Most of ABE schemes are having expensive decryption costs. The decryption cost linearly increases with the number of involved attributes in the access policy. Outsourcing the expensive decryption phase procedures to a third-party server is one of the solutions to this issue. The semi-trusted cloud server uses a transformation key derived from the user’s secret key. It generates a partially decrypted ciphertext of the same message and sends it to the user. The original message may then be recovered using the short ciphertext and the user's secret key with only one exponentiation operation. However, the semi-trusted cloud server partially decrypts the ciphertext, it cannot gain any information about the encrypted message. The users have to trust the semi-trusted third-party server for partial decryption.

5. Comparison of various multi-authority ABE schemes

In this section, all the enumerated multi-authority ABE schemes are theoretically investigated and assessed by comparing their salient characteristics and performance metrics. **Table 1** provides a summary of the notations.

Table 1. The notations in performance analysis

Notation	Description
$\|G\|$	No. of bits needed to represent an element in group G
$\|G_T\|$	No. of bits needed to represent an element in group G_T
$\|*\|$	No of elements in *
n	The size of universe of attributes

A_C	Attribute set used in encryption
A_U	User's attribute set
E	One exponential operation
P	One pairing operation
n_c	Count of CAs in the system
n_a	Count of AAs in the system
I	Attributes of satisfying set
n_{pud}	Number of AAs in public domain (PUD)
m	Number of attribute types in PUD
P_a	Size of attribute's path key
r	Number of revoked users
l_1', l_2', l_3'	Numbers of attributes of type 1, 2, and 3 respectively in policy update
n_v	Numbers of values all the attributes in the system may have (an attribute may have multiple values)
n_u	Numbers of possible values of the attribute the user holds
$\rho \in (0,1)$	Wildcard coefficient

5.1Basic milestone schemes

Multi-authority ABE was firstly proposed in the work [12] where a single CA and multiple AAs controlled the key management task. The CA and AAs were responsible for issuing keys for identity and keys for attribute respectively. The concept of global identifier (GID) was used to prevent user collusion problem. However, the CA was capable of decrypting any ciphertext. Also, due to use of the user's GID, his privacy could not be preserved. [10] designed a threshold MA-ABE without the requirement of CA. They employed protocol for key generation in distributed manner. To demolish the requirement of the CA, they used distributed key distribution protocol (DKG) and joint zero secret sharing (JZSS) protocols. The problem of this scheme was that the system requires choosing threshold 't' at the setup time and if more than 't' users collude, system's security could be compromised. [11] improved their scheme [12] and proposed the scheme CC-MA-ABE by removing CA and introducing anonymous key distribution mechanism with the help of pseudo random functions (PRF). [13] proposed a fully secure MACP-ABE scheme, where multiple CAs and AAs were involved in key management for the users. CAs managed keys regarding identity, while the AAs managed the attribute keys for the users. The scheme was proved secure under standard model. Authors in scheme [14] designed CP-ABE for decentralized system. They used linear secret sharing scheme aka LSSS for defining policy for access control. No authorities need to coordinate at the setup and key generation time. Due to decentralized system, the CA was not required. In this scheme, a hash function on the users' GID was used while issuance of attribute keys from multiple authorities. The scheme provided collusion resistance. The scheme was proved secure under random oracle model. In ESORICS 2014, [15] presented decentralized CP-ABE scheme in the standard model. To provide privacy-preservation, a key extract protocol was used, but the scheme was not able to resist collusion attacks. Authors in scheme [16] proposed an efficient MA-CPABE system for large-universe, which used the prime-order bilinear groups. The advantage of using prime-order groups is that they are faster than the groups of composite order. **Table 2** compares the characteristics of various milestone multi-authority ABE schemes. **Table 3** summarizes the comparison of storage overhead and computational costs of encryption and decryption process.

Table 2. Comparison of characteristics of various milestone schemes

Scheme	Description	CP/KP-ABE	Large Universe	Policy Expressiveness	Group Order	Security Model	Shortcoming
[12]	• Single CA and multiple AAs • GID was used to prevent user collusion problem	KP-ABE	χ	Threshold	Prime	SM	• CA was capable of decrypting any ciphertext • Only supported an AND policy • Privacy of user is not preserved due to use of consistent GID
[10]	• Threshold multi-authority ABE without the requirement of CA • DKG and JZSS protocols were used to remove the CA	MA-FIBE	χ	Tree	Prime	SM	• If more than 't' users collude, system's security can be compromised
[11]	• Removed requirement of CA by introducing anonymous key distribution mechanism with the help of PRF	KP-ABE	χ	Threshold	Prime	SM	• Only supported an AND policy • User should get at least one attribute from each of the authorities
[13]	• Multiple CAs and multiple AAs • Fully secure in standard model	CP-ABE	χ	LSSS	Composite	SM	• The cooperation of all CAs in order to provide identity-related keys to users may create issues in the system
[14]	• Decentralized CP-ABE scheme • No requirement of CA • Cooperation between the multiple authorities at the setup time is not required • The users' GID is fed to a hash function to incorporate collusion resistance • Fully secure in random oracle model	CP-ABE	χ	LSSS	Composite	ROM	• Composite order groups are slower • The authorities can trace user's GID and gain knowledge about his attributes
[15]	• Proposed decentralized CP-ABE supporting privacy preservation • Each authority can work independently; no change required if new authority joins the system or any authority leaves • GID's are used in user's secret keys' calculation and an anonymous credential system is used to preserve his privacy	CP-ABE	χ	LSSS	Prime	SM	• The scheme cannot resist collusion attacks • The scheme is unable to provide privacy of attributes
[16]	• Large-universe multi authority ciphertext-policy attribute-based encryption system • This uses the prime-order bilinear groups, thus efficient and faster	CP-ABE	√	LSSS	Prime	ROM	• Selective security, not the full security

Table 3. Comparison of storage and computation cost of various milestone schemes

Scheme	Storage Overhead			Computation Cost		Assumptions
	Public Key	User's Secret Key	Ciphertext	Encryption	Decryption	
[12]	$\|G_T\| + (n+1)\|G\|$	$(\|1 + A_U\|)\|G\|$	$(1 + \|A_C\|)\|G\| + \|G_T\|$	$(2 + \|A_C\|)\,E$	$\|A_C\|(P+E) + P$	DBDH
[11]	$\|G_T\| + (1 + n + n_a)\|G\|$	$(1 + \|A_U\|)\|G\|$	$(\|1 + A_C\|)\|G\| + \|G_T\|$	$(2 + \|A_C\|)\,E$	$\|A_C\|(P+E) + P$	DBDH

[13]	$2n\|G_1\| + n_c\|G_T\|$	$(2n_c + n_a n_c + \|A_U\|)\|G\|$	$(2\|A_C\| + 1)\|G_1\| + \|G_T\|$	$(2\| A_C\| + 2)\ E$	$(2\|I\| + 1)P + \|I\|E$	New
[14]	$n\|G_1\| + n\|G_T\|$	$(\|A_U\|)\|G\|$	$2\|A_C\|\|G_1\| + (\|A_C\| + 1)\|G_T\|$	$(5\| A_C\| + 1)E$	$(2\|I\|)P + \|I\|E$	New
[15]	$(2n + 4n_a)\|G\| + n_a\|G_T\|$	$(6n_a + \|A_U\|)\|G\|$	$5\|A_C\|\|G\| + \|G_T\|$	$(6\| A_C\| + 1)E$	$(6\|I\|)P + (2\|I\|)E$	q-type
[16]	$n_a\|G\| + n_a\|G_T\|$	$(2\|A_U\|)\|G\|$	$3\|A_C\|\|G_1\| + (\|A_C\| + 1)\|G_T\|$	$(6\| A_C\| + 1)E$	$(3\|I\|)P + (\|I\|)E$	q-type

5.2 Revocation techniques in MA-CP-ABE schemes

The term "revocation" refers to an action that modifies a user's access permissions by removing all or part of that user's credentials. There are a number of suggested attribute-based access control systems that address revocation feature. There are three types of revocation: the revocation of an attribute, the revocation of a user, and the revocation of a key. In attribute revocation schemes, an attribute is taken out of the system, and all the users who had it will no longer have it. Second, revocation at the user level removes all permissions for that user. Even with the matching set of credentials, he is denied access to the data. Third is key revocation, where when a user loses certain attributes and still has others that fulfil the access criteria, he will be granted access to the data. Key revocation is fine-grained revocation approach, while user-level revocation is a coarse-grained revocation approach. The schemes handling revocation should effectively satisfy the requirement of backward and forward secrecy. In a system with backward secrecy, a user who enters the system and receives a secret key for any attribute (if that fulfils the access policy) would not be able to decrypt any ciphertext that was released before he joined the system. Forward secrecy, on the other hand, ensures that a user whose attribute key has been revoked cannot utilize his old secret keys to decrypt any newly released ciphertext unless his remaining attributes still meet the access policy. There are two mechanisms for implementing revocation. The first one is direct revocation, where a revocation server is added to the system. Data owner attaches revocation list with ciphertext. User's secret key carries identity and attributes of the user. The users who are not on the revocation list and whose attributes meet the requirements of the access policy, perform the decryption of the ciphertext. The second is indirect revocation, where the authority only provides new keys to the users who have not been revoked. The revoked users can no longer decrypt any ciphertext that has been created after they were removed. This approach may cause significant computational overhead because of the need of ciphertext and key updation. Authors [17] proposed a revocable ABE for cloud environment. In their system, the data owner changes the ciphertext and sends it to all the users. This is done whenever an attribute is revoked from a user. This creates a heavy communication overhead, which becomes performance bottleneck in the system. It is also important that the data owner has constant internet access. [18] proposed an ABE scheme, which is derived from the [11] scheme. In their system, users were divided into public and personal domains aka PUD and PSD respectively depending upon their roles in the system. They used policy based on conjunctive normal form (CNF), but the revocation method proposed by them was only for KP-ABE scheme. [19] presented multi-authority anonymous ABE. To implement user revocation, privilege tree is used for the data re-encryption. [20] proposed revocation scheme in multi-authority setting. Here, version number is assigned to each attribute present in the system. In case of attribute revocation, the authority generates a new version key for the attribute. All the remaining non-revoked users update their secret keys with the update key generated after attribute revocation. The cloud server updates the affected ciphertext components with the

revoked attribute.[21] proposed the MA- CP-ABE scheme, which was developed using composite order bilinear groups that supports the attribute revocation and decryption outsourcing. When a revocation happens, the authority generates a new key, and a remote cloud server handles the re-encryption. [22] achieved attribute revocation by distributing task of decryption key generation to various AAs and they simply stop updating of the corresponding key when performing revocation. Schemes [23][24] also provided feature of outsourced decryption with revocation. [23] added policy update feature also. [25] handled the problem of key abuse.

A comparison of the characteristics of all the above mentioned revocable multi-authority schemes is presented in **Table 4**. **Table 5** summarizes the comparison of storage overhead and computational costs of encryption and decryption process of various schemes

Table 4. Comparison of characteristics of various revocable MA-CP-ABE schemes

Scheme	Description	Revocation Type	Large Universe	Policy	Group Order	Security Model	Key Update By	Cipher-text Update By	Shortcoming
[17]	• Proposed attribute revocation by updating [14] scheme	Attribute	χ	LSSS	Prime	ROM	χ	Data owner	• The data owner must re-encrypt the CT and send a new CT component to every user who has not been revoked. This incurs significant computation and communication cost. • Data owner should be online all time.
[18]	• Used multi-authority ABE by [11] to realize secure health record access control • Divided the users of the PHR system into PUD and PSD domains based on the authorities issuing them the credentials • No CA Exists	User and Attribute	χ	Threshold	Prime	SM	AA	Cloud Server	• The revocation method is only for KP-ABE systems
[19]	• The concept of privilege tree is used • Authorized users with privilege can re-encrypt the data to forbid revoked users' access	User	χ	Tree	Prime	ROM	χ	Users with privilege	• Authorized users may change the access policy when they perform re-encryption. This hampers the confidentiality of data • Each authority need to coordinate with others, which in turn increases communication cost and also results in low scalability
[20]	• Designed MA-CP-ABE scheme with revocation • Scheme permitted both forward and backward security • Introduced a version key into each attribute	Attribute	χ	LSSS	Prime	ROM	AA	Cloud Server	• AAs handle the computation overhead for an update key for each non-revoked user
[21]	• Designed an attribute-level user revocation method in standard model • Subset-cover revocation framework is used • A third-party sever used a set of	Attribute	χ	LSSS	Composite	SM	AA	Cloud Server	• To address revocation attribute key encryption key (KEK) binary trees are maintained; For large group maintaining binary tree becomes much harder

	attribute group keys aka AGAs to re-encrypt ciphertexts								• Users need to store KEKs additionally
[22]	• The AAs job is to update the attribute-related keys time-to-time • User's attribute secret key contains time attribute along with identifiers • The system has the advantage that it does not impose limits on the numbers of users, revoked user's attributes and time periods	Attribute	χ	LSSS	Composite	ROM	AA	χ	• The single-point failure issue arises because each AA is responsible for a different subset of the whole collection of attributes
[26]	• Scheme based on [14] scheme • Data owner designs a blacklist to resist role-based collusion in public domain • Lazy revocation mechanism used • Two revocation methods according to update settings (using the same update settings or using new ones)	User and Attribute	χ	LSSS	Composite	ROM	AA	Cloud Server	• Issues may occur while maintaining update parameters in the attribute history list (AHL) • Maintenance of blacklist is done by third party and also mapping of list to attributes is a challenging task
[23]	• Designed a practical MA- ABE scheme supporting attribute revocation and large-universe • Decryption outsourcing and policy updating features are added • Subset-cover revocation framework is used	Attribute	√	LSSS	Prime	ROM	AA	Cloud Server	• To address revocation attribute KEK binary trees are maintained; For large group maintaining binary tree becomes much harder • Users need to store KEKs additionally
[24]	• Scheme supported multi-authority setting, efficient user revocation and decryption outsourcing • Revocation list (RL) is maintained by the CAs • Cloud server performs re-encryption for ciphertext updation	User	√	LSSS	Prime	ROM	Cloud Server	Cloud Server	• For each revoked user present in RL, cloud server has to re-encrypt the ciphertext. It inserts the GIDs of revoked users into the new ciphertext • Refreshing of RL should be there so that no repetitions occur while updating CTs
[25]	• Author proposed scheme for decentralized MA-ABE with revocation and for large universe • No key abuse attacks may compromise the scheme. • User outsources decryption to CSP to minimize the number of decryption operations.	User, Key and Attribute	√	LSSS	Prime	ROM	χ	χ	• The security can be improved by proving it in SM. • Access structure can be hidden to improve privacy.

Table 5. Comparison of storage and computation cost of various revocable MA-CP-ABE schemes

Scheme	Storage Overhead			Computation Cost		Assumption
	Public Key	User's Secret Key	Ciphertext	Encryption	Decryption	
[17]	$n\|G_1\| + n\|G_T\|$	$(\|A_U\|)\|G\|$	$2\|A_C\|\|G_1\| + (\|A_C\| + 1)\|G_T\|$	$(5\|A_C\| + 1)E$	$(2\|I\|)P + \|I\|E$	New
[18]	$(n + n_a + 1)\|G_1\| + \|G_T\|$	$(\|A_U\| + m + 1)\|G\|$	$(\|A_C\| + m + n_{pud} - 1)\|G\| + \|G_T\|$	$(\|A_C\| + n_a + 2)E$	$(\|A_C\| + n_a)(P + E) + P$	DBDH
[20]	$(2n_a + 2n)\|G\| + n_a\|G_T\|$	$(2n_a + \|A_U\|)\|G\|$	$(2 + 4\|A_C\|)\|G\| + \|G_T\|$	$(5\|A_C\| + 3)E$	$(6\|I\|)P + (2\|I\|)E$	DBDH
[21]	$(n + n_a + 1)\|G_1\| + n_a\|G_T\|$	$(2 + n_a + \|A_U\|)\|G\| + n_a P_a\|Z_p\|$	$(1 + 2\|A_C\|)\|G\| + \|G_T\|$	$(2 + 3\|A_C\|)E$	E *Outsourced decryption $(\|I\|)E + (2\|I\| + 1)P$	new

[22]	$(n+1)\|G_1\|+n\|G_T\|$	$(\|A_U\|))\|G\|$	$2n_1\|G_1\|$ $+(n_1+1)\|G_T\|$	$(5\|A_C\|+1)E$	$(2I)\ P+(I)\ E$	new
[26]	$2n\|G_1\|$	$(\|A_U\|\ )\|G\|$	$2\|A_C\|\|G_1\|+$ $(\|A_C\|+1)\|G_T\|$	$(4\|\ A_C\|+1)E$	$(2\|I\|)P+\|I\|E$	new
[23]	$n_a\ (\|G\|+\|G_T\|)$	$(2\|A_U\|)\|G\|+n_a\ P_a\|Z_p\|$	$(3\ +\ 3\|A_C\|)\|G\|\ +(2\ +$ $3\|A_C\|)\|G_T\|+\|Z_p\|$	$(6\|A_C\|+1)\ E$	$(3\|I\|)P+(\|I\|+1)E$ *Outsourced decryption $(4\|I\|+1)E$	q-type
[24]	$(2n_a\ +1)\|G\|+n_a\ \|G_T\|$	$(2\|A_U\|+1)\|G\|+\|Z_p\|$	$(5\|A_C\|+2r)\|G\|+\|G_T\|$	$(7\|A_C\|+1)\ E$	E *Outsourced decryption $(4\|I\|)P+(2\|I\|)E$	q-DPBDHE2
[25]	$n_a\ (\|G\|+\|G_T\|)$	$\|Z_p\|$ *in CSP's UL $(3+\ 2\|A_U\|)\|G\|$	$3\|A_C\|\|G_1\|+$ $(\|A_C\|+1)\|G_T\|$	$(6\|\ A_C\|+1)E$	E *Outsourced decryption $(3\|I\|)P+(2\|I\|)E$	q-DPBDHE2

5.3 Policy updating techniques in MA-CP-ABE schemes

Deploying ABE schemes in practice require that the data owner may get the flexibility to update the access policy when required. In recent years, various MA-ABE schemes have included policy updation feature in their scheme. Effective access control with policy updating for big data in the cloud was suggested in a the study [32]. An effective attribute revocation and policy updating fine-grained access control method (FAC) for the smart grid was suggested by [27]. [28] proposed adaptively secure CP-ABE with policy updation feature in multi-authority scenario. They chose the standard model for proving security. Some large-universe multi-authority ABE schemes [23][29][30] were also proposed which support policy updating feature with added-on features of either the traceability or outsourced decryption. To update the policy dynamically, the scheme runs the algorithm for generating the update key and then CSP updates the ciphertext using that update key.[31] designed a privacy-preserving MA-ABE scheme for PHR system. They provided feature of dynamic policy update. **Table 6** compares the features of various policy updatable MA-ABE schemes. **Table 7** summarizes the comparison of storage overhead and computational costs of encryption and decryption process

Table 6. Comparison of characteristics of various MA-CP-ABE schemes with policy update

Scheme	Description	Large Universe	Policy	Group Order	Security Model	Shortcoming
[32]	• Proposed a novel scheme enabling efficient access control with dynamic policy updating for cloud based big data • The cloud server receives the query for policy update without decrypting the secured data • Algorithms for updating policies exist for a variety of access control policies	χ	LSSS	Prime	Generic bilinear Group	• The authors used the random oracle model as security model and used composite-order groups; however, they were unable to provide the proof of security.
[27]	• Presented a fine-grained access control framework for smart grid with features like attribute revocation and policy updation • Attribute revocation is supported with the use of a third-party auditor	χ	LSSS	Prime	SM*	• There was a need of a central authentication system to combine the secret keys. Every ciphertext in the system was vulnerable since the authentication system can decrypt them all • Having such a facility also raises the cost of computation and communication to operate and maintain
[28]	• Proposed a method called DPU-CP-ABE for dynamic policy update • Adaptive security in the standard model was presented for the scheme • The scheme had provision for update of any kind of policy	χ	LSSS	Composite	SM	• In the scheme, users get keys issued from multiple CAs and AAs. Since all CAs are involved, the cost of communication and storage goes up when user attribute keys are generated

[23]	• MA-ABE scheme for a large universe was proposed that allowed policy updates, attribute revocation, and decryption outsourcing	√	LSSS	Prime	ROM	• The scheme does not provide feature of privacy preservation and traceability. Traceability is needed to identify the malicious user who is responsible for leaking decryption keys
[31]	• Proposed a privacy-preserving MA-ABE scheme for PHR system • Authors provided feature of dynamic policy update	χ	LSSS	Prime	SM	• Large attribute domain is not a function of the scheme • It does not support traceability
[29]	• Authors presented a MA-CP-ABE scheme to support features like traceability, decryption outsourcing a and access policy update	√	LSSS	Prime	ROM	• The scheme does not provide feature of privacy preservation
[30]	• Proposed scheme with features like multiple authority, white box traceability, access policy update, and large universe	√	LSSS	Prime	ROM	• The scheme does not provide feature of privacy preservation

Table 7. Comparison of storage and computation cost of various MA-CP-ABE schemes with policy update

Scheme	Storage Overhead						Computation Cost	
	Public Key	User's Secret Key	Ciphertext	Update Keys			Encryption	Decryption
				Type1	Type2	Type3		
[32]	$n\|G_T\| + n\|G\|$	$\|G\|(\|A_U\|)$	$\|G_T\| + 3\|A_C\|\|G_1\|$	$2l'_1\|G\|$	$2l'_2\|G\| + \|Z_p\|$	$3l'_3\|G\|$	$(5\|A_C\| + 1)E$	$(2\|I\|)P + \|I\|E$
[27]	$(2n+1)\|G\| + (n+2)\|G_T\|$	$(2\|A_U\| + 2)\|G\| + \|Z_p\|$	$(2\|A_C\| + 1)\|G\| + (\|A_C\| + 1)\|G_T\|$	$2l'_1\|G\|$	$2l'_2\|G\| + \|Z_p\|$	$3l'_3\|G\|$	$(5\|A_C\| + 2)E$	E *Outsourced decryption $(2\|I\| + 1)P + (\|I\|)E$
[28]	$2n_a\|G_1\| + n_c\|G_T\|$	$(2n_c + n_a n_c + \|A_U\|)\|G\|$	$(2\|A_C\| + 1)\|G_1\| + \|G_T\|$	$l'_1\|G\|$	$l'_2\|G\| + \|Z_p\|$	$2l'_3\|G\|$	$(2\|A_C\| + 2)E$	$(2\|I\| + 1)P + \|I\|E$
[23]	$n_a(\|G\| + \|G_T\|)$	$(2\|A_U\|)\|G\| + n_a P_a\|Z_p\|$	$(3 + 3\|A_C\|)\|G\| + (2 + 3\|A_C\|)\|G_T\| + \|Z_p\|$	$2l'_1\|G\|$	$2l'_2\|G\| + \|Z_p\|$	$4l'_3\|G\|$	$(6\|A_C\| + 1)E$	$(3\|I\|)P + (\|I\| + 1)E$ *Outsourced decryption $(4\|I\| + 1)E$
[31]	$n_a\|G_T\| + (n + n_v)\|G\|$	$(2\|A_U\|)\|G\|$	$\|G_T\| + (2\|A_C\| + 1)\|G\|$	$l'_1\|G\|$	$l'_2(\|Z_p\| + \|G\|)$	$2l'_3\|G\|$	$(5\|A_C\| + 1)E$	$(3\|I\|)P + \|I\|E$
[29]	$(3n)\|G\| + n\|G_T\|$	$(4\|A_U\| + 1)\|G\|$	$(4\|A_C\|)\|G\| + (\|A_C\| + 1)\|G_T\|$	$2l'_1\|G\|$	$2l'_2\|G\| + \|Z_p\|$	$5l'_3\|G\|$	$(5\|A_C\| + 1)E$	$(4\|I\|)P + \|I\|E$
[30]	$(2n)\|G\| + n\|G_T\|$	$(4\|A_U\| + 1)\|G\|$	$(4\|A_C\|)\|G\| + (\|A_C\| + 1)\|G_T\|$	$2l'_1\|G\|$	$2l'_2\|G\| + \|Z_p\|$	$5l'_3\|G\|$	$(5\|A_C\| + 1)E$	$(4\|I\|)P + \|I\|E$

5.4 Policy privacy preservation techniques in MA-CP-ABE schemes

In most ABE schemes, the access structure and the related ciphertext are both open to the public. Hence, the user who gets the ciphertext, also can see the contents of access structure. The access structure could reveal sensitive information about the person doing the decrypting or encrypting. To avoid the leakage of this private information, the access structure should be made hidden. Several research works have been introduced where policies are kept partially hidden in CP-ABE schemes. The attribute values are kept hidden to protect the sensitive information. [33] presented the first of its kind policy hidden ABE scheme using multi-attribute authority construction. For this, the scheme incorporated the one-way anonymous key agreement protocol. [34] proposed the idea for a MA-CP-ABE scheme with hidden policy and constant length ciphertext. [35] designed PHOABE, an outsourced ABE scheme using semi trusted cloud server and hidden policy. [31] introduced a privacy preserving MA-ABE scheme. In their schemes, the policy hiding was only to hide the values of attributes and they used LSSS matrix access structure. The scheme suggested for multi-authority scenario. [36]

proposed hidden CP-ABE scheme with efficient decryption and support to large universe. **Table 8** and **Table 9** presents comparison of the features of several policy privacy preservation multi-authority ABE schemes and comparison of storage overhead and computational costs of encryption and decryption process respectively.

Table 8. Comparison of characteristics of various MA-CP-ABE schemes with policy privacy preservation

Scheme	Description	Hidden Policy	Way of policy hiding	Large Universe	Policy	Group Order	Security Model	Shortcoming
[33]	• Proposed the first of its kind policy hidden ABE scheme using multi-attribute authority construction	Fully	One-way anonymous key agreement	χ	LSSS	Prime	ROM	• Encryption and decryption required a excessive computing cost
[34]	• Proposed idea for a MA-CP-ABE scheme with hidden policy and constant length ciphertext	Fully	Multi-valued attributes	χ	Access Tree	Prime	ROM	• Weaker policy (attribute)-hiding model • Policy not known until finally decrypted.
[35]	• Introduced PHOABE, a Policy-Hidden ABE scheme with outsourcing • Decryption process for MA-ABE scheme is partly delegated to a semi trusted cloud server aka STCS • Made fully hidden policy by obfuscating the attributes	Fully	One-way anonymous key agreement	χ	LSSS	Prime	ROM	• The scheme is proven selectively secure • Policy not known until finally decrypted.
[31]	• Introduced a privacy preserving MA-ABE scheme for PHR system • Dynamic policy update available	Partial	Attributes are bifurcated in name-value pair	χ	LSSS	Prime	SM	• The scheme does not have the functions of large attribute domain. • It does not support traceability.
[37]	• Proposed a decentralized MA-ABE scheme • Fully hidden access policy mode • Viete's formulas is used to convert the policy into a vector	Fully	Inner-Product Encryption	χ	AND gate access policy	Prime	ROM	• The scheme only achieves selective security

Table 9. Comparison of storage and computation cost of various MA-CP-ABE schemes with policy privacy preservation

Scheme	Storage Overhead			Computation Cost		Assumptions
	Public Key	User's Secret Key	Ciphertext	Encryption	Decryption	
[33]	$(n+n_a)\|G\| + n\|G_T\|$	$(2\|A_U\|)\|G\|$	$(2\|A_C\|+1)\|G\| + (\|A_C\|+1)\|G_T\|$	$(5\|A_C\|+2)E$	$(2\|I\|)P + \|I\|E$	new
[34]	$n(\|G\| + \|G_T\|)$	$n_u\|A_U\|\|G\|$	$2(\|G\| + \|G_T\|)$	$3E$	$2P$	q-BDHE
[35]	$(n+n_a)\|G\| + n\|G_T\|$	$(2\|A_U\|)\|G\|$	$(3\|A_C\|+1)\|G\| + \|G_T\|$	$(5\|A_C\|+2)E$	E *Outsourced decryption $(3\|I\|)P + E$	DBDH
[31]	$n_a\|G_T\| + (n + n_v)\|G\|$	$(2\|A_U\|)\|G\|$	$(2\|A_C\|+1)\|G\| + \|G_T\|$	$(5\|A_C\|+1)E$	$(3\|I\|)P + \|I\|E$	q-PBDHE
[37]	$(4+5n_a)\|G\| + n_a\|G_T\|$	$(2+4\rho\|A_C\|)\|G\|$	$(2+4\rho\|A_C\|)\|G\| + \|G_T\|$	$((2+4\rho\|A_C\|)E$	E *Outsourced decryption $(2+4\rho\|I\|)P$	DBDH, DLIN

5.5 Fast decryption and computation outsourcing in MA-CP-ABE schemes

The high cost of decryption is a major drawback of MA-ABE schemes, which is generally proportional to the complexity of the policy. Several researchers devised ABE methods that maintain a constant ciphertext size by imposing a fixed number of pairing operations during decryption. However, those schemes have limitation of restrictive access structures like threshold or AND gates access structures. Computation outsourcing can be achieved by running the decryption method on a semi-trusted server. The ciphertext and the public transformation keys are passed to the semi trusted server, which partly decrypt the ciphertext. With this partially decrypted ciphertext, the user has to do just one exponentiation operation to get the original ciphertext. Several schemes have been discussed earlier, which uses outsourced decryption. Decryption cost of schemes [27], [23], [21], [24] and [25] are summarized in **Table 5** and **Table 7**.

6. Research challenges and directions

Cloud storage and outsourcing services focus on storing, managing and processing large-scale data. These services allow anyone to access the data with flexibility. As the data owners delegate their data management task to untrusted third-party cloud service providers, the data access control becomes a crucial necessity in cloud environment. This section focuses some of the most significant challenges associated with the deployment and use of attribute-based access control techniques in cloud environment. The comparative analysis of the several multi-authority ABE schemes presented in earlier sections highlight various pros and cons of state-of-the-art techniques. The analysis helped in identifying the necessary requirements of the domain and summarizing the research challenges. Here some major research challenges are highlighted for further investigation:

- **Lightweight ABE schemes for mobile cloud computing:** With the rising usage of mobile devices, IoT devices and sensors, a fundamental problem in the mobile cloud computing environment is the development of a lightweight access control approach to enhance the security of outsourced data. The ABE schemes must have low computation overhead and should provide fine-grained access control. The viable solutions can be achieved by outsourcing the most of the encryption and decryption work to the cloud servers. As the semi-trusted servers perform the delegated encryption and decryption task, there is a need to ensure that partially encrypted and decrypted data is correct and not being altered. This leads to the requirement of verifiable outsourced ABE. Some of the researchers [38] [39] [40] [41] have worked in the direction of verifiable outsourced ABE schemes.
- **To prevent the abuse of decryption rights:** As most of the real-world applications are using cloud-based storage services, a common threat to existing ABE schemes is the leakage of decryption keys. A user may reveal his private key to an illegitimate third party. The mechanisms are needed to trace or recover the global identity of the guilty user. Researchers are working on two tracing approaches, white-box traceability and black-box traceability. Multi-authority ABE schemes with traceability feature are required to sort out the access control requirement of real-world applications.
- **Revocation addressed with backward and forward security:** As ABE schemes are appropriate solution to provide attribute-based access control to a large group of users, there is a need to handle new joining of the users and the revocation of their existing privileges. Users who are just now joining the system must not have access to the published data even if they have the necessary attributes to decrypt it. On the other hand,

when a specific attribute is revoked, a group of users who had such attribute must be prevented from decrypting any new ciphertext by using the revoked attribute.

- **Efficient and expressive ABE schemes with numerous characteristics:** There is a need to propose a customization of all the required features in a single ABE scheme. It should be multi-authority scheme to target users from all the varied domains. It should incorporate features of revocation, privacy preservation, policy updation, traceability and computation outsourcing. The computational complexity of the encryption and decryption operations should be minimized. The scheme should also provide accountability [42] [43] [44] i.e. the auditor in the system should be able to detect any type of secret key abuse either by a user or by some authority.

7. Conclusion

The provision of cloud storage is an essential component of cloud computing model. It allows the business organizations and consumers to use applications to access the shared data at any time, from anywhere. The cloud-computing paradigm raises a number of problems with regard to users' privacy and safety, despite the fact that it offers numerous appealing benefits. The use of attribute-based encryption is becoming more popular as a method to improve the data security and user privacy offered by the cloud services. The aim of this survey is to provide a comprehensive analysis of the various multi-authority schemes available in the literature. Specifically, several prominent features were discussed like attribute and key management techniques, access policy structure and its expressiveness, revocation of access rights, policy updating techniques, privacy preservation techniques, fast decryption and computation outsourcing and proxy re-encryption. Schemes were evaluated, and some were deemed to have an adequate balance of desirable characteristics. The study concludes that there are still considerable challenges to overcome and security issues to address in the realm of cloud storage. Future work includes the design of customized ABE techniques for upcoming application areas like cloud-assisted Internet of Things, Block chain etc.

References

[1] D. Thilakanathan, S. Chen, S. Nepal, and R. A. Calvo, "Secure data sharing in the cloud," *Security, privacy and trust in cloud systems*, pp. 45-72, 2014. Article (CrossRef Link)

[2] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," in *Proc. of 8th international conference on collaborative computing: networking, applications and worksharing (CollaborateCom)*, pp. 711–718, October 2012. Article (CrossRef Link)

[3] M. Wazid, S. Zeadally, A. K. Das, and V. Odelu, "Analysis of security protocols for mobile healthcare," *J. Med. Syst.*, vol. 40, no. 11, pp. 1–10, 2016. Article (CrossRef Link)

[4] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *J. Netw. Comput. Appl.*, vol. 160, p. 102642, 2020. Article (CrossRef Link)

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of the 13th ACM conference on Computer and communications security*, pp. 89-98, October 2006. Article (CrossRef Link)

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. of 2007 IEEE symposium on security and privacy (SP'07)*, pp. 321-334, May 2007. Article (CrossRef Link)

[7] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Futur. Gener. Comput. Syst.*, vol. 72, pp. 273–287, 2017. Article (CrossRef Link)

[8] S. Moffat, M. Hammoudeh, and R. Hegarty, "A survey on ciphertext-policy attribute-based encryption (CP-ABE) approaches to data security on mobile devices and its application to IoT," in *Proc. of the International Conference on Future Networks and Distributed Systems*, July 2017. Article (CrossRef Link)
[9] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," *Comput. Commun.*, vol. 111, pp. 120–141, 2017. Article (CrossRef Link)
[10] H. Lin, Z. Cao, X. Liang, and J. Shao, Lin, H., Cao, Z., Liang, X., & Shao, J, "Secure threshold multi authority attribute based encryption without a central authority," in *Proc. of International Conference on Cryptology in India*, pp. 426–436, December 2008. Article (CrossRef Link)
[11] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. of the 16th ACM conference on Computer and communications security*, pp. 121-130, November 2009. Article (CrossRef Link)
[12] M. Chase, "Multi-authority attribute based encryption," in *Proc. of Theory of cryptography conference*, pp. 515-534, February 2007. Article (CrossRef Link)
[13] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in *Proc. of European Symposium on Research in Computer Security*, pp. 278-297, September 2011. Article (CrossRef Link)
[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. of Annual international conference on the theory and applications of cryptographic techniques*, pp. 568-588, May 2011. Article (CrossRef Link)
[15] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. Au, "PPDCP-ABE: Privacy-preserving decentralized ciphertext-policy attribute-based encryption," in *Proc. of European Symposium on Research in Computer Security*, pp. 73-90, September 2014. Article (CrossRef Link)
[16] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *Proc. of International Conference on Financial Cryptography and Data Security*, pp. 315–332, January 2015. Article (CrossRef Link)
[17] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *Proc. of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 91-98, November 2011. Article (CrossRef Link)
[18] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, 2013. Article (CrossRef Link)
[19] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in *Proc. of 2013 Proceedings IEEE INFOCOM*, pp. 2625–2633, April 2013. Article (CrossRef Link)
[20] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, 2014. Article (CrossRef Link)
[21] Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," *Comput. Secur.*, vol. 59, pp. 45-59, 2016. Article (CrossRef Link)
[22] H. Cui and R. H. Deng, "Revocable and decentralized attribute-based encryption," *Comput. J.*, vol. 59, no. 8, pp. 1220–1235, 2016. Article (CrossRef Link)
[23] Z. Liu, Z. L. Jiang, X. Wang, and S.-M. Yiu, "Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating," *J. Netw. Comput. Appl.*, vol. 108, pp. 112–123, 2018. Article (CrossRef Link)
[24] 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, p. 22026, 2019. Article (CrossRef Link)
[25] K. Huang, "Revocable Large Universe Decentralized Multi-Authority Attribute-Based Encryption Without Key Abuse for Cloud-Aided IoT," *IEEE Access*, vol. 9, pp. 151713–151728, 2021. Article (CrossRef Link)

[26] H. Zheng, J. Wu, B. Wang, and J. Chen, "Modified ciphertext-policy attribute-based encryption scheme with efficient revocation for PHR system," *Math. Probl. Eng.*, vol. 2017, 2017. Article (CrossRef Link)
[27] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, "Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 4, pp. 1404–1423, 2015. Article (CrossRef Link)
[28] Z. Ying, H. Li, J. Ma, J. Zhang, and J. Cui, "Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating," *Sci. China Inf. Sci.*, vol. 59, no. 4, pp. 1–16, 2016. Article (CrossRef Link)
[29] K. Sethi, A. Pradhan, and P. Bera, "Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation," *J. Inf. Secur. Appl.*, vol. 51, p. 102435, 2020. Article (CrossRef Link)
[30] J. Ling, J. Chen, J. Chen, and W. Gan, "Multiauthority attribute-based encryption with traceable and dynamic policy updating," *Secur. Commun. Networks*, vol. 2021, 2021. Article (CrossRef Link)
[31] X. Yan, H. Ni, Y. Liu, and D. Han, "Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR," *Comput. Sci. Inf. Syst.*, vol. 16, no. 3, pp. 831-847, 2019. Article (CrossRef Link)
[32] K. Yang, X. Jia, K. Ren, R. Xie, and L. Huang, "Enabling efficient access control with dynamic policy updating for big data in the cloud," in *Proc. of IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 2013–2021, April 2014. Article (CrossRef Link)
[33] H. Zhong, W. Zhu, Y. Xu, and J. Cui, "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage," *Soft Comput.*, vol. 22, no. 1, pp. 243-251, 2018. Article (CrossRef Link)
[34] F. Yundong, W. Xiaoping, and W. Jiasheng, "Multi-authority attribute-based encryption access control scheme with hidden policy and constant length ciphertext for cloud storage," in *Proc. of 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pp. 205–212, June 2017. Article (CrossRef Link)
[35] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Comput. Networks*, vol. 133, pp. 141-156, 2018. Article (CrossRef Link)
[36] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system," *IEEE Access*, vol. 7, pp. 33202-33213, 2019. Article (CrossRef Link)
[37] L. Zhang, J. Ren, L. Kang, and B. Wang, "Decentralizing Multi-Authority Attribute-Based Access Control Scheme with Fully Hidden Policy," *Int. J. Netw. Secur.*, vol. 23, no. 4, pp. 588–603, 2021. Article (CrossRef Link)
[38] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. forensics Secur.*, vol. 8, no. 8, pp. 1343–1354, 2013. Article (CrossRef Link)
[39] J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," *Secur. Commun. Networks*, vol. 2017, 2017. Article (CrossRef Link)
[40] Z. Li, W. Li, Z. Jin, H. Zhang, and Q. Wen, "An efficient ABE scheme with verifiable outsourced encryption and decryption," *IEEE Access*, vol. 7, pp. 29023–29037, 2019. Article (CrossRef Link)
[41] N. Deng, S. Deng, C. Hu, and K. Lei, "An efficient revocable attribute-based signcryption scheme with outsourced unsigncryption in cloud computing," *IEEE Access*, vol. 8, pp. 42805–42815, 2019. Article (CrossRef Link)
[42] G. Yu, X. Ma, Z. Cao, W. Zhu, and J. Zeng, "Accountable multi-authority ciphertext-policy attribute-based encryption without key escrow and key abuse," in *Proc. of International Symposium on Cyberspace Safety and Security*, pp. 337–351, October 2017. Article (CrossRef Link)
[43] F. Xhafa, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing," *J. Supercomput.*, vol. 71, no. 5, pp. 1607–1619, 2015. Article (CrossRef Link)

[44] J. Ning, X. Dong, Z. Cao, and L. Wei, "Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud," in *Proc. of European Symposium on Research in Computer Security*, pp. 270–289, September 2015. Article (CrossRef Link)

[45] M. Templier and G. Paré, "A framework for guiding and evaluating literature reviews," *Communications of the Association for Information Systems*, vol. 37, 2015. Article (CrossRef Link)

Reetu Gupta is a research scholar in School of Computer Science and IT, Devi Ahilya Vishwavidyalaya, Indore, India. She received B.E. (Bachelor of Engineering-Computer Science & Engg.), ME (Master of Engineering- Computer Science & Engg), in 2001 and 2010 respectively. She has around 20 years of teaching experience in various engineering colleges. Her areas of interest are Data Security, Cryptography and Algorithm Design.

Dr. Priyesh Kanungo is working as a professor in School of Computer Science and IT, Devi Ahilya Vishwavidyalaya, Indore, India. He received ME, M Phil, Ph D. in Computer Engineering. His areas of Research are Distributed Scheduling (Dynamic Load Balancing), Cloud Computing etc. He is having 34 years of teaching experience in M Tech, MCA, MBA, BE etc. in Devi Ahilya Vishwavidyalaya, Indore. He has guided many PhD students and has published several highly cited research papers.

Dr. Nirmal Dagdee is a professor of Computer Science and having 35 years of teaching experience in various engineering colleges. His areas of interest are Computer Graphics, Data Security, and Neural Networks. He has authored several research papers that are published in reputed journals and conference proceedings. Currently, he is Director at Shivajirao Kadam Institute of Technology & Management, Indore, India.